МВД России
Санкт-Петербургский университет

И. Н. Васильева, В. И. Куватов

КРИПТОГРАФИЧЕСКАЯ ЗАЩИТА ИНФОРМАЦИИ

Практикум

Санкт-Петербург
2017

План 2017, поз.86

УДК 003.26
ББК 32.973
В 19

Васильева И. Н., Куватов В. И.
В 19 Криптографическая защита информации: практикум. СПб.: Изд-во СПб ун-та МВД России, 2017. – 260 с.

Практикум предназначен для организации проведения практических занятий и помощи в освоении дисциплины «Криптографическая защита информации» курсантами, обучающимися по специальности 10.05.05 Безопасность информационных технологий в правоохранительной сфере и по направлению подготовки 09.03.02 Информационные системы и технологии. Может быть также использован обучающимися других специальностей для углубленного изучения криптографии в рамках дисциплины «Основы информационной безопасности».

УДК 003.26
ББК 32.973

Рецензенты:

Бабкин А. Н.,кандидат технических наук, доцент
(Воронежский институт МВД России);
Заломов С. Г., заместитель начальника информационного центра
ГУ МВД по Санкт-Петербургу и Ленинградской области –
начальник вычислительного центра

СОДЕРЖАНИЕ

ВЫБОР ВАРИАНТА ЗАДАНИЙ

Во всех заданиях номер вариантаV совпадает спорядковым номером Kкурсанта в официальном списке взвода. Если номер в списке $K>25$, то номер варианта рассчитывается как $V=K-25$.

ТЕМА 1. ИСТОРИЯ КРИПТОГРАФИИ. КЛАССИЧЕСКИЕ ШИФРЫ

Классические алгоритмысимметричного шифрования подразделяются на два класса: шифры замены (подстановки) и шифры перестановки.

Применяемые на практике современные шифры имеют достаточно сложную структуру, их анализдостаточно трудоемок и неэффективен без наличия специальных инструментальных средств. В то же время все современные симметричные шифры (такие как алгоритмы ГОСТ 34.12–2015, AESи др.) базируются на многократном применении замен и перестановок.

Изучение и анализ простых классических шифров (табличные перестановки, простая имногоалфавитная замена – шифр Виженера) иллюстрируют некоторые важные приемы и методы криптоанализа и упрощают дальнейшее освоение идей современной криптографии.

Практическая работа №1. Изучение шифра перестановки«Поворотные решетки Кардано»

Описание шифра

Решетка Кардано – это прямоугольная или квадратная карточка с четным числом строк и столбцов$2k\times2m$. В ней проделаны отверстия (трафарет) таким образом, что при последовательном отражении или поворачивании и заполнении открытых клеток карточки постепенно будут заполнены все клетки листа.

Для шифрования текста прямоугольную карточку-трафарет сначала отражают относительно вертикальной оси симметрии, затем – относительно горизонтальной оси, и снова – относительно вертикальной, записывая текст в свободные клетки.

Если решетка Кардано – квадратная, то возможен и другой вариант ее преобразований – поворот на 90° (рис. 1), такие решетки обычно называют *поворотными*.

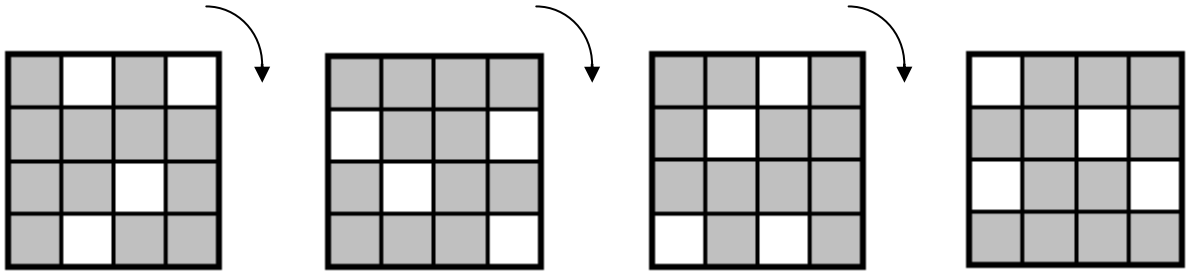


Рис. 1. Пример поворотной решетки Кардано

При записи текста в свободные клетки поворотной решетки обычным способом (слева направо и сверху вниз) словосочетание «наука о шифровании» (без пробелов) будет занесено в таблицу в следующем виде (рис. 2).

а	н	ф	а
а	р	н	о
и	ш	у	и
о	к	в	и

Рис. 2. Пример шифрования с помощью поворотной решетки

Записав текст из таблицы в одну строку, получим криптограмму «анфаарноишуиокви».

Получатель должен знать трафарет и наложить его в той же последовательности, что и при шифровании.

Решетки Кардано, также как и шифрующие таблицы, являются частными случаями шифра маршрутной перестановки.

Задание

Создать свой трафарет для поворотной решетки размером 6×6. Зашифровать текст с помощью созданного трафарета. Расшифровать криптограмму, полученную с помощью поворотной решетки, если известен использованный для шифрования трафарет.

Указания к выполнению практической работы

Для выполнения практической работы рекомендуется использовать файл *Решетка.docx*, содержащий пустую заготовку поворотной решетки.

Технология выполнения задания

Задание 1. Придумать секретное сообщение.Создать трафарет (поворотную решетку Кардано) размером 6×6 ячеек для шифрования секретного сообщения.

1. Придумать и записать осмысленный текст, состоящий из 36 букв, не считая пробелов и знаков препинания. Для подсчета числа букв в выделенном тексте MSWordможно использовать инструмент **Рецензирование/Статистика** .

Пример секретного сообщения (36 букв): «сегодня вечером жду в нашем месте с пакетом».

2. Открыть файл *решетка.docx*, содержащий заготовку трафарета.
3. Пронумеровать ячейки крайнего ряда решетки на каждой из сторон (пример – на рис.3), для этого:

- отступить с одной из сторон на одну ячейку;
- ввести номера (от 1 до 5) по часовой стрелке в области заголовка.

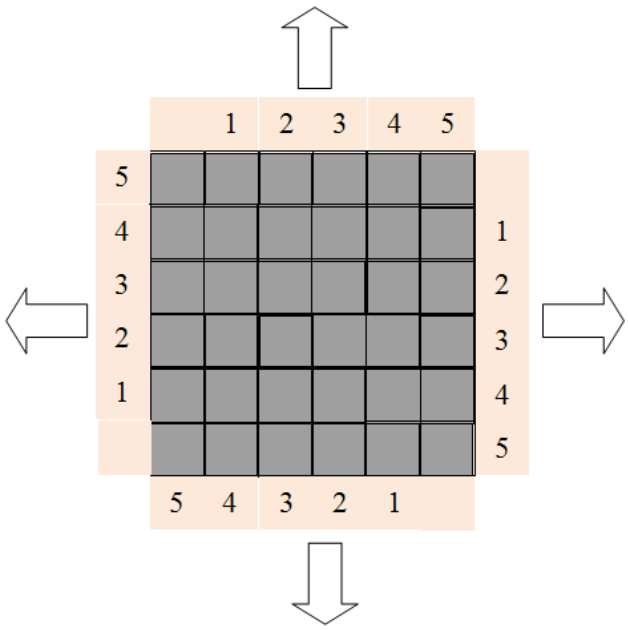


Рис. 3. Пример нумерации ячеек решетки: 1 этап.

4. «Открыть» ячейки трафарета в крайнем ряду, руководствуясь следующими правилами (пример – на рис.4):
   - на разных сторонах не должно быть открытых ячеек с одинаковым номером;
   - не желательно наличие нескольких подряд идущих «открытых» ячеек.

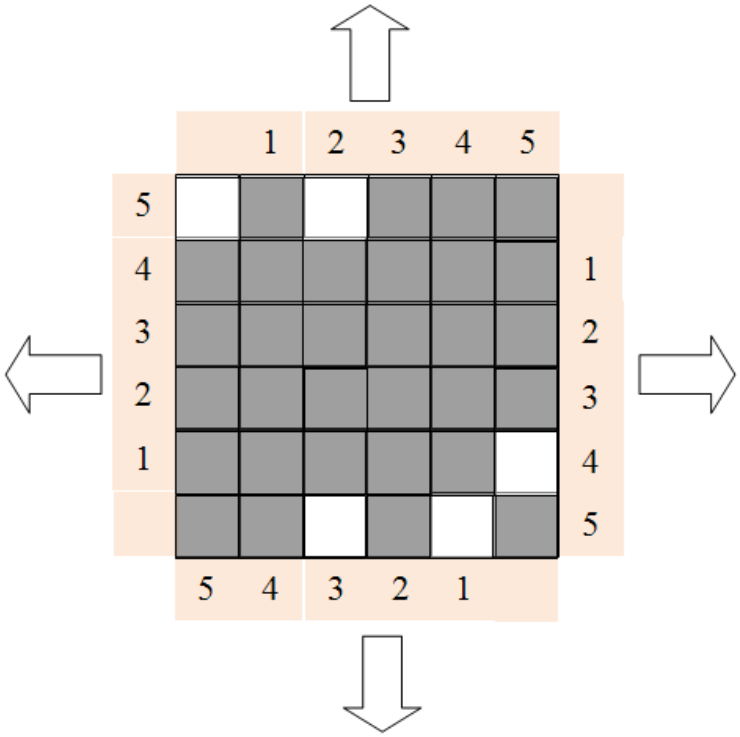


Рис.4. Пример трафарета: 1 этап (только крайний ряд).

Для «открытия» ячейки следует:

- Поместить решетку на передний план, для чего выделить решетку, щелкнув мышью в области одной из стрелок, а затем выполнить команду **Формат/На передний план**.
- Щелкнуть на границе ячейки мышью так, чтобы она выделилась «точками» по краям (рис.5) (при этом должна быть выделена и вся решетка целиком со стрелками).
- Затем щелкнуть на границе этой же ячейки правой кнопкой мыши и выбрать из контекстного меню команду **Формат автофигуры**.

- В окне команды на вкладке *Цвета и линии* в группе *цвет* изменить темно-серый цвет заливки на белый (новый цвет выбирается в выпадающем списке).

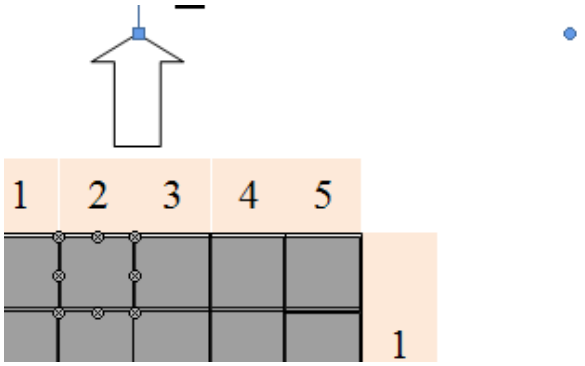


Рис. 5. Выделение ячейки решетки

5. Пронумеровать ячейки второго от края ряда решетки (от 1 до 3), отступив на две ячейки с одной из сторон и на одну ячейку – с другой (рис.6).

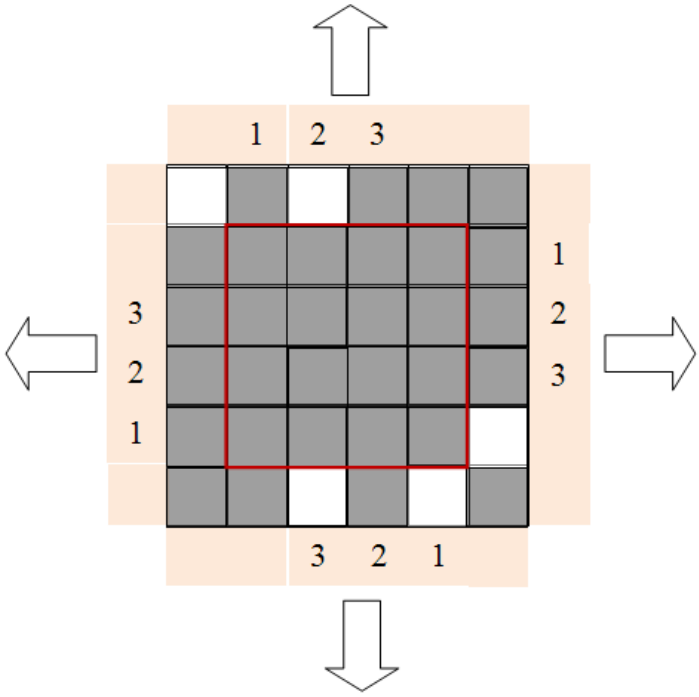


Рис. 6. Пример нумерации ячеек: 2 этап.

6. «Открыть» ячейки трафарета во втором от края ряду, руководствуясь приведенными выше правилами (пример – на рис. 7).

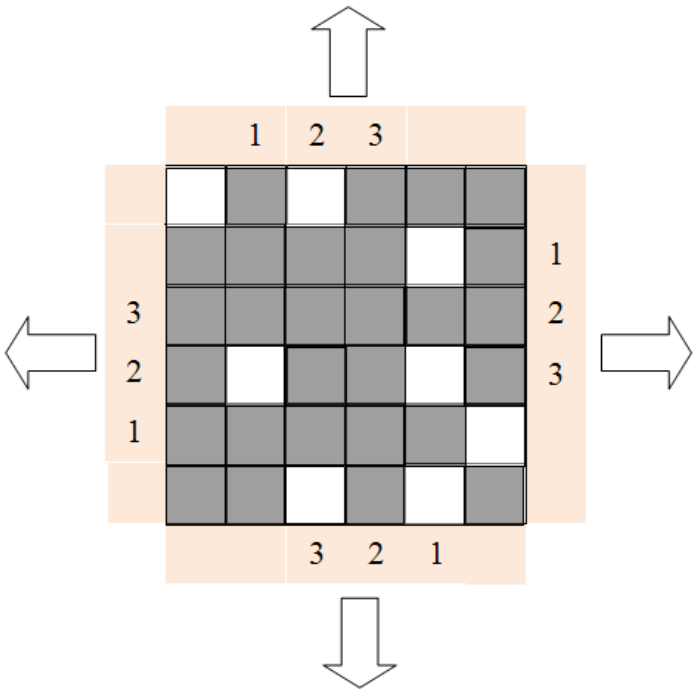


Рис. 7. Пример трафарета: 2 этап (крайний и второй с края ряды).

7. «Открыть» одну из ячеек внутреннего ряда (например, рис. 8).

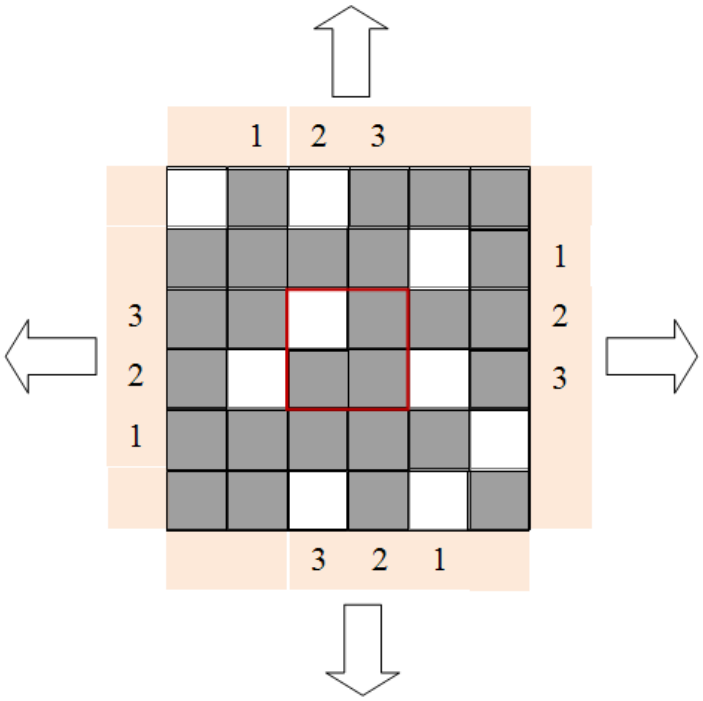


Рис. 8. Пример трафарета: 3 этап.

8. Повернуть (один или несколько раз) трафарет в любом направлении (по часовой или против часовой стрелки), для этого:

- Щелкнуть мышью в области верхней стрелки. Над стрелкой должна отобразиться зеленая точка.
- Навести на точку указатель мыши, чтобы он принял вид круговой стрелки, захватите точку мышью и, не отпуская, поверните в нужное положение.
- Если зеленая точка не отображается, следует щелкнуть в области стрелки мышью и выполнить команду **Формат/Повернуть вправо на 90°** (**Повернуть влево на 90°**) нужное количество раз.

Задание 2. Зашифровать секретное сообщение с помощью созданного трафарета.

9. Занести текст секретного сообщения в ячейки решетки, используя трафарет, для этого:

- Занести буквы текста последовательно (без пробелов и знаков препинания) в «открытые» ячейки решетки в направлении слева – направо и сверху – вниз (например, рис.9).

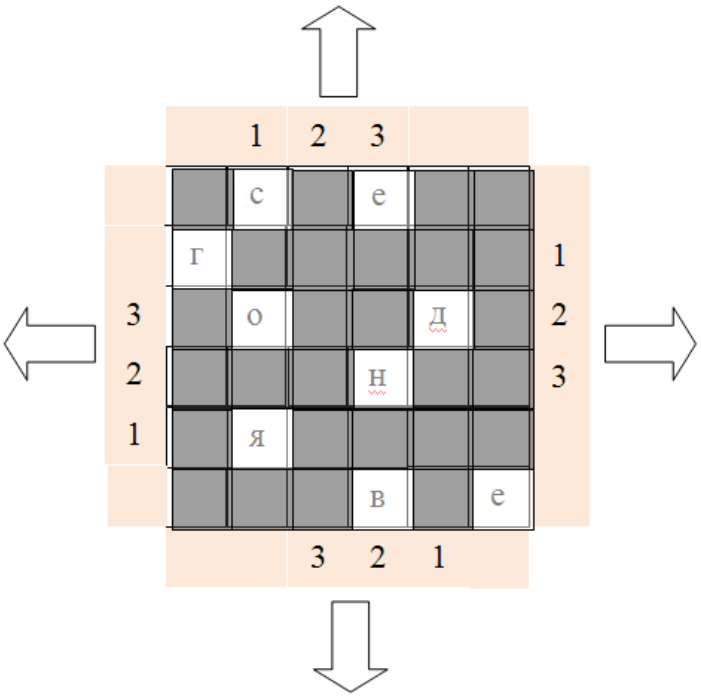


Рис. 9. Пример шифрования с использованием решетки

- Выбрать и запомнить направление поворота (влево или вправо) – далее поворот всегда будет осуществляться в одном направлении.

- После заполнения всех «открытых» ячеек повернуть трафарет на 90° в выбранном направлении.
- Повторять шаги по заполнению ячеек решетки, пока все ячейки не будут заполнены текстом. Если трафарет разработан правильно – всегда будут открываться только чистые (незаполненные ранее ячейки решетки).

10. Если текст в ячейках имеет различие в форматировании (например, центрированный и не центрированный), следует задать единый формат.
11. Повернуть трафарет один или несколько раз, чтобы усложнить выяснение его начального положения (важно, чтобы положение трафарета не совпадало с начальным!).

Задание 3. Расшифровать сообщение.

12. Обменяться зашифрованными сообщениями и расшифровать чужую криптограмму.В шифре с готовым трафаретом подобрать:
    - начальное положение трафарета,
    - направление поворота трафарета –

    таким образом, чтобы текст секретного сообщения можно было прочитать (чтение осуществляется так же, как и запись: слева – направо и сверху – вниз).
13. Записать расшифрованное сообщение.
14. Показать свое секретное сообщение, шифр (с трафаретом) и расшифровку чужого сообщения преподавателю.

Практическая работа №2. Криптоанализ шифров перестановки

Описание шифра и рекомендации покриптоанализу

В шифрах табличной перестановки криптограмма может быть получена разными способами. Для открытого текста длиной Nподбирается таблица размером $m \times n$, $m \times n \geq N$, символы текста записывается в ячейки таблицы. Запись может производиться как построчно, так и в столбец. В простейшем варианте текст из таблицы считывается в направлении, отличном от записи (например, по столбцам, если записывался по строкам).

Пример:

Запишем фразу «ТЕРМИНАТОР ПРИБЫВАЕТ СЕДЬМОГО В ПОЛНОЧЬ» в таблицу размером 5 × 7 по строкам (рис.10).

Выписав текст из таблицы по столбцам получим шифр: «ТНПВЕГЛЕАРАДОНРТИЕЬВОМОБТМПЧИРЫСООЬ».

	1	**2**	**3**	**4**	**5**
1	т	е	р	м	и
2	н	а	т	о	р
3	п	р	и	б	ы
4	в	а	е	т	с
5	е	д	ь	м	о
6	г	о	в	п	о
7	л	н	о	ч	ь

Рис.10. Пример шифрующей таблицы

Перед считыванием текста возможна перестановка строк, столбцов таблицы, либо совместная перестановка строк и столбцов (двойная перестановка). Порядок считывания текста в этом случае может и не меняться.

Пример: В таблице на рис.1 переставим столбцы в порядке: 4–3–5–1–2 (рис.11), а порядок считывания текста оставим тот же, что и порядок записи (по столбцам).

	4	**3**	**5**	**1**	**2**
1	м	р	и	т	е
2	о	т	р	н	а
3	б	и	ы	п	р
4	т	е	с	в	а
5	м	ь	о	е	д
6	п	в	о	г	о
7	ч	о	ь	л	н

Рис. 11. Пример шифрующей таблицы с перестановкой столбцов

Выписав текст из таблицы получим криптограмму: «МРИТЕОТРНАБИЫПРТЕСВАМЬОЕДПВОГОЧОЬЛН».

При решении задачи криптоанализа шифров перестановки необходимо восстановить начальный порядок следования букв текста.

Таким образом, в нашем примере при анализе криптограммы необходимо произвести действия, обратные шифрованию, то есть:

- записать текст криптограммы в таблицу в порядке ее считывания при шифровании;
- переставить строки, чтобы они следовали в исходном порядке;
- считать текст из таблицы в порядке его записи при шифровании.

Появления букв в открытом тексте нельзя считать независимыми друг от друга. Для восстановления исходного порядка символов текста используется анализ их совместимости, в чем может помочь таблицы сочетаемости символов, а также таблица вероятностей (частот) появления двухбуквенных сочетаний (биграмм) в текстах естественного языка.

Таблица сочетаемости букв (табл.1) содержит перечень букв, которые могут предшествовать, то есть находиться слева, и следовать, то есть находиться справа, от выбранной буквы. Вероятность предшествования и следования для гласных (Г) и согласных (С) неодинакова, она также указана в таблице (в процентах).

Вопрос о зависимости букв алфавита в открытом тексте от предыдущих букв исследовался известным русским математиком А.А.Марковым. Он показал, что появление букв в тексте естественного языка зависитне только от одной, но от значительного числа предшествующих букв. К.Шенноном было показано, что такая зависимость ощутима на глубину до 30 знаков, после чего она практически не ощущается. Однако для учебных целей достаточно ограничится анализом двухбуквенных сочетаний (биграмм).А.А.Марковым отмечена еще одна устойчивая закономерность открытых текстов, связанная с чередованием гласных и согласных букв. Частоты встречаемости гласных/согласных букв в зависимости от предыдущей гласной/согласной приведены в табл.2.

Таблица 1

Сочетаемость букв русского языка

Г	*С*	*Слева*	*Буква*	*Справа*	*Г*	*С*
3	97	л, д, к, т, в, р, н	**А**	л, н, с, т, р, в, к, м	12	88
80	20	я, е, у, и, а, о	**Б**	о, ы, е, а, р, у	81	19
68	32	я, т, а, е, и, о	**В**	о, а, и, ы, с, н, л, р	60	40
78	22	р, у, а, и, е, о	**Г**	о, а, р, л, и, в	69	31
72	28	р, я, у, а, и, е, о	**Д**	е, а, и, о, н, у, р, в	68	32
19	81	м, и, л, д, т, р, н	**Е**	н, т, р, с, л, в, м, и	12	88
83	17	р, е, и, а, у, о	**Ж**	е, и, д, а, н	71	29
89	11	о, е, а, и	**З**	а, н, в, о, м, д	51	49
27	73	р, т, м, и, о, л, н	**И**	с, н, в, и, е, м, к, з	25	75
55	45	ь, в, е, о, а, и, с	**К**	о, а, и, р, у, т, л, е	73	27
77	23	г, в, ы, и, е, о, а	**Л**	и, е, о, а, ь, я, ю, у	75	25
80	20	я, ы, а, и, е, о	**М**	и, е, о, у, а, н, п, ы	73	27
55	45	д, ь, н, о, а, и, е	**Н**	о, а, и, е, ы, н, у	80	20
11	89	р, п, к, в, т, н	**О**	в, с, т, р, и, д, н, м	15	85
65	35	в, с, у, а, и, е, о	**П**	о, р, е, а, у, и, л	68	32
55	45	и, к, т, а, п, о, е	**Р**	а, е, о, и, у, я ,ы, н	80	20
69	31	с, т, в, а, е, и, о	**С**	т, к, о, я, е, ь, с, н	32	68
57	43	ч, у, и, а, е, о, с	**Т**	о, а, е, и, ь, в, р, с	63	37
15	85	п, т, к, д, н, м, р	**У**	т, п, с, д, н, ю, ж	16	84
70	30	н, а, е, о, и	**Ф**	и, е, о, а, е, о, а	81	19
90	10	у, е, о, а, ы, и	**Х**	о, и, с, н, в, п, р	43	57
69	31	е, ю, н, а, и	**Ц**	и, е, а, ы	93	7
82	18	е, а, у, и, о	**Ч**	е, и, т, н	66	34
67	33	ь, у, ы, е, о, а, и, в	**Ш**	е, и, н, а, о, л	68	32
84	16	е, б, а, я, ю	**Щ**	е, и, а	97	3
0	100	м, р, т, с, б, в, н	**Ы**	л, х, е, м, и, в, с, н	56	44
0	100	н, с, т, л	**Ь**	н, к, в, п, с, е, о, и	24	76
14	86	с, ы, м, л, д, т, р, н	**Э**	н, т, р, с, к	0	100
58	42	ь, о, а, и, л, у	**Ю**	д, т, щ, ц, н, п	11	89
43	57	о, н, р, л, а, и, с	**Я**	в, с, т, п, д, к, м, л	16	84

Таблица 2

Чередование гласных и согласных

	Г	**С**	**Всего**
Г	6588	38310	44898
С	38296	16806	55102

Таблица 3. **Частоты биграмм русского языка**

	А	Б	В	Г	Д	Е	Ж	З	И	Й	К	Л	М	Н	О	П	Р	С	Т	У	Ф	Х	Ц	Ч	Ш	Щ	Ы	Ь	Э	Ю	Я	-
А	2	12	35	8	14	7	6	15	7	7	19	27	19	45	3	11	26	31	27	3	1	10	6	7	10	1			2	6	9	146
Б	5					9	1		6			6		2	21		8	1		6						1	11				2	3
В	35	1	5	3	3	32		2	17		7	10	3	9	58	6	6	19	6	7		1	1	2	4	1	18	1	2		3	61
Г	7				3	3			5		1	5		1	50		7			2												7
Д	25		3	1	1	29	1	1	13		1	5	1	13	22	3	6	8	1	10			1	1	1		5	1			1	11
Е	2	9	18	11	27	7	5	10	6	15	13	35	24	63	7	16	39	37	33	3	1	8	3	7	3	3			1	1	2	138
Ж	5	1			6	12			5					6				1														2
З	35	1	7	1	5	3			4		2	1	2	9	9	1	3	1		2							4				4	12
И	4	6	22	5	10	21	2	23	19	11	19	21	20	32	8	13	11	29	29	3	1	17	3	11	1	1			1	3	17	134
Й	1	1	4	1	3		1	2	4		5	1	2	7	9	7	3	10	2				1	3	2							65
К	24	1	4	1		4	1	1	26		1	4	1	2	66	2	10	3	7	10			1									36
Л	25	1	1	1	1	33	2	1	36		1	2	1	8	30	2		3	1	6		4		1			2	30		4	9	49
М	18	2	4	1	1	21	1	2	23		3	1	3	7	19	5	2	5	3	9	1			2			5	1	1		3	60
Н	54	1	2	3	3	34			58		3		1	24	67	2	1	9	9	7	1		5	2			36	3			5	28
О	1	28	84	32	47	15	1	18	12	29	19	41	38	30	9	18	43	50	39	3	2	5	2	12	4	3			2	3	2	161
П	7					15			4			9		1	46		41	1		6							2				2	1
Р	55	1	4	4	3	37	3	1	24		3	1	3	7	56	2	1	5	9	16		1	1	1	2		8	3			5	11
С	8	1	7	1	2	25			6		40	13	3	9	27	11	4	11	82	6		1	1	2	2		1	8			17	27
Т	35	1	27	1	3	31		1	28		5	1	1	11	56	4	26	18	2	10				1			11	21			4	64
У	1	4	4	4	11	2	6	3	2		8	5	5	5	1	5	7	14	7			1		8	3	2				9	1	51
Ф	2					2			2						1		1	1														1
Х	4	1	4	1	3	1		2	3		4	3	3	4	18	5	3	4	2	2	1			1								27
Ц	3					7			10		2				1					1							1					3
Ч	12					23			13		2			6					7	1					1			1				3
Ш	5					11			14		1	2		2	2					1								1				1
Щ	3					8			6					1						1												
Ы		1	9	1	3	12		2	4	7	3	6	6	3	2	10	3	9	4	1		16		1	2							43
Ь		2	4	1	1	2		2	2		6		3	13	2	4	1	11	3					1	4				1	3	1	78
Э											1				1			1	9													
Ю		2	1	2	1			3	1		1		1	1	1	3	1	1	7				1	1		4						26
Я	1	3	9	1	3	3	1	5	3	2	3	3	4	6	3	6	3	6	10			2	1	4	1	1			1	1	1	97
-	25	47	124	33	61	25	14	40	73		70	22	59	126	87	149	44	133	65	36	9	12	4	37	7	1			19	1	19	

Знание частот встречаемости пар букв (биграмм) позволяет легко вскрывать шифры табличной перестановки. Истинный порядок следования строк/столбцов в таблице можно восстановить, рассматривая и исключая маловероятные сочетания букв. Кроме того, на основе вероятностей появления биграмм можно рассчитать вероятность следования одной строки (столбца) за другой.

Пусть известно, что криптограмма была получена следующим образом: текст записан в таблицу построчно, осуществлена перестановка столбцов. Тогда, для того, чтобы оценить вероятность $p(i,j)$следования столбца jнепосредственно за столбцом i, надо для каждой строки рассмотреть сочетания символов из этих столбцов. Получим mвероятностей $p(e_{ki}, e_{kj})$биграмм, где m – число строк шифрующей таблицы, e_{ki}, e_{kj} – символы, стоящие в шифрующей таблице на пересечении kстроки и i, jстолбца соответственно.Окончательно имеем:

$$p(i, j) = \prod_{k=1}^{m} p(e_{ki}, e_{kj})$$

Пользуясь этой формулой, можно вычислить вероятности следования друг за другом всех возможных пар столбцов $p(i,j), i \neq j: i,j=1,\ldots,n$, n– число столбцовшифрующей таблицы.Если в исходном тексте jстолбец действительно стоит после i-того, то вероятность $p(i,j)$должна быть, в принципе, больше вероятностей $p(i,k)$, $k \neq j$ и $p(k,j)$, $k \neq i$.Руководствуясь этими соображениями, для таблиц небольшого размера можно не сложно восстановить истинный порядок следования столбцов.

Если текст в шифрующую таблицу записывался в столбец, и переставлялись строки, то интерес представляют символы, составляющие фрагмент осмысленного текста, то есть символы e_{ik}, e_{jk} двух строк одного столбца. Вероятность следования jстроки непосредственно за iстрокой в этом случае вычисляется как:

$$p(i, j) = \prod_{k=1}^{n} p(e_{ik}, e_{jk})$$

Если известны не вероятности, а частоты появления биграмм (как, например, в табл.3), можно рассчитать аналогичную статистику для частот.

При проведении криптоанализа двойных перестановок (переставляются и строки, и столбцы шифрующей таблицы) важно, каким образом записывался открытый текст в шифрующую таблицу:

- Если текст записывался построчно, то сначала надо восстановить истинный порядок следования столбцов, затем – строк.
- Если же открытый текст записывался в шифрующую таблицу в столбец, то сначала следует переставлять строки, затем – столбцы.

При этом сама последовательность перестановок (что сначала переставлялось – столбцы или строки) оказывается неважна.

Задание

Дешифровать криптограммы, полученные методами столбцовой и двойной перестановки.

Указания к выполнению практической работы

Для выполнения практической работы рекомендуется использовать файлы *Перестановка.xlsx* и *Двойная перестановка.xlsx*, реализующие расчет статистик на основе данных о частотах биграмм.

Технология выполнения задания

Задание1. Дешифровать криптограмму, полученную методом столбцовой перестановки. Известно, что текст записывался в шифрующую таблицу и считывался построчно, знаки пробела в тексте сохранены.

1. Выбрать текст криптограммы в соответствии с номером варианта (табл.4).

   Выполнить анализ криптограммы аналогично рассмотренному далее примеру.

   Пример: Известно, что в шифрующей таблице произведена перестановкастолбцов, текст записывался и выписывался из шифрующей таблицы построчно. Известно также, что при шифровании пробелы между словами сохранены (символ «_»).

Необходимо дешифровать криптограмму «СВПООЗ-ЛУЙЬСТЬ_ЕДПСКОКАОЙЗ».

Таблица 4

Варианты задания

1.	ОКЕСНВРП_ЫРЕАДЕЫН_В_РСИКО
2.	ДСЛИЕЗТЕА_Д_ЛЬЮВМИ_ _АОЧХК
3.	НМВИАИ_НЕВЕ_СМСТУОРДИАНКМ
4.	ЕДСЗЬНДЕ_МУБД_УЭ_КТЗЕМНАЫ
5.	СОНРЧОУО_ХДТ_ИЕИ_ВЗКАТРРИ
6.	_ОНКА_БНЫЕЦВЛЕ_К_ТГОАНЕИР
7.	НЗМАЕЕАА_Г_НОТВОССОТЬЯАЛС
8.	РППОЕААДТВЛ_ЕБЬЛНЫЕ_ПА_ВР
9.	ОПЗДЕП_ИХРДОТ_И_ВРИТЧ_САА
10.	ВКЫОСИРЙУ_ОЬВНЕ_СОАПНИОТС
11.	ПКТИРАОЛНАОИЧ_З_ЕСЬНЕЛНЖО
12.	ИПКСОЕ_ТСМНАЧИ_ОЕН_ГДЕЛА_
13.	АМВИННЬТЛЕАНЕ_ЙОВ_ОПХАРТО
14.	АРЫКЗЫ_КЙТНЛ_ААЫ_ОЛБКЫТРТ
15.	_ПАРИИВИАРЗ_БРА_ИСТЬЛТОЕК
16.	А_ЛНПАУВКЭИ_ЦИАКР_ОВОЕДРИ
17.	ЖВНОАН_АТЗОЬСН_ЫО_ФВИИКИЗ
18.	ОТВГОСЕЬЬТАДВ_С_ЬЗАТТЕЫАЧ
19.	ЯАМРИТ_ДЖЕХ_СВЕД_ТСУВЕТНО
20.	УЬБДТ_ОЕГТВ_ОЫКЭА_ВКАИУЦИ
21.	ЛТБЕИЛЖЫЕ_ _ОАПТЖРДУ_ЛМНОА
22.	ИПТКРРАФОГ_ВАИЯАЯ_ЖНУКАНА
23.	ПКЕЕРРПО_ЙУОТ_ИТПСУТЛЯЕИН
24.	ИЬЖЗНСД_ТУН_ЕТАНУВЕ_РЫГОЗ
25.	ЕОУРВА_НЬРИАДИЦЕПИ_РНШВЫЕ

2. Длина криптограммы– 25 символов, поэтому предположим, что она была записана с помощью таблицы 5×5. Для дальнейшего выполнения задания рекомендуется воспользоваться файлом *Перестановка.xlsx*, реализующим расчет статистик для оценки порядка следования столбцов.

3. Запишем символы криптограммы построчно в шифрующую таблицу 5×5 (лист *Криптограмма*) – рис. 12.

с	в	п	о	о
з	л	у	й	ь
с	т	ь	_	е
д	п	с	к	о
к	а	о	й	з

Рис. 12. Криптограмма, занесенная в шифрующую таблицу

4. Изучить таблицу статистик на листе *Криптограмма* и высказать гипотезу о порядке следования столбцов шифрующей таблицы:

- В таблице *Статистика (тыс) – порядок столбцов* на листе *Криптограмма* приведены значения получаемых для столбцов статистик.
- На листе *Частоты по столбцам* приведены частоты двухбуквенных сочетаний и расчет статистик для соответствующих столбцов. Например, для последовательно следующих столбцов 1 и 2 (1-2) имеем двухбуквенные сочетания: св, зл, ст, дп, ка, которым соответствуют частоты 7, 1, 82, 3, 24. Результирующее значение статистики 41 328.
- Для облегчения визуального анализа на листе *Криптограмма* отображается значение статистики в тысячах (/1000), то есть 41 (рис. 13).

	1	2	3	4	5
1	--	41	93	0	0
2	0	--	2	0	37 219
3	1	0	--	0	0
4	0	11	0	--	0
5	348	0	0	0	--

Рис. 13. Статистика криптограммы

Для оценки возможности того, что столбец стоит на первом/последнем месте в шифрующей таблице могут быть использованы частоты биграмм вида «_е» и «е_», где е – символ столбца, стоящий соответственно на пересечении первой или последней строки (лист *Частоты биграмм*).

Из анализа значений статистик для примера имеем наиболее вероятные последовательности столбцов: 1-3, 2-5, 5-1 и более слабые 1-2, 4-2, 3-1.Предположения о порядке следования столбцов можно указывать в области *Примечания* на листе *Криптограмма*.

На первом месте скорее всего стоят 3, 1 или 2 столбцы, а на последнем – 3 или 2.

- Посмотрим на символы, стоящие в третьей строке: «сть_е». Скорее всего, мягкий знак стоит в конце слова. Поэтому предположим, что столбец 4 следует за столбцом 3. Учитывая результаты, полученные в предыдущем пункте, предположим следующий порядок столбцов: 3-4-2-5-1.

5. Задать новый порядок следования столбцов, изменяя **только номера** (выделены красным шрифтом) столбцов таблицы *Перестановка столбцов - новый порядок* на листе *Криптограмма*.

В примере будет получена новая таблица, однако текст остается не читаемым (рис. 14):

3	**4**	**2**	**5**	**1**
п	о	в	о	с
у	й	л	ь	з
ь	_	т	е	с
с	к	п	о	д
о	й	а	з	к

Рис. 14. Новый порядок следования столбцов

В этом случае следует высказать новую гипотезу о порядке следования столбцов, используя анализ получаемого текста.

- Снова обратим внимание на третью строку. Значение частот биграмм «ТЕ» - 31, «СЕ» - 25, «ЕС» - 37, «ЕТ» - 33. Скорее всего, «ь» стоит после сочетания «тес» и представляет окончание глагола «тесь». Переставим в конец столбцы с символами «ь» и «_», сохранив их порядок, то есть зададим новую последовательность столбцов 2-5-1-3-4.

Теперь текст в таблице читается, это «ВОСПОЛЬЗУЙТЕСЬ ПОДСКАЗКОЙ».

6. После расшифрования текста показать его преподавателю.

Задание 2. Дешифровать криптограмму, полученную методом двойной перестановки. Известно, что текст записывался в шифрующую таблицу и считывался построчно, знаки пробела в тексте сохранены.

7. Выбрать текст криптограммы в соответствии с номером варианта (табл.5).Выполнить анализ криптограммы аналогично рассмотренному далее примеру.

Таблица 5

Варианты задания

1.	СЯСЕ_ _ЛУНЫИАККННОГЯДУЧАТН
2.	МСЕЫ_ЛЫВЕНТОСАНТУЕИ_РЛПОБ
3.	АМНРИД_УЕБСЫ_ЕЙРСООКОТНВ_
4.	ОПЧУЛС_БООНЕВ_ОЖАЕОНЕЩЕИН
5.	ЕШИАНИРЛПГЕЧАВРВ_СЕЫНА_ЛО
6.	АРАВНРСВЕЕОАВ_ЗАНЯА_КМРЕИ
7.	А_ЛТАВЙООЛСО_ТВ_ШЕЕНЕСТ_Ь
8.	ФИ_ЗИММУЫНУУКБ_Е_ДЬШЫИВЧУ
9.	ВР_ЕСДЕИ_ТПХРОИ_ЗБУАДНУА_
10.	ЩТААЙПЕЕ_ТБГУРРСВЬЕ_ОРЗВВ
11.	АВАРНСЧАА_НЕДВЕДЕРПЕОЙ_ИС
12.	ДОПК_СОПАЛЕИНЛ_ГИНЙОИЖЕ_Т
13.	ЛУАЗИЯНСА_ДТДЕАИ_ШРФЕОНП_
14.	С_ОЯНВ_СЬСЛААВРЧЕАРТОГДЕС
15.	ЗШАФИПРАЛОЕНЖ_ОЬН_ДАРВОНА
16.	КЭЕ_ТДУМБ_ЬСЗЕДНЕЗМАОР_ТУ
17.	_ЕАЛЯРАНВЯАЧДА_ЕРПЕСАНВ_Ч
18.	_И_ЕНТРЗИ_ОКЕВНОДЛЕША_ИМР
19.	РОБДОЕВПС_МСХЬА_ _ИВПСНИОТ
20.	ЕСДНОГТЕАНН_НЕОВМР_ЕУНПТЕ
21.	_ЙЕСТОВО_НИИНЛАЕТИЖДСОПВ_
22.	НДИАЕОЫЛПНЕ_ _НВЕАНГТ_ИЗЛА
23.	П_БИРДЛЬНЕВ_ОП_ОПЗДЕВЫГЕА
24.	МДООИТЕЬ_СМТ_НАДТЕСУБЕХНО
25.	АИНАЛЖНОЛЕШФ_ЗИ_УАРОЬСНЕ_

Пример: Известно, что использован шифр двойной перестановки, текст записывался в шифрующую таблицу построчно. Дешифровать криптограмму «ЫОЕЧ-ТТОУ_СНСОРЧТРНАИДЬН_Е».

8. Текст содержит 25 символов, что позволяет записать его в квадратную таблицу 5×5. Поскольку известно, что запись велась построчно, сначала следует восстановить порядок следования столбцов, а затем – строк. Для выполнения задания рекомендуется воспользоваться книгой *Двойная перестановка.xslx*, содержащей расчет статистик.
9. Запишем криптограмму построчно в таблицу (лист *Криптограмма*) – рис. 15.

ы	о	е	ч	т
т	о	у	_	с
н	с	о	р	ч
т	р	н	а	и
д	ь	н	_	е

Рис. 15. Исходная криптограмма в шифрующей таблице

10. Провести анализ статистик на листе *Криптограмма* и высказать гипотезу о порядке следования столбцов.

- Анализ статистик показывает, что наиболее вероятны следующие последовательности столбцов: 1-3, 2-4, 3-5, 4-3, 5-1.
- Проверка на первый последний столбец не проводится, так как порядок строк также изменен.
- Предположим следующую последовательность следования столбцов: 2-4-3-5-1.

11. Переставим столбцы в указанном порядке, меняя **номера столбцов** таблицы *Перестановка столбцов – новый порядок* (выделены красным) – рис. 16.

- Полученный порядок столбцов, скорее всего, правильный, так как в строках таблицы получили вполне читаемые фрагменты текста «очеты», «срочн», «ранит».

	2	4	3	5	1
1	о	ч	е	т	ы
2	о	_	у	с	т
3	с	р	о	ч	н
4	р	а	н	и	т
5	ь	_	н	е	д

Рис. 16. Криптограмма, записанная с учетом нового порядка следования столбцов

12. Высказать гипотезу о порядке следования строк.

- Фрагмент «срочн» составляет, скорее всего, слово «срочно», таким образом, после 3 строки должна следовать 1 или 2 строка. После строки с фрагментом «ранит», скорее всего, идет строка, начинающаяся с мягкого знака – «ранить» (4-5).
- На основании проверки строк на первую/последнюю (таблица *Частота биграмм – порядок строк*) предположим, что 3 строка идет первой. Тогда порядок строк очевиден: 3-2-4-5-1.

13. Осуществить перестановку строк, задав новые **номера строк** в таблице *Перестановка строк – новый порядок* (выделены красным).

Получен читаемый текст: «СРОЧНО_УСТРАНИТЬ_НЕДОЧЕТЫ».

14. После расшифрования текста показать его преподавателю.

Практическая работа № 3. Изучение шифров простой и многоалфавитной замены (шифр Цезаря и шифр Виженера)

Описание шифров

Шифр простой (одноалфавитной) замены заключается в замене символов алфавита исходного сообщения на новые. При этомодин и тот же символ открытого сообщения всегда одним и тем же символом криптограммы. Соответствие между символами алфавита исходного текста и символами алфавита криптограммы может задаваться с помощью таблицы или формулы. Заданное соответствие не меняется на всем протяжении шифрования.

Набор различных символов исходных сообщений называется *нормативным алфавитом*, а соответствующий им набор символов криптограмм – *шифралфавитом* (*алфавитом шифрования*).

Простейшим примером такого шифра является шифр Цезаря, в котором алфавит шифрования получается путем циклического сдвига влево исходного нормативного алфавита на Sпозиций (рис.17).

порядковый № символа	0	1	2	3	4		22	23	24	25
алфавит исходного текста	**a**	**b**	**c**	**d**	**e**		**w**	**x**	**y**	**z**
	↓	↓	↓	↓	↓	…	↓	↓	↓	↓
алфавит шифра	**d**	**e**	**f**	**g**	**h**		**z**	**a**	**b**	**c**
порядковый № символа	3	4	5	6	7		25	0	1	2

Рис. 17. Пример шифра Цезаря

Пронумеровав буквы алфавита, начиная с нуля, получим математическое описание этого шифра:

$c_i = (a_i + S) \bmod L$,

гдеa_i, c_i – i-тыйэлемент открытого текста и шифртекста соответственно, L – мощность (количество различных символов) нормативного алфавита, S– сдвиг, одинаковый для всех символов, $0 \le S \le L$-1. При S=0 алфавит шифрования совпадает с нормативным.

Многоалфавитные шифры используют не один, а целый набор алфавитов шифрования, примером многоалфавитной замены является шифр Виженера.

Шифрование осуществляется по таблице, представляющей собой квадратную матрицу размерностью $L \times L$, где L–мощность (число различных символов) используемого алфавита. Первая строка содержит все символы нормативного алфавита в обычном порядке. Каждая следующая строка получается из предыдущей циклическим сдвигом на один символ влево.

На рис. 18 показана таблица Виженера для русского языка (алфавит без буквы «Ё», содержит пробел). В таблице выделены

строки – алфавиты шифрования, используемые, если выбрано ключевое слово «МАЯК».

	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31	32
0	а	б	в	г	д	е	ж	з	и	й	к	л	м	н	о	п	р	с	т	у	ф	х	ц	ч	ш	щ	ъ	ы	ь	э	ю	я	-
1	б	в	г	д	е	ж	з	и	й	к	л	м	н	о	п	р	с	т	у	ф	х	ц	ч	ш	щ	ъ	ы	ь	э	ю	я	-	а
2	в	г	д	е	ж	з	и	й	к	л	м	н	о	п	р	с	т	у	ф	х	ц	ч	ш	щ	ъ	ы	ь	э	ю	я	-	а	б
3	г	д	е	ж	з	и	й	к	л	м	н	о	п	р	с	т	у	ф	х	ц	ч	ш	щ	ъ	ы	ь	э	ю	я	-	а	б	в
4	д	е	ж	з	и	й	к	л	м	н	о	п	р	с	т	у	ф	х	ц	ч	ш	щ	ъ	ы	ь	э	ю	я	-	а	б	в	г
5	е	ж	з	и	й	к	л	м	н	о	п	р	с	т	у	ф	х	ц	ч	ш	щ	ъ	ы	ь	э	ю	я	-	а	б	в	г	д
6	ж	з	и	й	к	л	м	н	о	п	р	с	т	у	ф	х	ц	ч	ш	щ	ъ	ы	ь	э	ю	я	-	а	б	в	г	д	е
7	з	и	й	к	л	м	н	о	п	р	с	т	у	ф	х	ц	ч	ш	щ	ъ	ы	ь	э	ю	я	-	а	б	в	г	д	е	ж
8	и	й	к	л	м	н	о	п	р	с	т	у	ф	х	ц	ч	ш	щ	ъ	ы	ь	э	ю	я	-	а	б	в	г	д	е	ж	з
9	й	к	л	м	н	о	п	р	с	т	у	ф	х	ц	ч	ш	щ	ъ	ы	ь	э	ю	я	-	а	б	в	г	д	е	ж	з	и
10	к	л	м	н	о	п	р	с	т	у	ф	х	ц	ч	ш	щ	ъ	ы	ь	э	ю	я	-	а	б	в	г	д	е	ж	з	и	й
11	л	м	н	о	п	р	с	т	у	ф	х	ц	ч	ш	щ	ъ	ы	ь	э	ю	я	-	а	б	в	г	д	е	ж	з	и	й	к
12	м	н	о	п	р	с	т	у	ф	х	ц	ч	ш	щ	ъ	ы	ь	э	ю	я	-	а	б	в	г	д	е	ж	з	и	й	к	л
13	н	о	п	р	с	т	у	ф	х	ц	ч	ш	щ	ъ	ы	ь	э	ю	я	-	а	б	в	г	д	е	ж	з	и	й	к	л	м
14	о	п	р	с	т	у	ф	х	ц	ч	ш	щ	ъ	ы	ь	э	ю	я	-	а	б	в	г	д	е	ж	з	и	й	к	л	м	н
15	п	р	с	т	у	ф	х	ц	ч	ш	щ	ъ	ы	ь	э	ю	я	-	а	б	в	г	д	е	ж	з	и	й	к	л	м	н	о
16	р	с	т	у	ф	х	ц	ч	ш	щ	ъ	ы	ь	э	ю	я	-	а	б	в	г	д	е	ж	з	и	й	к	л	м	н	о	п
17	с	т	у	ф	х	ц	ч	ш	щ	ъ	ы	ь	э	ю	я	-	а	б	в	г	д	е	ж	з	и	й	к	л	м	н	о	п	р
18	т	у	ф	х	ц	ч	ш	щ	ъ	ы	ь	э	ю	я	-	а	б	в	г	д	е	ж	з	и	й	к	л	м	н	о	п	р	с
19	у	ф	х	ц	ч	ш	щ	ъ	ы	ь	э	ю	я	-	а	б	в	г	д	е	ж	з	и	й	к	л	м	н	о	п	р	с	т
20	ф	х	ц	ч	ш	щ	ъ	ы	ь	э	ю	я	-	а	б	в	г	д	е	ж	з	и	й	к	л	м	н	о	п	р	с	т	у
21	х	ц	ч	ш	щ	ъ	ы	ь	э	ю	я	-	а	б	в	г	д	е	ж	з	и	й	к	л	м	н	о	п	р	с	т	у	ф
22	ц	ч	ш	щ	ъ	ы	ь	э	ю	я	-	а	б	в	г	д	е	ж	з	и	й	к	л	м	н	о	п	р	с	т	у	ф	х
23	ч	ш	щ	ъ	ы	ь	э	ю	я	-	а	б	в	г	д	е	ж	з	и	й	к	л	м	н	о	п	р	с	т	у	ф	х	ц
24	ш	щ	ъ	ы	ь	э	ю	я	-	а	б	в	г	д	е	ж	з	и	й	к	л	м	н	о	п	р	с	т	у	ф	х	ц	ч
25	щ	ъ	ы	ь	э	ю	я	-	а	б	в	г	д	е	ж	з	и	й	к	л	м	н	о	п	р	с	т	у	ф	х	ц	ч	ш
26	ъ	ы	ь	э	ю	я	-	а	б	в	г	д	е	ж	з	и	й	к	л	м	н	о	п	р	с	т	у	ф	х	ц	ч	ш	щ
27	ы	ь	э	ю	я	-	а	б	в	г	д	е	ж	з	и	й	к	л	м	н	о	п	р	с	т	у	ф	х	ц	ч	ш	щ	ъ
28	ь	э	ю	я	-	а	б	в	г	д	е	ж	з	и	й	к	л	м	н	о	п	р	с	т	у	ф	х	ц	ч	ш	щ	ъ	ы
29	э	ю	я	-	а	б	в	г	д	е	ж	з	и	й	к	л	м	н	о	п	р	с	т	у	ф	х	ц	ч	ш	щ	ъ	ы	ь
30	ю	я	-	а	б	в	г	д	е	ж	з	и	й	к	л	м	н	о	п	р	с	т	у	ф	х	ц	ч	ш	щ	ъ	ы	ь	э
31	я	-	а	б	в	г	д	е	ж	з	и	й	к	л	м	н	о	п	р	с	т	у	ф	х	ц	ч	ш	щ	ъ	ы	ь	э	ю
32	-	а	б	в	г	д	е	ж	з	и	й	к	л	м	н	о	п	р	с	т	у	ф	х	ц	ч	ш	щ	ъ	ы	ь	э	ю	я

Рис. 18. Пример таблицы Виженера

Далее выбирается ключ или ключевая фраза. После чего шифрование осуществляется следующим образом:

- под каждой буквой исходного сообщения последовательно записываются буквы ключа;
- если ключ оказался короче сообщения, его последовательно повторяют пока не будет достигнут конец сообщения;
- каждая буква шифртекста находится на пересечении столбца таблицы, определяемого буквой открытого текста, и строки, определяемой буквой ключа.

Пусть требуется зашифровать открытый текст «ГРУЗИТЕ АПЕЛЬСИНЫ БОЧКАМИ», выбрано ключевое слово «МАЯК» (рис. 19).

Открытый текст	Г Р У З И Т Е _ А П Е Л Ь С И Н Ы _ Б О Ч К А М И
Ключ	М А Я К М А Я К М А Я К М А Я К М А Я К М А Я К М
Криптограмма	П Р С С Ф Т Г Й М П Г Х З С Ж Ч Ж_ _ Ш В К Я Ц Ф

Рис. 19. Шифрование с помощью криптосистемы Виженера

В многоалфавитных шифрах один и тот же символ криптограммы может заменять разные символы открытого текста. Так, в рассмотренном примере буква «С» заменяет в разных случаях буквы «У», «З» и «С»; символ «_» – букву «Б» и символ «_».

Буквы ключа определяют величину смещения символов криптограммы относительно символов открытого текста. Таким образом,

$$c_i = (a_i + S_i) \bmod L,$$

где a_i, c_i – i-тыйэлемент открытого текста и шифр-текста соответственно, L – мощность (количество различных символов) нормативного алфавита, S_i– сдвиг, определяемый i-тым символом ключевой последовательности.Ключевая последовательность получается периодическим повторением ключевого слова. Например, ключевое слово «МАЯК» порождает последовательность вида «МАЯКМАЯКМАЯК…». S_i – числовой эквивалент соответствующей буквы ключа, $0 \le S_i \le L\text{-}1$.

Шифр Цезаря является частным случаем шифра Виженера с периодом ключевой последовательности, равным единице (ключ состоит из одной буквы).

Задание

Изучить процедуры шифрования и расшифрования в шифрах Цезаря и Виженера.

Указания к выполнению практической работы

Для выполнения практической работы рекомендуется использовать файлы *Алфавит.xlsx*, содержащий алфавит русского языка.

Технология выполнения задания

Задание 1. Зашифровать слово с помощью шифра Цезаря.

1. В приложении MSExcel открыть файл *Алфавит.xlsx* илисоздать книгу, содержащую пронумерованные символы русского алфавита: в первом столбце ввести номера от 0 до 32, во втором – символы алфавита по порядку, в третьем – снова нумерацию от 0 до 32. В книгу отформатировать (уменьшить) ширину столбцов для удобного введения в них текста побуквенно (рис. 20), для облегчения данной задачи можно использовать копирование форматов.

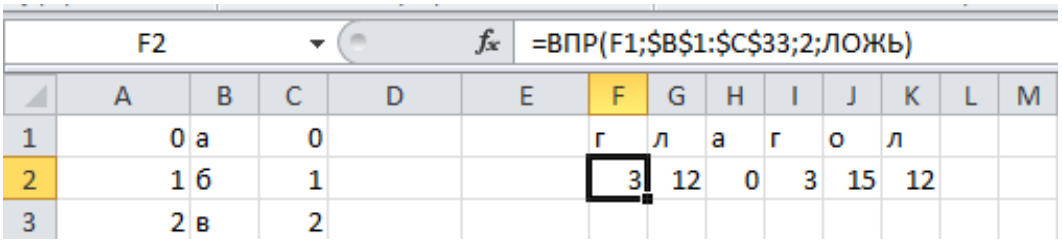
	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S
1	0	а	0																
2	1	б	1																
3	2	в	2																
4	3	г	3																
5	4	д	4																
6	5	е	5																
7	6	ё	6																
8	7	ж	7																
9	8	з	8																
10	9	и	9																
11	10	й	10																

Рис. 20. Пример содержания и форматирования книги «алфавит»

2. Выбрать значение ключа равным номеру варианта.
3. Зашифровать слово «семена» с помощью шифра Цезаря с выбранным ключом:

- ввести в ячейки первой строки отформатированной области побуквенно шифруемое слово, важно, чтобы символы алфавита в таблице и символы вводимого слова были набраны в одном регистре;
- строкой ниже получить числовой код символов шифруемого слова с помощью функции **ВПР**:
  - первым параметром (*Искомое_значение*) функции назначить ссылку на ячейку с текущим символом шифруемого слова,

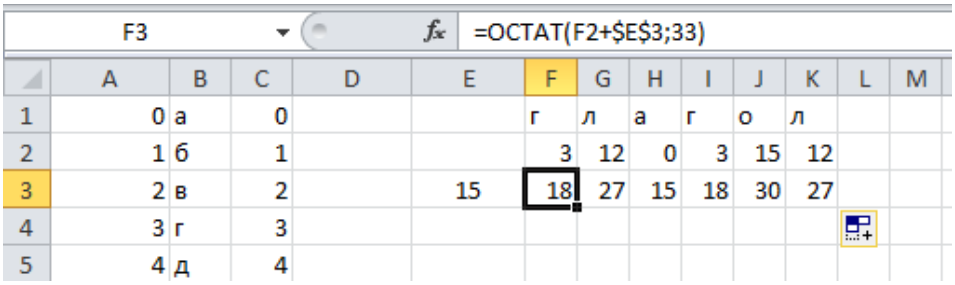
- вторым параметром (*Таблица*) функции назначить ссылку на таблицу с алфавитом начиная со второго столбца (2 и 3 столбцы), сделать ссылку абсолютной, нажав кнопку F4,
- значение третьего параметра (*Номер_столбца*) задать равным 2,
- в качестве значения четвертого параметра (*Интервальный_просмотр*) ввести слово *ложь*,например, **=ВПР(F1;$B$1:$C$33;2;ЛОЖЬ)**,скопировать функцию для всех символов шифруемого слова (рис. 21),



	A	B	C	D	E	F	G	H	I	J	K	L	M
1	0	а	0			г	л	а	г	о	л		
2	1	б	1			3	12	0	3	15	12		
3	2	в	2										

Рис. 21. Пример вычисления числового кода символа

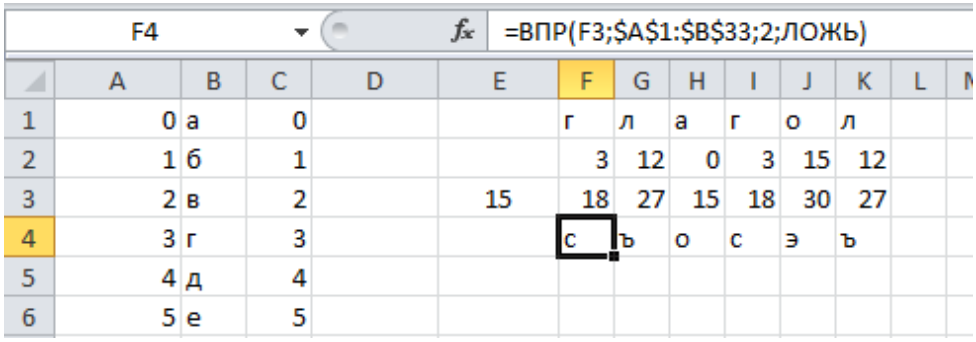
- строкой ниже получить код символа криптограммы, сложив по модулю 33 полученный код текущего символа со значением ключа:
  - ввести значение ключа,
  - во второй строке под текущим символом шифруемого слова вставить функцию **ОСТАТ**,
  - первым параметром (*Число*) функции указать сумму ячейки с кодом шифруемого символа и ячейки со значением ключа (ссылку на значение ключа сделать абсолютной),
  - второй параметр (*Делитель*) задать равным 33,например, **ОСТАТ(F2+$E$3;33)**, скопировать сформированную функцию **ОСТАТ** для всех символов шифруемого слова (рис.22).



	A	B	C	D	E	F	G	H	I	J	K	L	M
1	0	а	0			г	л	а	г	о	л		
2	1	б	1			3	12	0	3	15	12		
3	2	в	2		15	18	27	15	18	30	27		
4	3	г	3										
5	4	д	4										

Рис. 22. Пример вычисления кода криптограммы, ключ равен 15

- строкой ниже с помощью функции ВПР перевести полученный код криптограммы в символьный вид:
  - первым параметром функции назначить ссылку на ячейку с текущим кодом криптограммы,
  - вторым параметром функции назначить ссылку на таблицу с алфавитом начиная с первого столбца (1 и 2 столбцы), сделать ссылку на таблицу абсолютной,
  - значение третьего параметра (*Номер_столбца*) задать равным 2,
  - в качестве значения четвертого параметра (*Интервальный_просмотр*) ввести слово *ложь*,например, **=ВПР(F3;$A$1:$B$33;2;ЛОЖЬ)**,скопировать функцию для всех символов шифруемого слова (рис. 23) – криптограмма получена.



	A	B	C	D	E	F	G	H	I	J	K	L
1	0	а	0			г	л	а	г	о	л	
2	1	б	1			3	12	0	3	15	12	
3	2	в	2		15	18	27	15	18	30	27	
4	3	г	3			с	ъ	о	с	э	ъ	
5	4	д	4									
6	5	е	5									

Рис. 23. Пример текста, зашифрованного криптосистемой Цезаря

4. Проанализировать полученный текст криптограммы, обратив внимание на повторяющиеся символы.

Задание 2. Расшифровать криптограмму, полученную с помощью шифра Цезаря.

5. Выбрать значение ключа шифрования и криптограмму из таблицы 6 в соответствии с номером варианта.

Таблица 6

Варианты задания

№ варианта	Ключ шифрования	Криптограмма
1.	31	п ж й ж и м л
2.	29	ж ь и б з е ы
3.	28	ё а з к д и ю
4.	27	е ъ к н л я ё ц
5.	26	п ю ж ж з к л х
6.	25	й л н ж й к ж в
7.	24	ж ё г ё й е ё
8.	23	з я щ д ц в
9.	22	е ъ ё ъ щ х м х
10.	21	е г ж ф к э у
11.	20	ы у г ь е ю у
12.	19	ф б г б у ч ь
13.	18	э ъ г ъ з с
14.	17	с х у х э я г
15.	16	я ю ы ш ё ш о
16.	15	а ч н ь ч у
17.	14	я ц а б н д ц м
18.	13	ю х ъ ы ъ х щ
19.	2	й в г в д в
20.	11	т к л щ э к
21.	10	ф й ц о ъ й
22.	9	ъ ц с х ч у
23.	3	ъ з о с е з н
24.	7	о х т х щ х
25.	6	ч к ц к ж ц ф

6. Расшифровать криптограмму выбранным ключом:

- ввести в ячейки строки отформатированной области побуквенно текст криптограммы, важно, чтобы символы алфавита в таблице и символы вводимого слова были набраны в одном регистре;
- строкой ниже получить числовой код символов шифруемого слова с помощью функции **ВПР** (аналогично п.3);
- строкой ниже получить код символа расшифрованного теста, вычтя по модулю 33 значение ключа из полученного кода текущего символа криптограммы, используя функцию **ОСТАТ** (рис. 24).

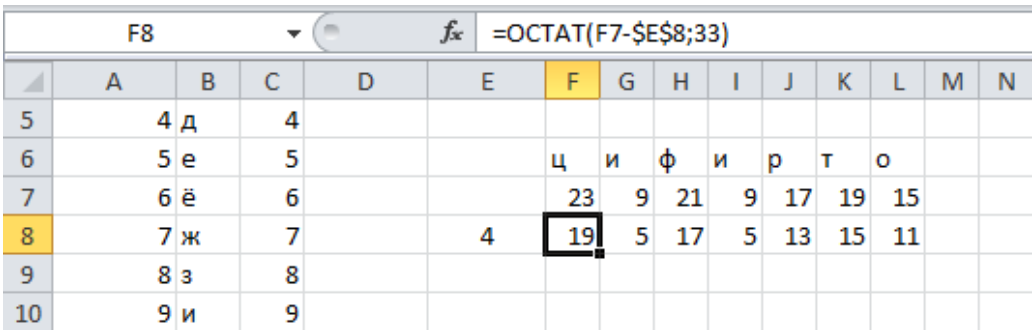


Рис. 24. Пример вычисления кода открытого текста, ключ равен 4

- строкой ниже с помощью функции **ВПР** перевести полученный код криптограммы в символьный вид (аналогично п.3, рис.25). Критерием правильности расшифрования является получение осмысленного слова.

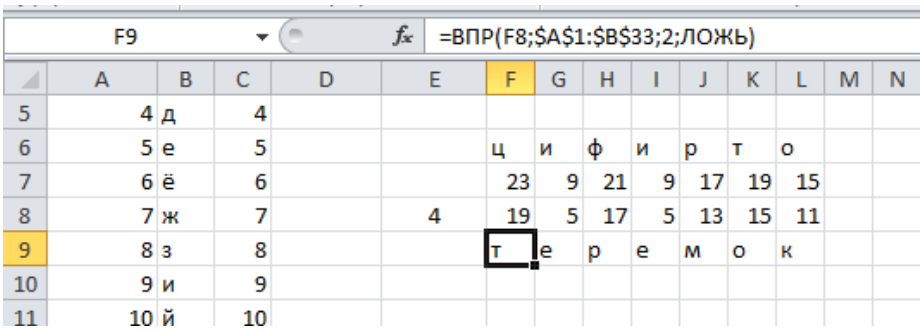


Рис. 25. Пример расшифрования текста

Задание 3.Зашифровать слово с помощью шифра Виженера.

7. Выбрать значение ключа шифрования из таблицы 7 в соответствии с номером варианта.

Таблица 7

Варианты задания

№ варианта	Ключ шифрования	Криптограмма
1.	слон	г ф ь а ц ю ч ш с
2.	клин	х ф й т ы щ н а у ц и
3.	смех	ю м ч ъ ю м ч ю ь м
4.	звон	з т ч в ф ж б ц т в
5.	приз	м ю н ш т х ы р ъ р
6.	лист	ю н э ч ш н д г ф з
7.	свет	ь р с я е п н э с ш н с

8.	вой	ф у х ж р т ё у ч к у
9.	мир	ю к х я ч ф х ч ф
10.	час	а н г й а э г я з а я
11.	кол	к ю р ц ъ к б ч к
12.	слово	ь ъ ь ц ч х р ь ш ч с ч к п э г ю к
13.	клуб	б р я п ь ю б п ь ю п
14.	стул	х б е ю е в б ъ г е п
15.	флаг	ф ц т ц ф ч ь р г э т я
16.	дрель	х т у р ю ф х с р й с я ц ю ш
17.	цена	б у ю р ы п а н е ц а ь
18.	парус	б и э а ц в р щ к я ю с г п
19.	скунс	ю ш в р а щ ш у е я а ь ё й
20.	кот	ч э а щ ю б ц ч с
21.	право	у х л р ю а я и й р ю ф с ф р ю
22.	куча	о в в у ч ш е т щ в ш о ы в й
23.	мост	ы р а л с р а ц ю б у б
24.	окно	х у п э б ш ь р э о я б р щ
25.	глаз	п щ о к с у а л г г н ц ф ю ь

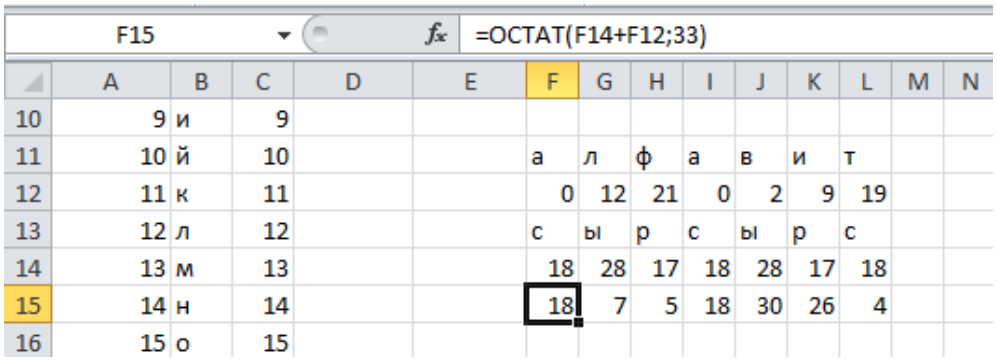
8. Зашифровать слово «алфавит» с помощью шифра Виженера с выбранным ключом:

- ввести в ячейки строки отформатированной области побуквенно шифруемое слово, важно, чтобы символы алфавита в таблице и символы вводимого слова были набраны в одном регистре;
- строкой ниже получить числовой код символов шифруемого слова с помощью функции **ВПР**(аналогично п.3);
- строкой ниже ввести побуквенно ключ шифра Виженера, циклически повторяя его, пока не будет достигнут конец шифруемого слова (рис.26);

	A	B	C	D	E	F	G	H	I	J	K	L	M	N
10	9	и	9											
11	10	й	10			а	л	ф	а	в	и	т		
12	11	к	11			0	12	21	0	2	9	19		
13	12	л	12			с	ы	р	с	ы	р	с		
14	13	м	13											

Рис. 26. Пример ключевой строки шифра Виженера (ключ «сыр»)

- строкой ниже получить числовой код символов ключевой строки с помощью функции **ВПР**(аналогично п.3);
- строкой ниже получить код символа криптограммы, сложив по модулю 33 полученный код текущего символа шифруемого слова с кодом текущего символа ключевой строки, используя функцию **ОСТАТ**(рис.27);



	A	B	C	D	E	F	G	H	I	J	K	L	M	N
10	9	и	9											
11	10	й	10			а	л	ф	а	в	и	т		
12	11	к	11			0	12	21	0	2	9	19		
13	12	л	12			с	ы	р	с	ы	р	с		
14	13	м	13			18	28	17	18	28	17	18		
15	14	н	14			18	7	5	18	30	26	4		
16	15	о	15											

Рис. 27. Пример вычисления кода криптограммы шифра Виженера

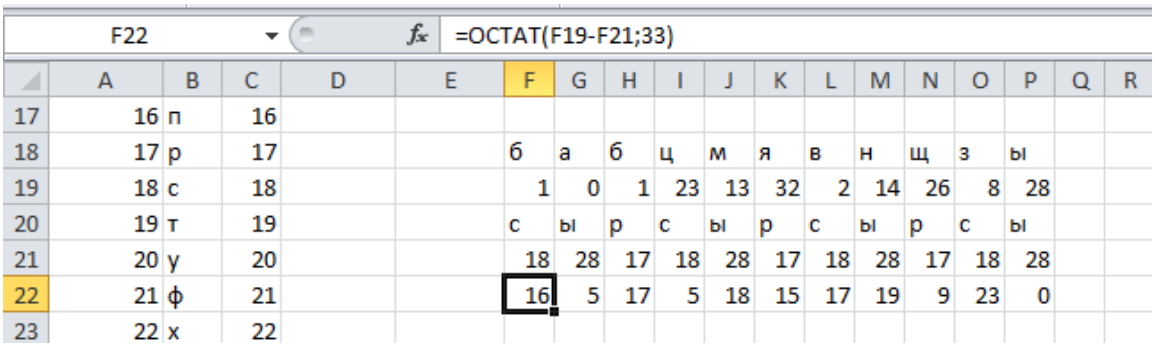
- строкой ниже с помощью функции **ВПР** перевести полученный код криптограммы в символьный вид (аналогично п.3).

Задание 4. Расшифровать криптограмму, полученную с помощью шифра Виженера.

9. Выбрать значение ключа шифрования и криптограмму из таблицы 7 в соответствии с номером варианта.
10. Расшифровать криптограмму выбранным ключом:

- ввести в ячейки строки отформатированной области побуквенно текст криптограммы, важно, чтобы символы алфавита в таблице и символы вводимого слова были набраны в одном регистре;
- строкой ниже получить числовой код символов шифруемого слова с помощью функции **ВПР** (аналогично п.3);
- строкой ниже сформировать ключевую строку (аналогично п.8);
- строкой ниже получить числовой код символов ключевой строки с помощью функции **ВПР**(аналогично п.3);
- строкой ниже получить код символа открытого текста, вычтя по модулю 33 код текущего символа ключевой строкиис кода-

текущего символа криптограммы, используя функцию **ОСТАТ**(рис.28);



	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R
17	16	п	16															
18	17	р	17			б	а	б	ц	м	я	в	н	щ	з	ы		
19	18	с	18			1	0	1	23	13	32	2	14	26	8	28		
20	19	т	19			с	ы	р	с	ы	р	с	ы	р	с	ы		
21	20	у	20			18	28	17	18	28	17	18	28	17	18	28		
22	21	ф	21			16	5	17	5	18	15	17	19	9	23	0		
23	22	х	22															

Рис. 28. Пример вычисления кода открытого текста шифра Виженера

- строкой ниже с помощью функции **ВПР** перевести полученный код криптограммы в символьный вид (аналогично п.3).Критерием правильности расшифрования является получение осмысленного слова.

11. Показать полученные значения криптограмм и открытых текстов преподавателю.

Практическая работа №4. Криптоанализ шифра простой замены

Описание шифра и рекомендации по криптоанализу

Шифр простой (одноалфавитной) замены – один из древнейших. Частным случаем одноалфавитной замены является шифр Цезаря.

Рассмотрим случай, когда соответствие между нормативным алфавитом и алфавитом шифрования задается таблицей.

Пусть соответствиемежду нормативным и шифрующим алфавитом задано таблицей 8. Зашифруем слово «ЗВЕЗДА».

Таблица 8

Пример одноалфавитной замены

нормативный алфавит	а	б	в	г	д	е	ж	з	и	й	к	л	м	н	о	п	…
алфавит шифрования	ф	к	с	э	и	у	х	п	о	б	ь	р	а	щ	з	г	…

Исходное сообщение: З В Е З Д А
Криптограмма: П С У П И Ф

Число вариантов ключа в таком шифре достаточно велико, однако криптоанализ осмысленных текстов не представляет большого труда, поскольку шифр простой замены сохраняет статистические характеристики исходного сообщения. Анализ шифра простой замены основан на использовании статистических закономерностей естественного языка. Так, например, известно, что в русском языке чаще всего встречается буквы «О», «А» и «Е», а наиболее редки «Ц», «Щ», «Э», «Ф» (без учета «Ё» и «Ъ»). Частоты букв русского языка в алфавите с символом пробела приведены в табл.9.

Таблица 9

Частоты символов русского языка (с пробелом)

Символ	**Частота**	**Символ**	**Частота**	**Символ**	**Частота**	**Символ**	**Частота**
-	0,175	Р	0,040	У	0,021	Х	0,009
О	0,089	В	0,038	Я	0,018	Ж	0,007
Е,Ё	0,072	Л	0,035	Ы	0,016	Ю	0,006
А	0,062	К	0,028	Ь,Ъ	0,014	Ш	0,006
И	0,062	М	0,026	Б	0,014	Ц	0,004
Т	0,053	Н	0,025	Г	0,013	Щ	0,003
Н	0,053	Д	0,025	Ч	0,012	Э	0,003
С	0,045	П	0,023	Й	0,010	Ф	0,002

Шифры простой замены обладают важным свойством: они не нарушают статистических характеристик языка исходного текста, то есть частоты появления символов, а также *k*-буквенных сочетаний (*k*-грамм) сохраняются. Это позволяет криптоаналитику получить открытый текст при помощи *частотного анализа*. Метод частотного анализа заключается в том, что наиболее часто встречающиеся буквы криптограммы заменяются наиболее вероятными символами нормативного алфавита.

Неравновероятность*k*-грамм (и даже слов) тесно связана с избыточностью текстана естественном языке – наличием в нем большого числа повторений отдельных фрагментов текста: корней, окончаний, суффиксов, слов и фраз. Для русского языка

наиболее частыми фрагментами являются биграммы и триграммы:

СТ, НО, НЕ, ЕН, ТО, НА, ОВ, НИ, РА, ВО, КО, ПО
СТО, ЕНО, НОВ, ТОВ, ОВО, ОВА, ОГО, ПРО, АТЬ, ЕНИ

Следует, однако, отметить, что частоты появления символов в конкретном тексте могут отличаться от стандартных, и достаточно существенно. Эти отличия могут проявиться тем сильнее, чем короче сообщение. Поэтому частотный анализ коротких сообщений иногда бывает весьма затруднителен.

Приведем некоторыесоветы по выполнению частотного анализа русских текстов:

1. Сначала следует подсчитать частоты появления каждого символа в криптограмме. Далее следует сопоставить полученные значения с таблицей стандартных частот русского языка (табл.9). Совпадение может быть не точным, однако возможно определить наиболее часто встречающиеся символы. Если нормативный алфавит включает пробел, то наиболее частый символ – это «_» (появляется с частотой более 15%), далее следуют гласные «О» и «Е». Можно предположить, что следующие по частоте символы – также гласные: «А» и «И». Также можно сделать предположение относительно наиболее редко встречающихся символов (менее 1%) – скорее всего, это согласные: «Х», «Ж», «Ш», «Ц», «Щ», «Ф», или «Э», «Ю».
2. Если, как это часто бывает, прямое сопоставление частот не приводит сразу к раскрытию текста сообщения, рекомендуется обратить внимание на пары повторяющихся букв. В русском языке чаще всего повторяются буквы **нн**, **сс** (в середине слов, перед окончанием); **ии,ее,мм**(как в середине слов, так и окончание), **оо** (только в середине слов), **вв** (в начале или в середине слов).
3. Если в шифртексте имеются пробелы между словами, то можно постараться определить слова, состоящие из одной, двух или трех букв. Таблица 10 содержит частотный список (в порядке убывания частоты появления в текстах) первых однобуквенных, двухбуквенных, трехбуквенных и четырехбуквенных лексем русского языка.

Лексема охватывает все словоформы (изменение слова по падежам и спряжение для глаголов). Полный частотный список лексемможно найти, например, в «Новом частотном словаре русской лексики»[1].

Таблица 10

Частотный список коротких лексем русского языка

Однобуквенные	*Двухбуквенные*		*Трехбуквенные*		*Четырехбуквенные*
в	не	за	что	год	быть
я	на	от	как	все	этот
с	он	же	это	его	весь
а	по	вы	они	еще	свой
к	но	ты	она	или	мочь
у	мы	бы	так	уже	себя
о	из	ее	для	вот	если

Следует обратить внимание и на слова-палиндромы (слова, читающиеся одинаково как слева направо, так и справа налево),а также на другие слова с особенностями орфографии, например, на слова, пишущиеся через дефис (табл. 11).

Таблица 11

Слова-палиндромы, слова с дефисами

Слова-палиндромы	**Слова с дефисами**	
как	как-то, что-то, какой-то, кто-то, чего-то, когда-то	пол-яблока
еще	из-за, из-под	давай-ка
или	все-таки, прямо-таки	северо-запад, юго-восток
ее	какой-нибудь, что-нибудь, кто-нибудь	научно-исследовательский, железно-бетонный, сине-зеленый
оно	во-первых, во-вторых	вице-президент, генерал-лейтенант

[1]ЛяшевскаяО.Н., Шаров С.А.,Частотный словарь современного русского языка (на материалах Национального корпуса русского языка). М.: Азбуковник, 2009: [Электронный ресурс]URL: http://dict.ruslang.ru/freq.php

еле	по-видимому по-своему, по-моему, по-нашему	по-французски, по-немецки, по-хозяйски
тот, тут	вот-вот, еле-еле, чуть-чуть, ха-ха	по-старому, по-новому, по-хорошему
лил, летел, лишил	как-либо, куда-либо, какой-либо	давным-давно, мало-помалу, крепко-накрепко, крест-накрест, как-никак, волей-неволей, нежданно-негаданно
иди	кое-где, кое-кто, кое-что	

4. При анализе криптограммы рекомендуется учитывать не только частность отдельных символов, но и частоту появления *k*-грамм (табл.1,3), сочетание гласных и согласных (табл.2), а если в тексте оставлены пробелы – то и частоты первых/последних букв. Так, например, в качестве первых букв слова чаще всего встречаются буквы «С», «П», «В», «Н», «О», «И», «М» и«К», первыми буквами не могут быть «Ы» и «Ь», «Ъ», что отличается от данных общей частотной таблицы (табл. 9).
5. Тексты разных жанров имеют свои особенности. Если это возможно, следует подготовить таблицу частотности текстов, учитывающую жанровые особенности сообщения, которое требуется дешифровать. Например, в телеграфных сообщениях обычно опускают предлоги и союзы, отсутствие таких словбудет снижать частотность некоторых наиболее часто встречающихся букв. В этом случае следует использовать частотную таблицу, созданную на основе подсчета статистики других телеграфных сообщений.
6. Если есть возможность сделать некоторые предположения о содержании открытого текста, можно попытаться угадатьего типовые фрагменты или формулировки (часто присутствуют, например, в деловой переписке, распорядительных документах), помогающие решить задачу криптоанализа.
7. В некоторых случаях частотность букв криптограммы уже совпадает с частотностью букв в таблице, и все же зашифрованный текст не читаем. В этом случае, скорее всего, использован не шифр замены, а шифр перестановки. Все буквы остались теми же, но находятся не на своих местах.

Рассмотрим пример частотного анализа шифра простой замены.Пусть дан текст криптограммы:

«УТЦПАКПЩНСЩГАЛЙЮБШИАРБУТЦПФБСНЫАШЙ
АЬЙЛБАНСЙСТНСТОБНДЩМЩАЙШЙЖТЛЙАСБДНСЙАШ
ЩАСЩЖЕДЩАБНЖТАЩШАРЩНСЙСЩОШЩАРЖТШ-
ШИГ».

Известно, что нормативный алфавит содержит пробел.

Подсчитаем частоты появления различных символов в криптограмме и проведем их сравнение со стандартными частотами (табл.12):

Таблица 12

Сопоставление частот

Частоты появления символов в криптограмме												
Символ	А	Щ	С	Й	Ш	Н	Б	Т	Ж	Д	Р	…
Частота	0,131	0,103	0,093	0,084	0,075	0,075	0,065	0,065	0,037	0,028	0,028	
Стандартные частоты												
Символ	_	О	Е	А	И	Н	Т	С	Р	В	Л	…
Частота	0,175	0,089	0,072	0,062	0,062	0,053	0,053	0,045	0,04	0,038	0,035	

Заменим два наиболее часто встречающихся символа криптограммы: «А» − на символ пробела «_» и «Щ» −на «О». Получим соответствие:

У Т Ц П А К П Щ Н С Щ Г А Л Й Ю Б Ш И А Р Б У Т Ц П Ф Б С
- - - - _ - - о - - о - _ - - - - - - - _ - - - - - - - - -
Н Ы А Ш Й А Ь Й Л Б А Н С Й С Т Н С Т О Б Н Д Щ М Щ А Й Ш
- - _ - - _ - - - - _ - - - - - - - - - - - - о - о _ - -
Й Ж Т Л Й А С Б Д Н С Й А Ш Щ А С Щ Ж Е Д Щ А Б Н Ж Т А Щ
- - - - - _ - - - - - - _ - о _ - о - - - о _ - - - - - _ о
Ш А Р Щ Н С Й С Щ О Ш Щ А Р Ж Т Ш Ш И Г
- _ - о - - - - о - - о _ - - - - - - - -

Обратим внимание на двухбуквенные слова «Ш Щ» и «Щ Ш», а также на сдвоенное «Ш Ш» в последнем слове. Поскольку «Щ» заменено на букву «О», то «Ш» − согласная, может быть буквой «Н» или «Т», «Д», «П». Скорее всего это «Н», в этом

случае последнее слово – прилагательное, а «НН» стоит перед окончанием. Сделаем замену «Ш» − «Н».

У Т Ц П А К П Щ Н С Щ Г А Л Й Ю Б Ш И А Р Б У Т Ц П Ф Б С
- - - - _ - - о - - о - _ - - - - - н - _ - - - - - - - - - -
Н Ы А Ш Й А Ь Й Л Б А Н С Й С Т Н С Т О Б Н Д Щ М Щ А Й Ш
- - _ н - _ - - - - - _ - - - - - - - - - - - - - - о - о _ - н
Й Ж Т Л Й А С Б Д Н С Й А Ш Щ А С Щ Ж Е Д Щ А Б Н Ж Т А Щ
- - - - - _ - - - - - - - _ н о _ - о - - - о _ - - - - - _ о
Ш А Р Щ Н С Й С Щ О Ш Щ А Р Ж Т Ш Ш И Г
н _ - о - - - - о - н о _ - - - н н - -

Можно предположить, что стоящее на конце седьмого слова сочетание «Щ М Щ» – это окончание «ОГО» прилагательного, тогда «М» − «Г». Если это так, то следующее за прилагательным слово, скорее всего, существительное мужского рода в родительном падеже, и окачивается на «А». Отсюда «Й» − «А». Данное предположение не противоречит таблице частот.

Тогда:

У Т Ц П А К П Щ Н С Щ Г А Л Й Ю Б Ш И А Р Б У Т Ц П Ф Б С
- - - - _ - - о - - о - _ - а - - н - _ - - - - - - - - - -
Н Ы А Ш Й А Ь Й Л Б А Н С Й С Т Н С Т О Б Н Д Щ М Щ А Й Ш
- - _ н а _ - а - - _ - - а - - - - - - - - - о г о _ а н
Й Ж Т Л Й А С Б Д Н С Й А Ш Щ А С Щ Ж Е Д Щ А Б Н Ж Т А Щ
а - - - а _ - - - - - а _ н о _ - о - - - о _ - - - - - _ о
Ш А Р Щ Н С Й С Щ О Ш Щ А Р Ж Т Ш Ш И Г
н _ - о - - а - о - н о _ - - - н н - -

Пятым словом является предлог «НА», поэтому следующее слово оканчивается, скорее всего, на «Е». Заменим «Б» − «Е».

У Т Ц П А К П Щ Н С Щ Г А Л Й Ю Б Ш И А Р Б У Т Ц П Ф Б С
- - - - _ - - о - - о - _ - а - е н - _ - е - - - - - - е -
Н Ы А Ш Й А Ь Й Л Б А Н С Й С Т Н С Т О Б Н Д Щ М Щ А Й Ш
- - _ н а _ - а - е _ - - а - - - - - - - - е - - о г о _ а н
Й Ж Т Л Й А С Б Д Н С Й А Ш Щ А С Щ Ж Е Д Щ А Б Н Ж Т А Щ
а - - - а _ - е - - - а _ н о _ - о - - - о _ е - - - - _ о
Ш А Р Щ Н С Й С Щ О Ш Щ А Р Ж Т Ш Ш И Г
н _ - о - - а - о - н о _ - - - н н - -

Рассмотрим слово «АНА - - - А». Предположим, что это слово «АНАЛИЗА». Сделаем замены: «Ж» − «Л», «Т» − «И», «Л» − «З». Получили:

У Т Ц П А К П Щ Н С Щ Г А Л Й Ю Б Ш И А Р Б У Т Ц П Ф Б С
- и - - _ - - о - - о - _ з а - е н - _ - е - и - - - е -
Н Ы А Ш Й А Ь Й Л Б А Н С Й С Т Н С Т О Б Н Д Щ М Щ А Й Ш
- - _ н а _ - а з е _ - - а - и - - и - е - - о г о _ а н
Й Ж Т Л Й А С Б Д Н С Й А Ш Щ А С Щ Ж Е Д Щ А Б Н Ж Т А Щ
а л и з а _ - е - - - а _ н о _ - о л - - о _ е - л и _ о
Ш А Р Щ Н С Й С Щ О Ш Щ А Р Ж Т Ш Ш И Г
н _ - о - - а - о - н о _ - л и н н - -

Слово «Е - ЛИ» – это, скорее всего «ЕСЛИ», последнее слово «- ЛИНН - -» похоже на «ДЛИННЫЙ», а в словосочетании «НА - АЗЕ» (АНАЛИЗА) – стоит слово «БАЗЕ». Сделаем соответствующие замены: «Н» − «С», «Р» − «Д», «И» − «Ы», «Г» − «Й», «Ь» − «Б».

У Т Ц П А К П Щ Н С Щ Г А Л Й Ю Б Ш И А Р Б У Т Ц П Ф Б С
- и - - _ - - о с - о й _ з а - е н ы _ д е - и - - - е -
Н Ы А Ш Й А Ь Й Л Б А Н С Й С Т Н С Т О Б Н Д Щ М Щ А Й Ш
с - _ н а _ б а з е _ с - а - и с - и - е с - о г о _ а н
Й Ж Т Л Й А С Б Д Н С Й А Ш Щ А С Щ Ж Е Д Щ А Б Н Ж Т А Щ
а л и з а _ - е - с - а _ н о _ - о л - - о _ е с л и _ о
Ш А Р Щ Н С Й С Щ О Ш Щ А Р Ж Т Ш Ш И Г
н _ д о с - а - о - н о _ д л и н н ы й

Обратим внимание на слово «С - А - ИС - И - ЕС - ОГО» (АНАЛИЗА), что похоже на слово «СТАТИСТИЧЕСКОГО», если это так, то читается и слово «ДОС - А - О - НО» – «ДОСТАТОЧНО». Сделаем замены: «С» − «Т», «О» − «Ч», «Д» − «К». Получили:

У Т Ц П А К П Щ Н С Щ Г А Л Й Ю Б Ш И А Р Б У Т Ц П Ф Б С
- и - - _ - - о с т о й _ з а - е н ы _ д е - и - - - е т
Н Ы А Ш Й А Ь Й Л Б А Н С Й С Т Н С Т О Б Н Д Щ М Щ А Й Ш
с - _ н а _ б а з е _ с т а т и с т и ч е с к о г о _ а н
Й Ж Т Л Й А С Б Д Н С Й А Ш Щ А С Щ Ж Е Д Щ А Б Н Ж Т А Щ
а л и з а _ т е к с т а _ н о _ т о л - к о _ е с л и _ о
Ш А Р Щ Н С Й С Щ О Ш Щ А Р Ж Т Ш Ш И Г
н _ д о с т а т о ч н о _ д л и н н ы й

Теперь, заметив, что первое и четвертое слова криптограммы имеют общую последовательность букв «УТЦП», и, исходя из контекста, не сложно сделать оставшиеся замены. Получили открытый тест: «ШИФР ПРОСТОЙЗАМЕНЫДЕШИФРУЕТСЯ НА БАЗЕ СТАТИСТИЧЕСКОГО АНАЛИЗА ТЕКСТА НО ТОЛЬКО ЕСЛИ ОН ДОСТАТОЧНО ДЛИННЫЙ».

В таблице 13 приведен ключ шифра – соответствие между символами нормативного алфавита и алфавита шифрования, по которому проводится их замена. Вопросительные знаки соответствуют буквам, ни разу не встретившимся в тексте криптограммы.

Таблица 13

Ключ шифра простой замены из примера

Нормативный алфавит	_	А	Б	В	Г	Д	Е	Ж	З	И	Й	К	Л	М	Н	О
Алфавит шифрования	?	_	е	?	й	к	ь	л	?	ы	а	п	з	г	с	ч
Нормативный алфавит	П	Р	С	Т	У	Ф	Х	Ц	Ч	Ш	Щ	Ы	Ь	Э	Ю	Я
Алфавит шифрования	р	д	т	и	ш	у	?	ф	?	н	о	я	б	?	м	?

Задание

Дешифровать криптограмму, полученную шифром простой замены. Символы криптограммы закодированы двузначными числами. В тексте криптограммы сохранены пробелы и пунктуация. Символ пробела и знаки препинания в нормативный алфавит не входят.

Указания к выполнению практической работы

Для выполнения практической работы рекомендуется использовать файл *Простая замена.xlsm*. Тексты криптограмм для анализа приведены в Приложении 1.

Технология выполнения задания

1. Открыть книгу MSExcel*Простая замена.xlsm*, в строке предупреждения включить выполнение макросов.
2. Скопировать текст криптограммы из Приложения 1в соответствии с номером варианта.

3. Перейти на лист *Загрузить криптограмму* и выбрать ячейку **B3**. Установить курсор мыши в строку формул, вставить в нее скопированный текст и нажать Enter.Затем нажать кнопку **Загрузить криптограмму**.
4. После загрузки криптограммы будет открыт лист *Криптограмма*. Под символами криптограммы в процессе расшифрования должны отображаться символы открытого текста. Первоначально отображаются знаки #, что указывает на то, что не установлено никаких соответствий между символами криптограммы и символами нормативного алфавита.

ЗАМЕЧАНИЕ: В силу особенностей реализациикниги *Простая замена.xlsm*, текст криптограммы, наряду с цифрами – символами алфавита шифрования должен содержать только знаки пробела, двойных кавычек, «.», «,», «;», «:», «!», «-». Если текст содержит другие знаки (например, «?», скобки, «…» и т.п.), после загрузки криптограммы следует очистить ячейки, содержащие эти символы, с помощью клавиши Del. Нельзя использовать операцию вырезки  , используйте только операцию копирования и клавишу Del.

5. Подсчитать частоты появления символов криптограммы:

- Двузначные числа, составляющие криптограмму,последовательно занести в столбец **G** таблицы *Назначить* на листе *Частоты символов*. По мере занесения чисел соответствующие им знаки # на листе *Криптограмма* будут заменены на символ подчеркивания «_». Заносить в таблицу следует только те числа, для которых отображается знак #.
- После того, как все символы шифралфавита занесены в таблицу *Назначить* (о чем свидетельствует отсутствие знаков # на листе *Криптограмма*), скопировать значения из столбца **G** таблицы в столбец **A** таблицы *Статистика - Криптограмма* на листе *Частоты символов*. В столбце **B** отобразятся частоты встречаемости в криптограмме символов шифралфавита (использованных для шифрования текста двузначных чисел).

6. После того, как все символы криптограммы занесены в таблицы *Криптограмма* и *Назначить*, следует снять защиту с листа *Частоты символов*. Для этого перейти на лист Частоты сим-

волов и выполнить команду**Рецензирование/Снять защиту листа**.

7. На листе *Частоты символов*с помощью команды **Данные/Сортировка** отсортировать таблицу *Криптограмма* по столбцу *Част* в порядке убывания частот (внимание, выделяйте всю таблицу!), а таблицу *Назначить* – по столбцу *Крипт* в порядке возрастания значений символов шифр-алфавита.
8. После сортировки установить защиту листа *Частоты символов* с помощью команды **Рецензирование/Защитить лист**.
9. На листе *Частоты символов* приведены стандартные частоты символов русского языка для нормативного алфавита без пробела. Диаграммы позволяют провести визуальное сравнение стандартных частот и частот криптограммы.
10. Высказать предположение относительно соответствия наиболее часто встречающихся символов буквам «О» и «Е» и занести эти буквы в таблицу *Назначить*в столбец **Н**рядом с нужными символами шифралфавита. Буквы отобразятся на листе *Криптограмма* в соответствующих местах текста.

ЗАМЕЧАНИЕ: Поскольку текст криптограммы не слишком велик, следует учесть, что закономерности русского языка могут проявляться в нем не в строгом соответствии с таблицей стандартных частот.

11. Проанализировать полученные фрагменты теста на листе *Криптограмма* с точки зрения закономерностей русского языка и оценить правильность выдвинутой гипотезы о соответствии символов. Если имеется несоответствие, следует изменить назначение букв символам шифралфавита в таблице *Назначить* на листе *Частоты символов*.
12. Используя рекомендации по криптоанализу, последовательно выдвинуть гипотезы относительно соответствия между другими символами криптограммы и буквами русского языка, каждый раз:

- задавая соответствие в таблице *Назначить* на листе *Частоты символов*,
- проводя анализ корректности полученногона листе *Криптограмма*частично дешифрованного текста с точки зрения русского языка,

- изменяя или удаляя, в случае несоответствия, сделанные на листе *Частоты символов* назначения.

13. После завершения дешифрования текста показать его преподавателю.

Практическая работа №5. Криптоанализ многоалфавитного шифра (шифраВиженера)

Рекомендации по криптоанализу

Шифры простой замены могут быть вскрыты с помощью частотного анализа, поскольку не меняют статистику открытых текстов. В отличие от них, шифры сложной (многоалфавитной) замены маскируют естественную частоту появления символов в тексте. Поэтому многоалфавитные замены значительно надежнее, однако, частотный анализ применим и к ним.

Частотный анализ шифра Виженера с использованием статистик (метод индекса совпадений) предложен в 1922 году американским криптографом Уильямом Фридманом. Это первый пример успешного применения вероятностно-статистических методов в криптоанализе, однако методы взлома шифра Виженера были описаны еще в XIXвеке.

Пусть M – длина ключевого слова в шифре Виженера. Если ключевое слово короче шифруемого текста, оно будет последовательно повторяться, чтобы длина ключевой последовательности (гаммы) совпала с длиной шифруемого сообщения. ВеличинаM-называется*периодом гаммы*.

Разобьем криптограмму на блоки, равные по длине периоду гаммы. Символы криптограммы, занимающие одинаковое положение в таких блоках, зашифрованы одним и тем же символом ключа, то есть для их получения использован один и тот же шифр простой замены, а именно, шифр Цезаря.

Описанное свойство позволяет применить частотный анализ для каждой группы символов криптограммы, соответствующей определенной букве ключа. Такие группы символов называют *группами периода*. Число групп периода равно длине ключаM.

Как известно, алфавит шифрования в криптосистеме Цезаря представляет собой циклически сдвинутый влево нормативный алфавит. Величина сдвига для каждой из групп периода определяется соответствующей буквой ключа. В результате частотного анализа символов, составляющих группу периода, будет определена величина этого сдвига. Проделав эту процедуру для каждой из групп, можно получить ключ шифрования. Такой метод криптоанализа может быть эффективен, если длина криптограммы Nпревышает $20M$($N > 20M$), M – длина ключа.

Однако, для получения групп периода надо знать длину ключевого слова. Поэтому криптоанализ шифра Виженера проводится в два этапа. На первом этапе определяется длина ключаM, на втором этапе – само ключевое слово.

ЧислоMможет быть определено разными способами. Так, в 1863 г. был предложен метод, получивший название **теста Казиски** в честь своего автора. Тест основан на простом наблюдении, что два одинаковых отрезка открытого текста, отстоящих друг от друга на расстоянии, кратном M, будут зашифрованы одинаково. Тест сводится кпоиску в криптограмме повторяющихся фрагментов длиной, не меньшей трех, и определению расстояния между ними. Случайное появление в шифртекстеповторяющихсяфрагментовдостаточной длины маловероятно.

Пусть d_1,d_2,... – найденные расстояния между повторениями и d– наибольший общий делитель (НОД) этих чисел. Тогда Mкратноd. Чем больше повторяющихся фрагментов имеется вкриптограмме, тем больше вероятность того, что M совпадет с d.

Для определения значения M, может быть использован и **автокорреляционный метод**. Текст криптограммы выписывается в строку, под ним выписываются строки, в которых текст сдвинут влево на 1, 2, 3, 4 и так далее позиции (t=1,2,3,…). Затем для каждой строки подсчитывается число позиций (столбцов), в которых символ строки совпал с символом исходной строки в той же позиции (c_i=c_{i+t}). Затем для каждой строки вычисляются *автокорреляционные коэффициенты*, равные отношению числа совпадений к длине строки. Для значений сдвигаt, кратных периоду гам-

мы, автокорреляционные коэффициенты должны быть заметно больше, чем для сдвигов, не кратных периоду.

Для проверки правильности выбора значения M, можно применить**методиндекса совпадений**.

Индексом совпадений$I_C(x)$для последовательности $x = (x_1,...,x_m)$,составленной из букв алфавита A, называется вероятность того, что две случайно выбранные буквы из этой последовательности совпадают.

Пусть A–алфавит мощностью L,состоящий из символов a_i, $i=0,\ldots,L-1$; $A=\{a_1,...,a_{L-1}\}$.Значение индекса совпадениявэкспериментальноможет быть получено как:

$$I_C(x) = \frac{\sum_{i=0}^{L-1} f_i(f_i - 1)}{m(m-1)},$$

где f_i–число вхождений буквы a_iв последовательности x.

Пусть x– строка осмысленного текстана естественном языке. Допустим, что буквы в xпоявляются в любом месте текста с вероятностями $p_0,...,p_{L-1}$ независимо друг от друга, где p_i– вероятность появления буквы a_iв осмысленном тексте. Тогда при достаточно больших m и определении p_iкак $p_i=f_i / m$ получаем приближенную формулу:

$$I_C(x) \approx \sum_{i=0}^{L-1} p_i^2 .$$

Взяв за основу значения вероятностей p_iдля открытых текстов на естественном языке (например, изчастотных таблиц), можно получитьтеоретически ожидаемые значения индекса совпадения для разных языков (табл.14).

Таблица 14

Значения индекса совпадений европейских языков

Язык	Русский	Русск. с пробелом	Алгл.	Франц.	Нем.	Итал.	Испан.
$I_C(x) \approx$	0,055	0,068	0,066	0,078	0,076	0,074	0,077

Шифрование открытого с помощьюпростой замены не изменяет значения индекса совпадений. Действительно, в этом случае вероятности p_iпереставляются местами, но значение суммых

квадратов остается неизменной. Таким образом, значения из таблицы 14 будут справедливы для любых шифров простой замены, в том числе, и в случае, когда x является группой периода шифра Виженера.

В то же время, если последовательность x– реализация независимых испытаний равномерно распределеннойслучайной величины (появление всех символов равновероятно), то индекс совпадения может быть вычисленкак:

$$I_c(x) = \sum_{i=0}^{L-1} \frac{1}{L^2} = L \cdot \frac{1}{L^2} = \frac{1}{L},$$

где L– мощность алфавита Aслучайной последовательности x. Значение индекса совпадений будет в этом случае ощутимо ниже – порядка$1/L$. Для русского языка, например, это значение составляет 0,03.

Заметная разница значений $I_C(x)$ для осмысленных текстов и случайных последовательностей букв позволяет в большинстве случаев установить точное значение периода гаммы (длины ключевого слова) Mв шифре Виженера.

Пусть$y=(y_1,y_2,\ldots,y_N)$–криптограмма, полученная шифром Виженера, и пусть высказано предположение относительно периода гаммы (длины ключевого слова) M. Выпишем последовательность yпострочно с периодом M. Столбцы получившейся таблицы составляют группы периода шифра, обозначим их черезY_i, $i=1,\ldots,M$ (рис. 29).

Y_1	Y_2	…	Y_M
y_1	y_2	…	y_M
y_{M+1}	y_{M+2}	…	y_{2M}
y_{2M+1}	y_{2M+2}	…	y_{3M}
…	…	…	…

Рис. 29. Получение групп периода

Еслидлина ключевого словаMопределена правильно, то каждый столбец Y_i, $i=1,\ldots,M$, представляет собой группу периода, то естьнабор символов открытого текста, зашифрованных простой заменой – шифром Цезаря со сдвигомS_i, определяемым i-

тымсимволом ключевого слова.Поэтому для русского текста должно быть получено$I_C(Y_i) \approx 0{,}055$ при любом i.

С другой стороны, если значение Mвыбрано неверно и отличается от длины ключевого слова, то столбцы Y_iбудут более похожи на случайные последовательности символов, поскольку они являются результатом зашифрования фрагментов открытого текста многоалфавитным шифром. Тогда значения$I_C(Y_i)$будут приближенык числу $1/L \approx 0{,}03$ (для русского языка).

Предположим, что на первом этапе найдена длина ключевого слова M. Теперь требуетсянайти само ключевое слово, то есть определить сдвиги S_i, $i=1,\ldots,M$, каждой из групп периода относительно нормативного алфавита.

Для решения этой задачи может быть использована статистика, названная*взаимныминдексом совпадений.*

Пусть $x=(x_1,...,x_m)$, $y=(y_1,...,y_{m'})$– две строки символов алфавита A.

Взаимным индексом совпадения$MI_c(x,y)$называется вероятность того, что случайно выбранная буква из xсовпадает со случайно выбранной буквой из y.

Пусть $f_0, f_1,\ldots, f_{L-1}$и $f'_0, f'_1,\ldots, f'_{L-1}$–частотывхождений букв алфавита A в строки xи yсоответственно.Тогда

$$MI_C(x,y) = \frac{\sum_{i=0}^{L-1} f_i \cdot f'_i}{m \cdot m'}.$$

Рассмотрим относительные сдвигиS_i–S_jгрупп периода Y_iиY_j. При нулевом сдвиге между группами периода индекс $MI_c(x,y)$ близок к значениям индекса совпаденийв естественном языке (табл.14).Ненулевые относительные сдвиги дают более низкие значениявзаимногоиндекса совпадений. Это наблюдение позволяет определить верные величины относительных сдвигов групп периода между собой. Тогда можносоставить систему уравнений, связывающую относительные сдвиги различных групп периода. В результате останется 33 (для русского языка) варианта для ключевого слова, из которых можно выбрать верное ключевое слово, если оно является осмысленным текстом.

Этот метод эффективен для небольших значений *M*, поскольку для получения надежных статистик потребуются тексты достаточно большой длины.

Задание

Дешифровать криптограмму, полученную шифром Виженера.Известно, что алфавит открытого текста совпадает с алфавитом русского языка без буквы «ё» с добавлением символа пробела (33 буквы).

Указания к выполнению практической работы

Для выполнения практической работы рекомендуется использовать файл *Шифр Виженера.xlsm*. Тексты криптограмм содержатся в приложении 2.

Технология выполнения задания

Задание 1. Определить длину использованного ключевого слова (период гаммы) шифра Виженера.

1. Выбрать в соответствии с номером варианта криптограмму для анализа из Приложения 2 и скопировать ее в новый документ MSWord.
2. Выполнить тест Казиски, заключающийся в поиске повторяющихся фрагментовв шифртексте.Для выполнения теста Казиски рекомендуется использовать возможности текстового редактора MSWord:

- Установить курсор в начало текстакриптограммы. Выполнить команду **Главная/Найти**. В окне команды набрать первые три символа текста криптограммы, будет осуществлен поиск совпадений.
- В случае, если повторения не найдено, выполнить поиск повторений для 2, 3 и 4 символов криптограммы, и так далее, пока не будет найден повторяющийся фрагмент, состоящий из 3 или более символов (вероятность случайного повторения двухбуквенных сочетаний достаточно высока).
- В случае, если найдено повторение, следует выделить все вхождения этого сочетания букв (например, заливкой цветом), для

перехода к следующему найденному фрагменту следует воспользоваться кнопками со стрелками в окне поиска.

- После того, как все повторения фрагмента выделены, следует проанализировать следующие за повторениями символы с целью выяснить, не имеет ли повторяющийся фрагмент большую длину. Если это так, дополнительные символы также следует выделить (рис. 30).

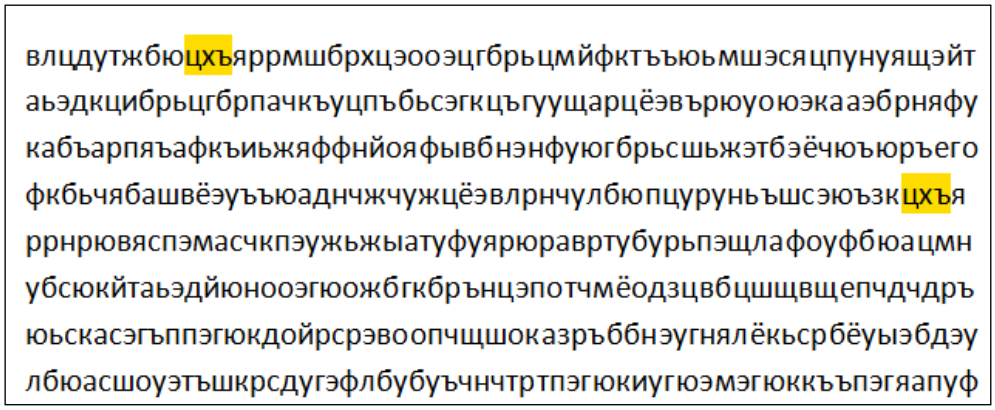


Рис. 30. Пример поиска повторений с помощью тестаКазиски

В примере на рис. 30, первый найденный трехбуквенный фрагмент – «цхъ». Для него в тексте криптограммы имеется лишь одно повторение. Видно, что следующие за этим фрагментом буквы также повторяются, поэтому фрагмент имеет длину 6 символов и выглядит как «цхъярр». Случайное появление столь длинного повторяющегося фрагмента маловероятно.

3. После нахождения и выделения нескольких повторяющихся фрагментов следует определить расстояние между повторениями каждого из фрагментов:

- Выделить текст от начала первого повторяющегося фрагмента до начала следующего его вхождения в текст, не включая сам следующийфрагмент (или от конца первого фрагмента до конца следующего).
- Выполнить команду **Рецензирование/Статистика** . Расстояние в знаках указано в строке *Знаков (с пробелами)* в окне команды.

Так, расстояние между повторяющимися фрагментами «цхъярр» на рис. 30составило 210 знаков.

- Если фрагмент встречается в тексте более двух раз, следует определить расстояния между каждыми соседними повторениями.

4. Полученные значения расстояний между фрагментами следует занести в книгу *Шифр Виженера.xlsm*:

- Открыть книгу *Шифр Виженера.xlsm*, включить выполнение макросов в строке предупреждения. Занести текст каждого из повторяющихся фрагментов и значения расстояний между повторениями в форму на лист *Опред-е периода1* (рис. 31).

Сочетание	Расстояния			Кол-во повторений
цхъярр	210			2
цгбр	40			2
гбр	40	80	550	4
брьц	35	595		3

Рис. 31. Пример заполнения формы для определения периода гаммы с помощью теста Казиски

- В низу формы будет рассчитано значение НОД введенных расстояний.

Для расстояний, указанных на рис. 31, будет получено значение НОД, равное 5, тогда, скорее всего, период гаммы (длина ключевого слова)*M*=5.

Период гаммы *M*кратен или находится среди делителей НОД расстояний. Желательно, чтобы найденные в тексте повторения позволяли однозначно определить период гаммы, для этогоНОД должен быть простым числом (делится нацело только на себя и на 1). Таким образом, рекомендуется, если это возможно, производить поиск повторяющихся фрагментов в тексте до тех пор, пока значение НОД не будет простым числом.

5. Определить период гаммы методом автокорреляции:

- На лист *Опред-е периода2* в строку 2 (*Криптограмма*) занести посимвольно текст криптограммы. Поскольку шифртекстимеет большую длину, можно занести лишь первые 75-100 его символов.

ЗАМЕЧАНИЕ: Для удобства занесения символов криптограммы, можно загрузить ее в книгу *Шифр Виженера.xlsm*. Для этого следует перейти на лист *Загрузить криптограмму*, выделить ячейку **E3** ивставить текст криптограммы в адресную строку. Затем перейти в ячейку **B3**, задать значение периода 7, после чего загрузить криптограмму, нажав кнопку **Загрузить криптограмму**.

После этого можно осуществлять копирование символов криптограммы построчно с листа *Криптограмма* (столбцы **B-H**) и вставлять их в строку 2 на лист *Опред-е периода2*. Уже просмотренную и скопированную часть шифртекстана листе *Криптограмма* рекомендуется выделять цветом.

- Скопировать заполненную 2 строку (*Криптограмма*) листа *Опред-е периода2*, начиная со второго символа, и вставить ее в 3 строку (*Сдвиг = 1*) командой **Специальная вставка/Значения**. Последний, незаполненный символ строки 3 заполнить следующим символом из текста криптограммы.
- Заполнить строки 4-12, каждый раз копируя предыдущую строку со сдвигом на 1 символ влево, использовать команду **Специальная вставка/Значения**. Недостающие символы в конце строк дополнить следующими символами криптограммы так, чтобы все строки были одинаковой длины.
- Цветом (инструмент **Условное форматирование**) будут выделены символы в строках, совпадающие с символом первой строки в том же столбце. Для каждой строки вручную подсчитать количество совпадений (число выделенных ячеек в строке) и занести эти значения в ячейки **B16-B25**на листе*Опред-е периода2*.
- В ячейках **J16-L25**будут выведены значения коэффициентов автокорреляции, наибольшие из которых определяют сдвиг (сдвиги), кратные периоду гаммы (рис. 32).

Сдвиг	*Число совпадений*	*Коэффициент автокорреляции*
1	3	0,040
2	2	0,027
3	1	0,013
4	2	0,027
5	7	0,093
6	1	0,013
7	2	0,027
8	1	0,013
9	2	0,027
10	7	0,093

Рис. 32. Пример определения периода гаммы методом автокорреляции

На рис. 32 наибольшие значения коэффициента автокорреляции получены при величинах сдвига 5 и 10, откуда можно сделать вывод, что период гаммы (длина ключевого слова), скорее всего кратна (или равна) 5.

6. Проверить гипотезу о том, что период гаммы равен определенному в предыдущих тестах значению *M*(например, 5) с помощью метода индекса совпадений:

- Очистить данные, занесенные ранее на лист *Криптограмма* (столбцы **B-H**) – от этого зависит правильность подсчета индексов совпадений.
- Перейти на лист *Загрузить криптограмму*, вставить шифртекст в ячейку **E3** (если это не было сделано ранее), в ячейку **B3** занести проверяемое значение *M*(например, 5), затем нажать кнопку **Загрузить криптограмму**. Данные будут загружены на лист *Криптограмма*, каждый из полученных столбцов представляетпредполагаемую группу периода Y_i.
- Перейти на лист *Статистика период*. Для каждого столбца – группы периода Y_i в строке 38 приведен расчет индекса совпадения $I_C(Y_i)$. В случае, если период гаммы определен правильно, все значения индекса должны быть не менее 0,05, в этом случае они будут выделены цветом (табл. 16).

В примере значения всех индексов совпадения превышают 0,05, что свидетельствует о правильности определения периода гаммы.

Таблица 16

Пример значений индекса совпадений для групп периода в случае правильного определения *M*

Номер столбца –группы периода	**1**	**2**	**3**	**4**	**5**
Значение индекса совпадения	0,0571	0,0560	0,0634	0,0582	0,0723

- Если период гаммы определен неправильно, все или некоторые значения индексов совпадения окажутся близки к 1/33 ≈ 0,03 (не выделяются цветом). В этом случае гипотезу о значении периода гаммыследует пересмотреть.

Задание 2. Определить относительные сдвиги групп периода относительно первой группы. Определить ключевое слово и дешифровать криптограмму.

7. Определить относительные сдвиги между столбцами – группами периода:

- Перейти на лист *Статистика сдвиги* книги *шифр Виженера.xlsx*. В диапазоне **B4:AH11**приведены частоты встречаемости символов. Строка 4 содержит частоты букв в русском языке, приведенные к размеру групп периода. В строках 5-11 содержатся частоты групп периода рассматриваемой криптограммы. Распределения этих частот «сдвинуты» относительно русского языка и относительно друг друга.Для каждой группы периода цветом (инструмент **Условное форматирование**) выделены наибольшие значения частот.
- Определить сдвиг второй группы периода (*Столбец 2*) относительно первой (*Столбец 1*), для этого можно воспользоваться сопоставлением пиковых частот в строках 5 и 6 (рис. 33), либо сопоставлением начала/конца фрагмента алфавита с малыми частотами (длинный фрагмент без цветового выделения – рис. 34). Сопоставление начала фрагмента с малыми частотами более надежно.

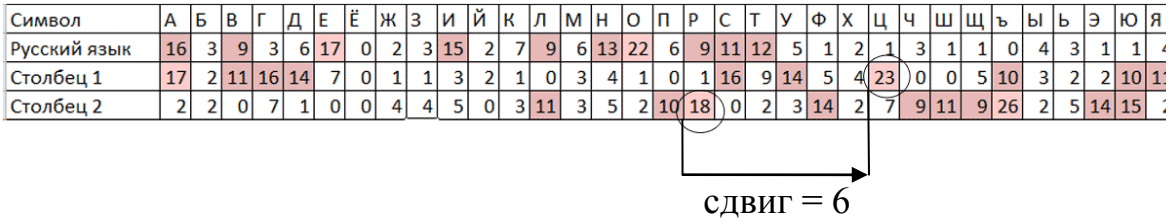


Рис. 33. Пример определения сдвига сопоставлением пиковых частот

Рис. 34. Пример определения сдвига по началу фрагмента с малыми частотами

По сути, требуется определить направление, в котором надо сместить алфавит в строке 6, чтобы распределение частот стало сходным с распределением частот в строке 5, а также величину этого смещения в позициях. При сдвиге вправо его величина считается положительной (рис. 33), а при сдвиге влево – отрицательной (рис. 34); в последнем случае значение следует взять по модулю L (L – число символов алфавита, для русского языка L=33). Для вычисления значения по модулюможно воспользоваться функцией Excel**ОСТАТ()**.

Для визуального определения величины сдвига можно использовать гистограммы частот на листе *Статистика сдвиги*. Приведены гистограммы распределения частот для первой группы периода, второй группы периода и второй группы периода с учетом определенного сдвига. При визуальном анализе также следует учитывать не только пиковые (наибольшие) значения частот, но и наличие достаточно длинного промежутка низких значений частот.

- После определения сдвига, его значение заносится в столбец **AI**(для *Столбца2*–в ячейку **AI6**). Затем можно сравнить гистограммы *Столбца1*и*Столбца2* с учетом определенного сдвига. Они должны быть схожими (рис. 35).

Рис. 35. Пример визуальной проверки правильности определения относительного сдвига групп периода

- После определения сдвига, в диапазоне **B15:AH20** отобразится «сдвинутое» распределение, в столбце **AI**– значение взаимного индекса совпадений (для *Столбца2* – в ячейке **AI15**). Если сдвиг определен правильно, то значения индекса взаимного совпадения будет выше 0,05.
- В случае, если значение индекса взаимного совпадения ниже 0,05, следует рассмотреть другую гипотезу о значении относительного сдвига и изменить его значение (для начала можно проверить значения, равные +/- 1 от определенного ранее).
- Аналогичным образом определить относительные сдвиги остальных столбцов – групп периодаотносительно *Столбца 1*.Для визуального определения и проверки правильности определения величины сдвига *Столбца 3*, *Столбца 4* и т.д. с помощью гистограмм, в гистограммах *Столбец 2* и *Столбец 2 сдвиг* следует изменить исходные данные (щелкнуть на гистограмме правой кнопкой мыши, выполнить команду **Выбрать данные** и выбрать соответствующую строку с данными).

8. Определение относительных сдвигов $S(i)$ позволяет составить систему уравнений для определения сдвигов $g(i)$ групп перио-

да Y_i, $i \neq$ 1относительно алфавита первой группы периода (*Столбца1*). Уравнения отображается в строках **25-28** на листе *Статистика сдвиги*.

Например, в случае $M = 5$ будут составлены 4 уравнения с 5 неизвестными $g(1)$, $g(2)$, …, $g(5)$.

$g(1)-g(2)= S(2)$,откуда	$g(2)=g(1)-S(2)$,
$g(1)-g(3)=S(3)$,	$g(3)=g(1)-S(3)$,
$g(1)-g(4)=S(4)$,	$g(4)=g(1)-S(4)$,
$g(1)-g(5)=S(5)$.	$g(5)=g(1)-S(5)$.

9. Теперь для получения ключевого словатребуется определить значение $g(1)$, то есть величину сдвига *Столбца1* относительно алфавита открытого текста. Поскольку возможно всего 33 варианта сдвига (от 0 до 32), сдвиг $g(1)$ нетрудно определить перебором всех вариантов первого символа ключевого слова.

- Подбор ключа отображается в строках **33-66**на листе *Статистика сдвиги*.Первый символ в каждой строке– предполагаемый первый символа ключевого слова, остальные символы ключевого слова вычисляются на основе полученных ранее из уравнений.
- Из полученных вариантов следует выбрать тот, который является осмысленным словом.

10. Зная ключ, провести дешифрование криптограммы:

- Для получения открытого текста на листе *Криптограмма* ввести найденное ключевое слово посимвольно в диапазон ячеек **K1:Q1**. Расшифровка текста содержится в столбцах **K-Q** (чтение текста осуществляется по строкам).
- Если в результате дешифрованияне был получен осмысленный текст, следует опробовать другой правдоподобный вариант ключевого слова из списка полученных (если таковой имеется).

11. Показать результат выполнения лабораторной работы преподавателю

ТЕМА 2. СИММЕТРИЧНЫЕ КРИПТОСИСТЕМЫ. СОВРЕМЕННЫЕ БЛОЧНЫЕ ШИФРЫ

Подавляющее большинство современных алгоритмов симметричного шифрования относятся к классу блочных шифров. Информация разбивается на блоки фиксированной длины (обычно, 64 или 128 битов), после чего эти блоки поочередно шифруются одним и тем же ключом.

Над шифруемым текстом выполняется некоторое преобразование с участием ключа шифрования, которое повторяется определенное число раз (раундов). Чаще всего исходный ключ шифрования также модифицируется для его дальнейшего использования в процессе преобразований. Такая модификация называется *расширением ключа*; в каждом раунде используется свой подключ – *ключ раунда*.

Таким образом, алгоритм шифрования можно логически разделить на две части: собственно шифрующее преобразование и процедура расширения ключа.

Примерами современных блочных шифров являются алгоритмы «Магма» и «Кузнечик» российского стандарта шифрования ГОСТ Р 34.12–2015, современный американский стандарт AES (шифр Rijndael), а также другие известные алгоритмы: DES, RC6, IDEAи др.

Практическая работа №6. Криптоанализ симметричного блочного шифра (слайдовая атака)

Описание шифра и метода криптоанализа

Существует множество видов криптоанализа, каждый из которых зависит, в наибольшей степени, от имеющейся у криптоаналитика информации. Универсальные методы криптоанализа, такие как метод полного перебора («грубой силы»),анализ на основе использования словарей, применимы ко многим шифрам, однако в большинстве случаев оказываются неэффективными. Эффективность других методов, таких как линейный и дифференциальный криптоанализ падает с ростом числа раундов криптоалгоритма. Однако существуют методы анализа, эффектив-

ность которых не зависит от числа раундов шифрующего преобразования и определяется особенностями ключа шифра.

К таким методам относится «слайдовая атака» («скользящая атака», *slideattack*), применимая к любому алгоритму при условии использования одинаковых раундовых ключей. Слайдовая атака использует степень самоподобия функции преобразования алгоритма шифрования, то есть использование одной и той же раундовой функции*F*, зависящей от одного и того же подключа в каждом раунде. Слайдовая атака может эксплуатировать как слабость процедуры формирования подключей, так и более общие структурные свойства шифра.

Обычная слайдовая атака рассчитана на анализ криптоалгоритмов, состоящих из *r*раундов, каждый из которых осуществляет *F*-преобразование входного текста, зависящее от одного и того же значения ключа *K*.

Идея заключается в том, что можно сопоставить один процесс зашифрования с другим таким образом, что один из процессов будет «отставать» от другого на один раунд (рис. 36).

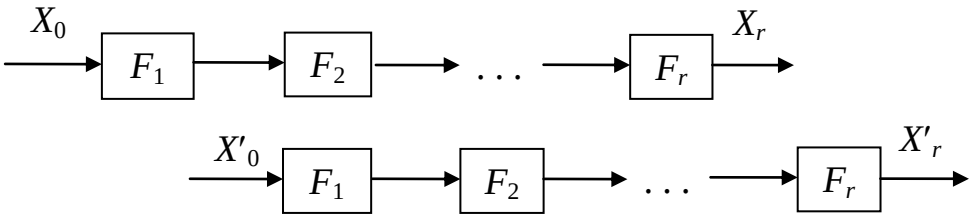


Рис. 36. Схема обычной слайдовой атаки

Пусть X_0 иX'_0 – некоторые открытые тексты, $X_j=F_j(X_{j-1})$, $X'_j=F_j(X'_{j-1})$, j=1,2,…,r. Предположим, что $X'_{j-1}=X_j$, тогда можно сказать, что $X'_j=F(X'_{j-1})=F(X_j)=X_{j+1}$, то есть для любого раунда выход первого процесса шифрования будет совпадать со входом второго процесса.Поэтому, если имеется некоторая пара значений, такая что выход первого раунда первого процесса шифрования является входом первого раунда второго процесса шифрования: $X'_0 = X_1$, то тогда выход последнего раунда первого процесса шифрования будет входом последнего раунда второго процесса шифрования: $X'_{r-1}=X_r$.

Пара открытых текстов и соответствующих им шифртекстов (P,C) (P',C')называется *слайдовой парой* в том случае, если $F(P)=P'$ и $F(C)=C'$.

Слайдовая атака проходит следующим образом. Получают пары *открытый текст–закрытый текст*(P_i,C_i) с помощью одного и того же ключа, среди которых ожидают найти хотя бы одну слайдовую пару. После того, как слайдовая пара найдена, могут быть найдены и некоторые биты ключа. Для определения оставшихся битов секретного ключа следует определить следующую слайдовую пару, и с ее помощью опять провести анализ, и так далее. Для определения секретного ключа достаточно найти несколько слайдовых пар.

В случае, когда речь идет об алгоритмах шифрования, построенных на схеме Фейстеля, раундовая функция преобразует только половину входного сообщения. Поэтому условие $F(X)=X'$можно легко проверить, сравнив левую часть сообщения Xи правую часть сообщения X'. Таким образом, сложность атаки может быть снижена до $2^{n/2}$открытых текстов, где n–длина блока алгоритма шифрования.

Для сети Фейстеля условие нахождения потенциальной слайдовой пары может быть сформулировано следующим образом: (P,C)образует слайдовую пару совместно с(P',C'), если левые половины текстов P' и Cравны соответственно правым половинам Pи C'.

Если существует возможность выбора открытых текстов, то для сети Фейстеля сложность анализа может быть снижена до $2^{n/4}$открытых текстов. В этом случае выбирается произвольное $n/2$-битовое значениеx, затем подбирается массив открытых текстов $P'_i=(x,y_i)$, которые будут различаться только случайновыбранной правой частьюy_i, и массив $P_j=(y_j,x)$, которые будут различаться только случайной левой частьюy_j.Отбор слайдовых пар производится по совпадению правой части криптограммы C'_iс левой частью C_j.

Слайдовые атаки применимы и для алгоритмов, в которых функция формирования подключей периодична, то есть один и тот же подключ повторяется через равное количество раундов. Известны эффективные слайдовые атаки для сети Фейстеля с

двухраундовымсамоподобием: слайдовая атака с использованием дополнений, которая основана на отборе открытых текстов, различия которых компенсируют различие подключей, слайдовая атака с петлей, основанная на сопоставлении процессов шифрования и расшифровки; комбинация этих методов позволяет проводить атаки на сети Фейстеля с четырехраундовымсамоподобием.

Самый простой вид слайдовой атаки обычно легко пресечь, избавившись от самоподобия в алгоритме шифрования. Более сложные варианты предполагают и более сложный анализ, однако против них гораздо сложнее защититься.

В практической работе рассматривается применение метода слайдовой атаки к учебному алгоритму, полученному на основе алгоритма S-DES (упрощенного DES). Алгоритм S-DESявляется блочным алгоритмом шифрования, построенным по схеме Фейстеля, с длиной открытого текста 8 бит.

В учебном алгоритме (рис.37), в отличие от S-DES, опущены начальная и конечная перестановки, так как они не влияют на криптографическую стойкость алгоритма. Для простоты в каждом раунде алгоритма используется один и тот же ключ и опускается процедура начального преобразования ключа (получение 8-битового ключа из исходного 10-битового). Поскольку метод криптоанализа на основе слайдовой атаки не зависит от числа раундов, учебный алгоритм включает 20 раундов шифрования, а не 2 как в S-DES.

На вход каждого (i-того) раунда учебного алгоритма подается 8-битовый текст. F-преобразованиюподвергается 4-битовое значение, представляющее собой правую половину R_iвходного блока, обозначим это значение как (b_1,b_2,b_3,b_4).

Первой операцией F-преобразования является операция перестановки с расширением E/P, в результате которой 4-битовое сообщение преобразуется к 8-битовому путем перестановки и повторения битов.

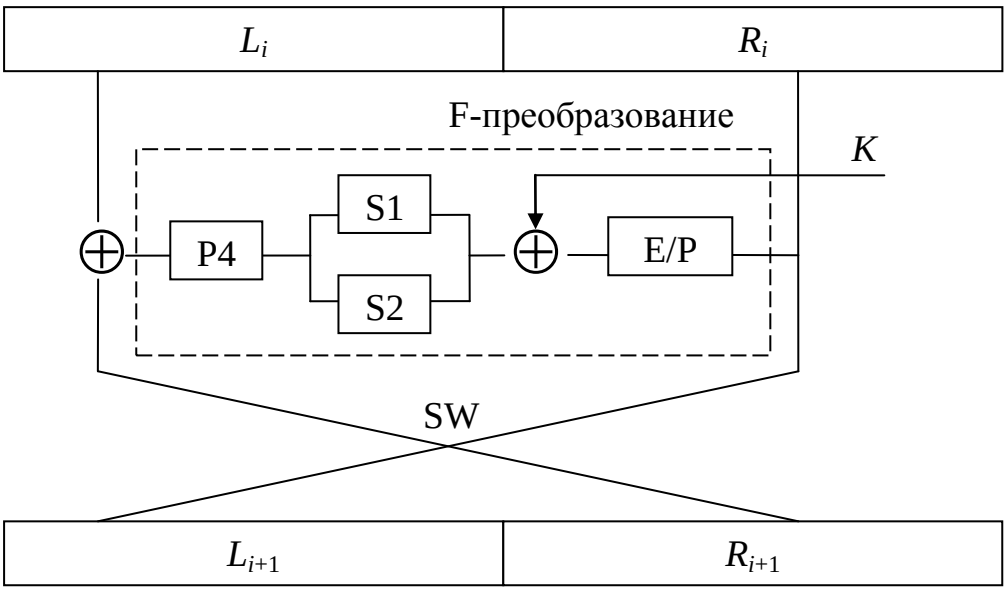


Рис. 37. Схема i-того раунда учебного алгоритма

Пусть операция E/P задана таблицей 17.Тогда результате применения операции E/P исходное 4-битовое значение (b_1,b_2,b_3,b_4) преобразуется к виду (b_4,b_1,b_2,b_3,b_2,b_3,b_4,b_1), где b_i – биты правого подблокаR_i входных данных.

Таблица 17

Пример перестановки с расширением E/P

4	1	2	3	2	3	4	1

К полученному 8-битовому значению применяется операция побитового сложения по модулю два (XOR) с 8-битным секретным ключом K=(k_1,k_2,k_3,k_4,k_5,k_6,k_7,k_8).

Полученная 8-битовая последовательность делится на две части: левая поступает на вход блока замены S1, правая – на вход блока S2. Выходами S-блоков являются двухбитовыепоследовательности.

Пусть работа S-блоков задана таблицей 18. S-блоки действую следующим образом: первый и четвертый биты входной последовательности рассматриваются как 2-битовые числа (от 00 до 11 в двоичном представлении или от 0 до 3 – в десятичном), определяющие строку, а второй и третий – столбец таблицы S-блока. Элемент, находящийся на пересечении соответствующих строки и столбца задает выход S-блока.

Таблица 18

S-блоки, десятичное представление

Блок S1

S1	**0**	**1**	**2**	**3**
0	1	0	3	2
1	3	2	1	0
2	0	2	1	3
3	3	1	3	1

Блок S2

S2	**0**	**1**	**2**	**3**
0	1	1	2	3
1	2	0	1	3
2	3	0	1	0
3	2	1	0	3

Для простоты использования на основе таблицы 18 можно построить сводную таблицу входов и выходов S-блоков (табл. 19).

Таблица 19

Входы и выходы S-блоков, двоичное представление

Вход	Выход S1	Выход S2
0000	01	01
0001	11	10
0010	00	01
0011	10	00
0100	11	10
0101	01	01
0110	10	11
0111	00	11
1000	00	11
1001	11	10
1010	10	00
1011	01	01
1100	01	01
1101	11	00
1110	11	00
1111	01	11

Из выходов блоков S1 и S2 получается общая 4-битовая последовательность, к которой применяется операция перестановки P4. Пусть эта операция задана таблицей 20. Результат перестановки P4 является выходом функции *F*.

Таблица 20

Таблица перестановки P4

2	4	3	1

К выходу функции применяется операция побитного XORс левой частью входного текста раунда.Поскольку алгоритм построен по схеме Фейстеля, между раундами шифрования используется функция SW, которая меняет местами первые и последние 4 бита (левую преобразованную и правую исходнуючасти) последовательности, чтобы в следующем раунде *F*-функция работала уже с другой четверкой битов.После последнего раунда перестановка не проводится.

Криптоанализ с помощью слайдовой атаки состоит в поиске слайдовых пар и сопоставлении входов и выходов первого и последнего раундов шифрования для этих пар.Это, в свою очередь, позволяет проанализировать изменение значений внутри раунда, чтобы получить возможные варианты ключа шифрования.

Для получения значений битов ключа в ходе анализа часть преобразований раунда выполняется в прямом направлении, а часть – в обратном (рис. 38).

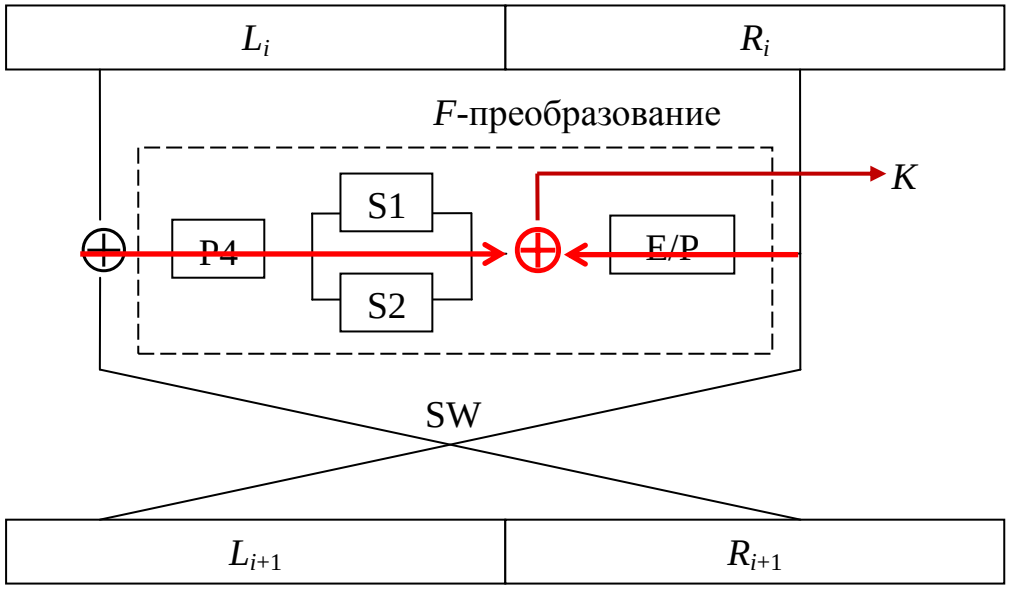


Рис. 38. Ход выполнение анализа раунда учебного алгоритма

Получив возможные значения на входе и выходе операции побитового XOR с ключом, можно восстановить возможные варианты ключа.

Анализ новых раундов и новых слайдовых пар позволяет сузить число возможных вариантов ключа. Если в ходе анализа

первых и последних раундов одной из отобранных пар не будет получено совпадений вариантов ключа, значит, такая пара не является слайдовой и должна быть исключена из рассмотрения.

Задание. Найти секретный ключ *K*учебного алгоритма с помощью с помощью обычной слайдовой атаки.

Указания к выполнению практической работы

Для выполнения практической работы рекомендуется использовать файл *Слайдовая атака.xlsm*. Параметры учебного алгоритма, определяемые вариантами задания приведены в Приложении 3.

Технология выполнения задания

Задание 1. Выбрать слайдовые пары для последующего анализа.

1. Изучить теоретическое описание учебного алгоритма и слайдовой атаки.
2. Открыть книгу *Слайдовая атака.xlsm*, в строке предупреждения включить выполнение макросов.
3. На листе *параметры шифра* следует ввести номер варианта, определяемые вариантом значения в таблицы: перестановки с расширением E/P, перестановки P4, S-блоков (в десятичном виде),маски. Варианты задания приведены в Приложении 3.

Провести криптоанализ алгоритма шифрования аналогично рассмотренному ниже примеру.

Пример. В качестве таблицE/P, P4, S-блоков используются таблицы 17, 18, 20, маска: 1101.

4. Перейти на лист *данные для анализа* и нажать кнопку **Получить данные для анализа**. Будут заполнены значениями таблицы *Отбор по левой половине текста* и *Отбор по правой половине текста*.

Хотя для проведения криптоанализа достаточно всего по $2^{8/4}$=4 текста со случайно выбранными правыми и со случайными левыми частями, программа выдаст все возможные варианты от-

крытых текстов с фиксированной (совпадающей с маской) левой частью и фиксированной правой частью (по 16).

5. Для проведения дальнейшего анализа следует отобрать из сгенерированных текстов слайдовые пары. Согласно определению слайдовой пары для сети Фейстеля, слайдовыми парами являются тексты *i* и *j*, для которых:
   a. левая половина X_Lоткрытого текста P_i совпадает с правой половиной X′_Rтекста P'_j, а также
   b. правая половина Y_R шифр-текста C_iсовпадает с левой половиной Y′_L шифр-текста C'_j.

   Условие (a) выполняется для всех сгенерированных текстов.

- Следует отобрать тексты, для которых выполнено условие (b). Части текстов, по которым следует проводить отбор, находятся в столбцах с выделением цветом. Для уменьшения перебора возможные слайдовые пары следует искать только среди текстов с неповторяющимися значениями Y_R (Y′_L).Для облегчения этого поиска повторяющиеся значения Y_R (Y′_L) выделены цветом (инструмент Excel**Условное форматирование**).

Проверку условия (b)желательно проводить среди невыделенных текстов. Рекомендуется выделять каждую из найденных слайдовых пар своим цветом (инструмент **Заливка**).

- Отобранные слайдовые пары занести в строки **23-…** на листе данные для анализа.

Для рассматриваемого примера выделены следующие возможные слайдовые пары, представленные на рис. 39.

ОТОБРАННЫЕ СЛАЙДОВЫЕ ПАРЫ

№	X_L	X_R	Y_L	Y_R
12	1101	1011	0101	0011
13	1101	1100	1000	1110
15	1101	1110	0110	1010
16	1101	1111	1100	1011
1	1101	0000	1110	1000
5	1101	0100	0111	0100

№	X'_L	X'_R	Y'_L	Y'_R
4	0011	1101	0011	1101
5	0100	1101	1110	0110
7	0110	1101	1010	0010
8	0111	1101	1011	0000
9	1000	1101	1000	1101
13	1100	1101	0100	1111

Рис. 39. Пример слайдовых пар

Задание 2. Провести анализ первых раундов слайдовой пары.

6. Занестипервую слайдовую пару в строку **3** на лист *анализ* книги *Слайдовая атака.xlsm*. Провести анализ первого раунда слайдовой пары.

- Пусть выбрана слайдовая пара 12, 4 (рис. 39). После занесения ее на лист анализ, схема сопоставления начальных раундов шифрования (левая схема) примет следующий вид (рис. 40).

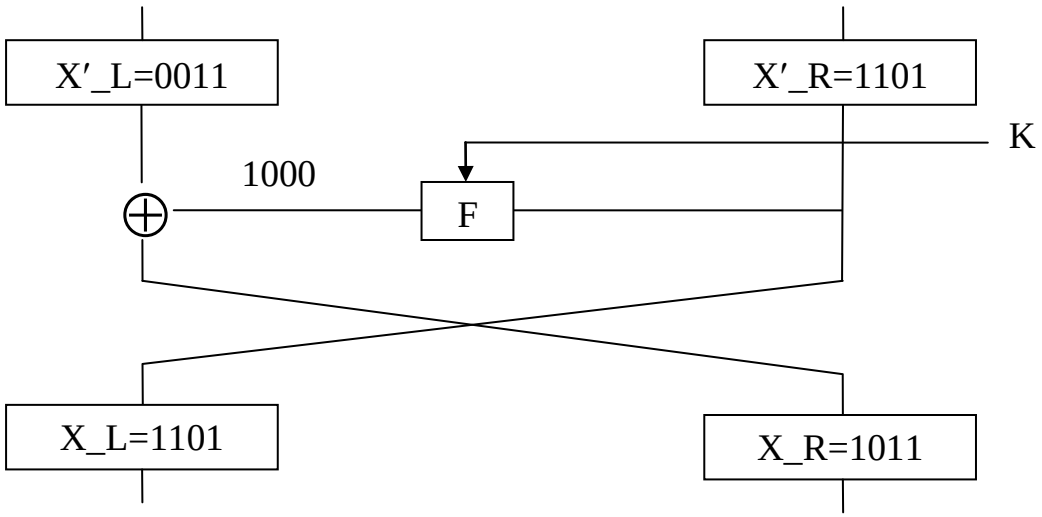


Рис.40. Данные для анализа первых раундов первой слайдовой пары

7. Вычислить выход *F*-функции:

- Зная X_R и X′_L, можно вычислить значение выхода *F*-функции как результат побитовой операцииXORэтих значений.

ЗАМЕЧАНИЕ: Операцию побитового XOR можно производить вручную, воспользоваться Калькулятором Windows (режим *Программист*) или использовать функцию MSExcel 2013 **БИТ.ИСКЛИЛИ** (группа Инженерные).

В примере X_R= 0011, X′_L= 1001, X_R ⊕ X′_L = 1000.

- Занести полученное значение в ячейку **D15**.

8. Так как перед выходом из *F*-функции производится перестановка P4,применить обратное преобразование – $P4^{-1}$к полученному в ячейке **D15** значению:

- Определить преобразование, обратное к P4, аналогично рассмотренному ниже примеру.

В примере перестановка P4 задана таблицей 17: 2, 4, 3, 1. Это означает, что при прямом преобразовании в первую позицию ставится второй бит, во вторую – четвертый бит, в третью – третий бит, в четвертую позицию – первый бит текста. Поэтому при обратном преобразовании значение в ячейке таблицы означает номер позиции, в которую надо переставить текущий бит (рис. 41).

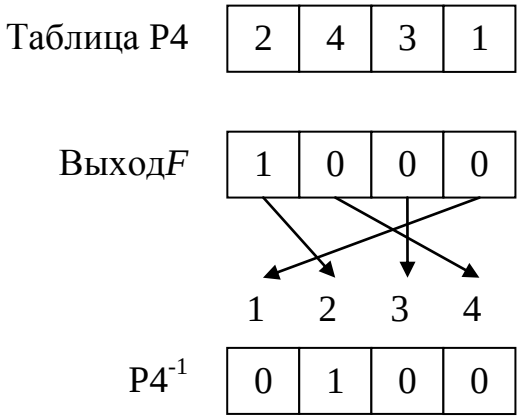


Рис. 41. Выполнение преобразования $P4^{-1}$

В примере получаем, что обратная перестановка $P4^{-1}$ может быть задана таблицей {4, 1, 3, 2}, а выходом $P4^{-1}$ при входе 1000 является значение 0100.

- Занести номера битов, задающих таблицу обратной перестановки $P4^{-1}$ в ячейку **D17**, а значения переставленных битов – в диапазон ячеек **A19:D19**.

9. Определить возможные входы S-блоков.

В примере получили, что на вход перестановки P4 поступило значение 0100, а значит, на выходе блока S1 получено значение 01, на выходе блока S2 – значение 00.

- Занести первые два бита полученного на выходе $P4^{-1}$ (входе P4) значения в ячейку **B21**, а последние два бита – в ячейку **D21**.
- Чтобы проанализировать, какими могут быть значения входов S-блоков, на основе двоичного представления S-блоков составляется таблица вида 19. Таблица 19 размещена в диапазоне **M3:O19**листа *анализ*.
- Определить значения 4-битовых входов S1 (первый столбец таблицы входов и выходов S-блоков) по значению выхода, за-

несенному в ячейку **B21** (второй столбец таблицы). Занести полученные значения в диапазон ячеек **B23-…**

- Определить значения 4-битовых входов S2 (первый столбец таблицы) по значению выхода, занесенному в ячейку **D21** (третий столбец таблицы). Занести полученные значения в диапазон ячеек **D23-…**

В примере на основе анализа таблицы 19, получаем, что возможными входами блока S1 могут быть 0000, 0101, 1011, 1100 и 1111. Возможными входами блока S2 являются значения 0011, 1010, 1101, 1110.

10. Определить значения входа *F*-функциии результата преобразованияE/P:

- Значение входа ***F***-функции совпадает с X′_R.

В примере значение входа ***F***-функции – 1101.

- После входа в***F***выполняется преобразование E/P (перестановка с расширением), согласно таблице 20. Для удобства последовательность номеров бит, определяющую преобразование E/P, можно занести на лист *анализ*, например, в ячейку **I15**, а результат этой операции – в ячейку **P15**.

Выполним E/P-преобразование для входа 1101. Получаем значение 11101011.

11. Определить возможные значения ключа шифрования.

На полученное в ячейке **P15**значение будет наложено с помощью операции побитового XORзначение секретного ключа*K*=(*K*1,*K*2), а результат подан на вход S-блоков.

Так, в рассматриваемом примере на вход блока S1 будет подано значение 1110⊕*K*1, а на вход блока S2 – 1011⊕*K*2.

- Занести первые 4 бита значения из ячейки **P15**в ячейку**G21,** а последние 4 бита – в ячейку**I21**, определяющие входы S-блоков.
- Возможные значения входов S1, занесенные в диапазон **B23-…,** и значение в ячейки **G21**позволяют определить возможные значения первой части *K*1 секретного ключа *K*. Для этой цели для каждого значения, определенного как вход S1-блока, надо провести XOR-операцию со значением **G21**. Занести результаты вычислений в диапазон ячеек **G23-…**листа*анализ*.

- Возможные значения входов S2 из диапазона **D23-…**и значение в ячейки **I21**позволяют определить возможные значения второй части *K*2секретного ключа *K*. Для этой цели для каждого значения, определенного как вход S2-блока, надо провести XOR-операцию со значением **I21**. Результаты вычислений следует занести в диапазон ячеек **I23-…** листа *анализ*.

Результаты вычисления ключа в рассматриваемом примере приведены на рис. 42.

входы S1		*K*1	входы S2		*K*2
0000	⊕1110	1110	0011	⊕1011	1000
0101	⊕1110	1011	1010	⊕1011	0001
1011	⊕1110	0101	1101	⊕1011	0110
1100	⊕1110	0010	1110	⊕1011	0101
1111	⊕1110	0001			

Рис. 42. Пример вычисления ключа (анализ первых раундов первой слайдовой пары)

12. Скопировать полученные значение ключа (а лучше результаты всех проведенных расчетов) на новый лист, пометив (на новом листе) для каких раундов и для какой слайдовой пары проведен анализ. При копировании использовать вставку значений (**Главная/Вставить/Вставить значения**).
13. Очистить результаты предыдущих вычислений на листе *анализ*, кроме слайдовой пары и последовательностей номеров бит, задающих операции $P4^{-1}$ и E/P (если они были занесены на лист в ходе предыдущего анализа).

Задание 3. Провести анализ последних раундов первой слайдовой пары.

14. Теперь следует провести анализ последних раундов шифрования для первой слайдовой пары (рис. 43):
- Исходные данные для анализа будут отображены на схемевходов и выходов последних раундов (правая схема). Дальнейший анализ проводится аналогично анализу первых раундов.

- Вычислить значение выхода *F*-функциина основании значенийY_L и Y′_R.

В примере получаем значение выхода *F*-функции– 1000). Анализ этого значения выхода *F* был проведен ранее, имеем возможные входы блока S1 – 0000, 0101, 1011, 1100 и 1111, возможные входы блока S2 – 0011, 1010, 1101, 1110.

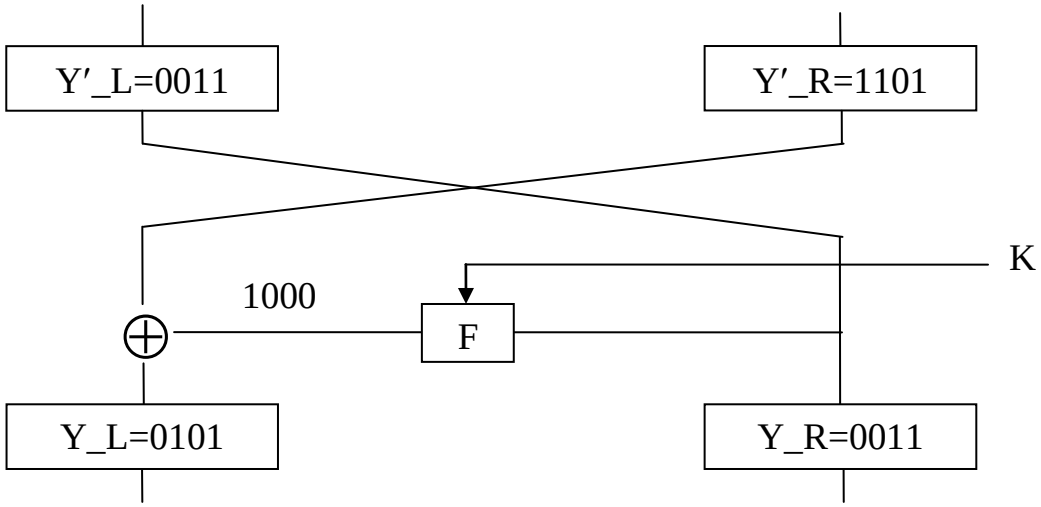


Рис. 43. Пример данных для анализа последних раундов первой слайдовой пары

- Определить значение входа *F*-функции (совпадает с Y′_L), в примере имеем – 0011.
- Выполнить преобразование E/P, в примере получено значение 10010110. Тогда на вход блока S1 подано значение 1001⊕*K*1, блока S2 – значение 0110⊕*K*2.
- Определить возможные значения ключа. В примере получены возможные значения *K*1: 1001, 1100, 0010, 0101, 0111. Возможные значения *K*2: 0101, 1100, 1011, 1000.

15. Скопировать полученные в ходе анализа значение ключа (а лучше результаты всех проведенных расчетов) на новый лист, пометив анализ каких раундов и для какой слайдовой пары был проведен. При копировании использовать вставку значений (**Главная/Вставить/Вставить значения**).
16. Очистить результаты предыдущих вычислений на листе *анализ*, кроме последовательностей номеров бит, задающих операции $P4^{-1}$ и E/P (если они были занесены на лист в ходе предыдущего анализа).

17. Сопоставить значения ключа,полученные при анализе первых и последних раундов слайдовой пары. Такое сопоставление обычно позволяет сократить число вариантов ключа, поскольку оставляются только совпадающие значения. Сопоставление производится отдельно для подключа *K*1 и подключа *K*2.

В примере сопоставление возможных значений подключей K1 и K2, полученные в ходе анализа первых и последних раундов первой слайдовой пары дает совпадение двух значений *K*1 и двух значений *K*2, что позволяет получить всего 4 возможных варианта искомого ключа (рис. 44).

*K*1	
первые,	последние раунды
1110	1001
1011	1100
0101	0010
0010	0101
0001	0111

*K*2	
первые,	последние раунды
1000	0101
0001	1100
0110	1011
0101	1000

Рис. 44. Пример сопоставления полученных значений подключей (первая слайдовая пара)

Таким образом, *K*1 может принимать значения 0101 или 0010, *K*2 –значения 1000 или 0101.

ЗАМЕЧАНИЕ: Варианты искомого ключа получаются как сочетания вариантов *K*1 с любым из вариантов *K*2. Таким образом, если имеется *m*вариантов *K*1 и *k*вариантов *K*2, то можно определить *mk*различных вариантов искомого ключа.

Для дальнейшего сужения круга значений ключей следует проанализировать другие слайдовые пары.

ЗАМЕЧАНИЕ: Если при анализе не найдено совпадений среди вариантов значений *K*1 или *K*2, значит, пара не является слайдовой (или в ходе анализа допущены вычислительные ошибки), и следует перейти к анализу следующей пары.

Задание 4.Провести анализ следующей слайдовой пары.

18. Занести на лист *анализ* значения текстов второй слайдовой пары из отобранных на листе данные для *анализа*. Провести анализ пары аналогично заданиям 2 и 3.

- В примере в качестве второй слайдовой пары выбрана пара 13, 5(рис. 39).
- При анализе первых раундов второй слайдовой пары, получаем: выход *F* – 1000, вход – 1101. Это совпадает с данными первых раундов первой слайдовой пары (задание 2) и не даст новых результатов.
- Анализ последних раундов второй слайдовой пары (рис.45) дает значение выхода *F*-функции – 1110. После обратного преобразования $P4^{-1}$получаем выход S-блоков: 0111, выход S1 – 01, выход S2 – 11.
- С помощью таблицы 19, получены возможные входы S1: 0000, 0101, 1011, 1100 и 1111; возможные входы S2: 0110, 0111, 1000, 1111.
- Входом *F*-функции является значение 1110. E/Pпреобразование дает значение 01111101. На вход блока S1 подано значение 0111⊕*K*1, блока S2 – значение 1101⊕*K*2.

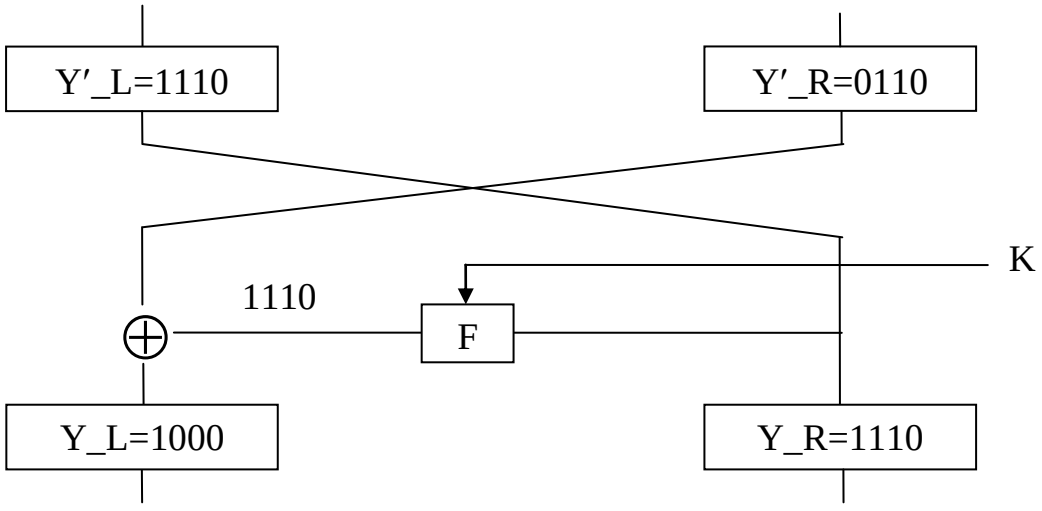


Рис. 45. Пример данных для анализа последних раундов второй слайдовой пары

- Возможными значениями *K*2 являются: 1011, 1010, 0101, 0010. Сравнение с результатами анализа первых раундов этой слай-

довой пары (рис. 42) даетодносовпадение: 0101. Таким образом, подключ*K*2 однозначно определен.

- Поскольку найдены совпадающие значения для обеих частей ключа, пара может быть признана слайдовой.

19. Проверить наличие совпадающих значений ключа с результатами анализа предыдущих слайдовых пар.

- В примере со значениями *K*1, полученными в ходе анализа первой слайдовой пары (рис. 44),совпадаеттолько одно значение – 0010. Таким образом, подключ*K*1 однозначно определен: *K*1 = 0010.
- Найденное значение *K*2 = 0101 совпадает с одним из значений, полученных при анализе первой слайдовой пары (рис. 44).
- Таким образом, получили однозначно определенный истинный ключ *K* = *K*1 &*K*2 = 00100101.

20. Для проверкиполученного значения ключа следует ввести его значениев ячейку **K21** листа *анализ* и нажать кнопку**Проверить ключ**. В случае правильно определенного значения будет выдано подтверждение о верности значения секретного ключа (*ключ верен*).

ЗАМЕЧАНИЕ: Если анализ 3-4 слайдовых пар не позволяет однозначно определить значение секретного ключа, следует поочередно проверить все отобранные в ходе анализа варианты секретных ключей и выбрать правильный.

21. Поскольку в рассматриваемом примере значение секретного ключа найдено верно, анализ остальных слайдовых пар можно не проводить.

22. Продемонстрировать преподавателю полученное значение секретного ключа *K*, правильность которого подтверждена с помощью файла *Слайдовая атака.xlsm*.

Практическая работа №7. Изучение шифра AES

Описание алгоритма шифрования

Алгоритм AESиспользует для шифрования 128-битовые блоки текста и ключи трех фиксированных размеров: 128, 192 и 256 битов.

Алгоритм AESпредставляет блок данных в виде двумерного массива байтов размером 4×4.Запись байтов в массив производится по столбцам. Все операции производятся над отдельными байтами массива, а также над независимыми столбцами и строками.

Для шифрования вкаждомраундеалгоритмаиспользуютсяследующиепреобразования: *SubBytes*, *ShiftRows*, *MixColumns*, *AddRoundKey* (рис.46).

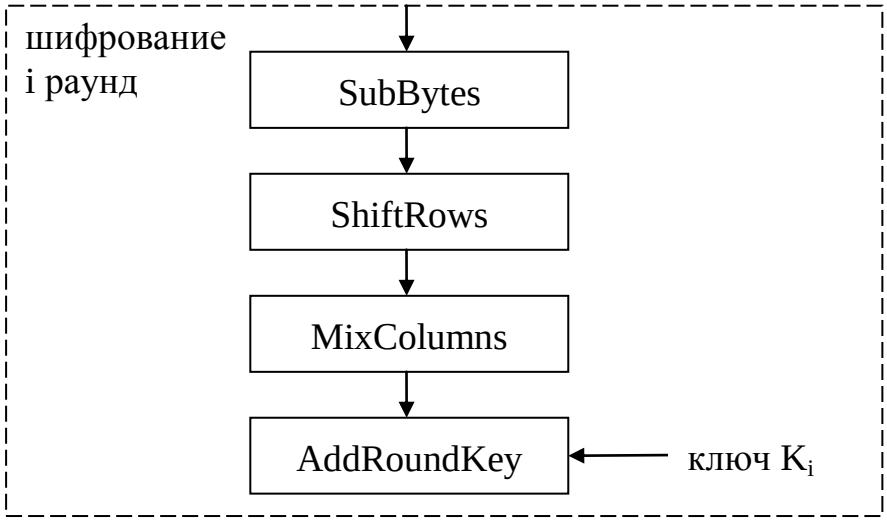


Рис. 46. Раунд шифрования алгоритма AES

Операция *SubBytes*представляет собой табличную замену каждого байта массива данных. Замена производится в соответствии с табл. 21. Байты представляются двухразрядными шестнадцатеричными числами. Первый шестнадцатеричный разряд определяет строку, а второй – столбец таблицы 21, определяющие новое значение байта.

Примеры операции SubBytes: 7C → 10, F4 →BF.

Таблица 21

Таблица замен операции SubBytes

	0	**1**	**2**	**3**	**4**	**5**	**6**	**7**	**8**	**9**	**A**	**B**	**C**	**D**	**E**	**F**
0	63	7C	77	7B	F2	6B	6F	C5	30	01	67	2B	FE	D7	AB	76
1	CA	82	C9	7D	FA	59	47	F0	AD	D4	A2	AF	9C	A4	72	C0
2	B7	FD	93	26	36	3F	F7	CC	34	A5	E5	F1	71	D8	31	15
3	04	C7	23	C3	18	96	05	9A	07	12	80	E2	EB	27	B2	75
4	09	83	2C	1A	1B	6E	5A	A0	52	3B	D6	B3	29	E3	2F	84
5	53	D1	00	ED	20	FC	B1	5B	6A	CB	BE	39	4A	4C	58	CF

6	D0	EF	AA	FB	43	4D	33	85	45	F9	02	7F	50	3C	9F	A8
7	51	A3	40	8F	92	9D	38	F5	BC	B6	DA	21	10	FF	F3	D2
8	CD	0C	13	EC	5F	97	44	17	C4	A7	7E	3D	64	5D	19	73
9	60	81	4F	DC	22	2A	90	88	46	EE	B8	14	DE	5E	0B	DB
A	E0	32	3A	0A	49	06	24	5C	C2	D3	AC	62	91	95	E4	79
B	E7	C8	37	6D	8D	D5	4E	A9	6C	56	F4	EA	65	7A	AE	08
C	BA	78	25	2E	1C	A6	B4	C6	E8	DD	74	1F	4B	BD	8B	8A
D	70	3E	B5	66	48	03	F6	0E	61	35	57	B9	86	C1	1D	9E
E	E1	F8	98	11	69	D9	8E	94	9B	1E	87	E9	CE	55	28	DF
F	8C	A1	89	0D	BF	E6	42	68	41	99	2D	0F	B0	54	BB	16

Операция *ShiftRows* выполняет циклический сдвиг влево последних трех строк массива данных (рис.47).

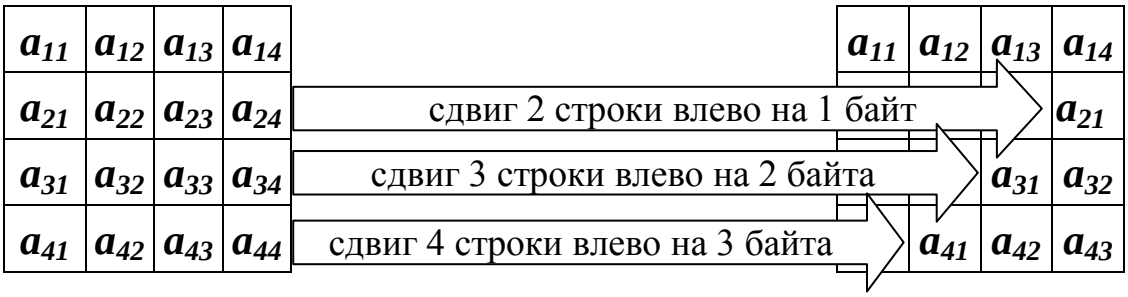


Рис. 47. Операция ShiftRows

Пример операции ShiftRows:

D4	E0	B8	1E
27	BF	B4	41
11	98	5D	52
AE	F1	E5	30

$\rightarrow$

D4	E0	B8	1E
BF	B4	41	27
5D	52	11	98
30	AE	F1	E5

Операция *MixColumns* производится над каждым из столбцов массива данных. Выполняется умножение столбца, который рассматривается как полином в конечном поле Галуа $GF(2^8)$ на фиксированный полином $g(x) = 3x^3 + x^2 + x + 2$. Умножение выполняется по модулю $x^4 + 1$.

Элементы a_kстолбца рассматриваются как коэффициенты полинома третьей степени, в результате, новые значения b_kстолбца байтов могут быть вычислены по формуле:

$$\begin{pmatrix} b_1 \\ b_2 \\ b_3 \\ b_4 \end{pmatrix} = \begin{pmatrix} 02 & 03 & 01 & 01 \\ 01 & 02 & 03 & 01 \\ 01 & 01 & 02 & 03 \\ 03 & 01 & 01 & 02 \end{pmatrix} \begin{pmatrix} a_1 \\ a_2 \\ a_3 \\ a_4 \end{pmatrix},$$

или

$$b_1 = 02 \bullet a_1 \oplus 03 \bullet a_2 \oplus a_3 \oplus a_4$$
$$b_2 = a_1 \oplus 02 \bullet a_2 \oplus 03 \bullet a_3 \oplus a_4$$
$$b_3 = a_1 \oplus a_2 \oplus 02 \bullet a_3 \oplus 03 \bullet a_4$$
$$b_4 = 03 \bullet a_1 \oplus a_2 \oplus a_3 \oplus 02 \bullet a_4,$$

где 02, 03 – двузначные шестнадцатеричные числа, a_k–элементы исходного столбца, представленные как элементы из $GF(2^8)$. Каждое значение a_k может быть представлено в виде восьмиразрядного двоичного числа (8-битовой строки), которому соответствует полином 7 степени, коэффициенты которого (0 или 1) определяются значениями соответствующих бит.

Например, шестнадцатеричному числу 10_{16} соответствует двоичное число 00010000_2 и полином $0 \cdot x^7+0 \cdot x^6+0 \cdot x^5+1 \cdot x^4+0 \cdot x^3+ +0 \cdot x^2+0 \cdot x+0 \cdot 1 = x^4$.

Числу $BF_{16} = 10111111_2$ соответствует полином $1 \cdot x^7+0 \cdot x^6+ +1 \cdot x^5+1 \cdot x^4+1 \cdot x^3+1 \cdot x^2+1 \cdot x+1 \cdot 1 = x^7+x^5+x^4+x^3+x^2+x+1$.

Операция $\oplus$ – сложение в поле $GF(2^8)$, которое определяется как побитовая операция XOR.

Например, в шестнадцатеричном виде: $10 \oplus BF = AF$, в полиномиальном виде: $x^4+x^7+x^5+x^4+x^3+x^2+x+1= x^7+x^5+x^3+x^2+x+1$, в двоичном виде: 00010000+10111111=10101111.

Операция $\bullet$ – умножение в поле $GF(2^8)$ по модулю $m(x) = x^8+x^4+x^3+x+1$.В отличие от сложения, в $GF(2^8)$простой операции умножения на уровне байтов не существует.

Например, $BF \bullet 10=05$, или, в полиномиальном представлении:

$(x^7+x^5+x^4+x^3+x^2+x+1) \cdot x^4=x^{11}+x^9+x^8+x^7+x^6+x^5+x^4=$
$(x^8+x^4+x^3+x+1)(x^3+x+1)+x^2+1=$
$(x^{11}+x^7+x^6+x^4+x^3+x^9+x^5+x^4+x^2+x+x^8+x^4+x^3+x+1)+x^2+1=$
$x^{11}+x^9+x^8+x^7+x^6+x^5+x^4$.

Далее следует взять остаток от деления полученного результата на $m(x)$, чтобы получить элемент поле $GF(2^8)$, то есть сте-

пень результирующего результата, не превышающую 7. В примере получимx^2+1 (000000101 в двоичном представлении или 05 в шестнадцатеричном).

Пример операции *MixColumns*:

D4		04
BF	→	66
5D		81
30		E5

Операция *AddRoundKey*выполняет наложение на массив данных материала ключа, а именно для каждого байта массива данных выполняется побитовая операция XORс соответствующим байтом ключа раунда.

$b_{kl} = a_{kl} \oplus Ki_{kl}$

Например, если первый байт массива данных – 04, а первый байт ключа раунда – F5, то результат *AddRoundKey* для первого байта составитF1.

Количество раундов алгоритма AESопределяется длиной ключа (табл.22).

Таблица 2

Число раундов AES

Размер ключа в битах	128	192	256
Количество раундовN	10	12	14

Перед первым раундом выполняется предварительное наложение на открытый текст материала ключа с помощью операции *AddRoundKey*.

Последний раунд отличается от предыдущих тем, что в нем не выполняется операция *MixColumns*.

Рассмотрим далее *процедуру расширения ключа*только для алгоритмаAES с 128-битовыми ключами (AES-128).

Формируются константы раунда *RCon*– 4-х байтовые столбцы, первый байт которых равен $2^{i-1} \bmod 256$, *i*–номер раунда, а остальные байты – нулевые (табл.23).

Таблица 23

Константы раунда *RCon*

1	**2**	**3**	**4**	**5**	**6**	**7**	**8**	**9**	**10**
01	02	04	08	10	20	40	80	1B	36
00	00	00	00	00	00	00	00	00	00
00	00	00	00	00	00	00	00	00	00
00	00	00	00	00	00	00	00	00	00

Ключ *Ki*раунда *i*– массив байтов размером 4×4. Обозначим столбцы этой таблицы через Ti_k. Ключ *Ki*раунда *i*формируется на основании ключа предыдущего раунда*Ki*-1 и константы раунда$RCon_i$.

Ti_1 формируется следующим образом:

$Ti_1 = SubBytes(RotWord(Ti\text{-}1_4))\oplus RCon_i \oplus Ti\text{-}1_1$.

- К первому столбцу $Ti\text{-}1_4$ ключа предыдущего раунда *Ki*-1 применяется преобразование *RotWord*, заключающееся в циклическом сдвиге на 1 байт влево.
- К результату операции RotWord применяется операция *SubBytes* в соответствии с таблицей 21.
- К результатуприменяется операция побитовогоXOR с константой раунда и с $Ti\text{-}1_1$.

Пример вычисления первого столбца ключа 2 раунда:

*K*1 – ключ предыдущего раунда

$T1_1$			$T1_4$	*RotWord*$T1_4$	*SubBytes*	$\oplus$ $RCon_2$	$\oplus$ $T1_1$	$T2_1$
F5	01	AE	88	3B	E2	E0		15
D5	D2	12	3B	→ BB	→ EA	→ EA	→	3F
9A	13	C3	BB	36	05	05		9F
32	7A	C7	36	88	C4	C4		F6

Ti_k, $k\neq1$ получаются применением к предыдущему столбцу ключа $Ti_{k\text{-}1}$ операции побитового XOR с соответствующим столбцом $Ti\text{-}1_k$ ключа предыдущего раунда: $Ti_k = Ti_{k\text{-}1}\oplus Ti\text{-}1_k$.

В рассмотренном выше примере, следующие столбцы ключа 2 раунда вычисляются как:

$T2_1 \oplus T1_2$			$T2_2 \oplus T1_3$		$T2_3 \oplus T1_4$		$T2_4$
15	01		14	AE	BA	88	32
3F	D2	→	ED	12	→ FF	3B	→ C4
9F	13		8C	C3	4F	BB	F4
F6	7A		8C	C7	4B	36	7D

Получаемые значения 2, 3 и 4 столбца ключа выделены цветом.

Для расшифрования вкаждомраундеалгоритмаиспользуютсяпреобразования: *InvShiftRows*, *InvSubBytes*, *AddRoundKey*, *InvMixColumns* (рис.48).

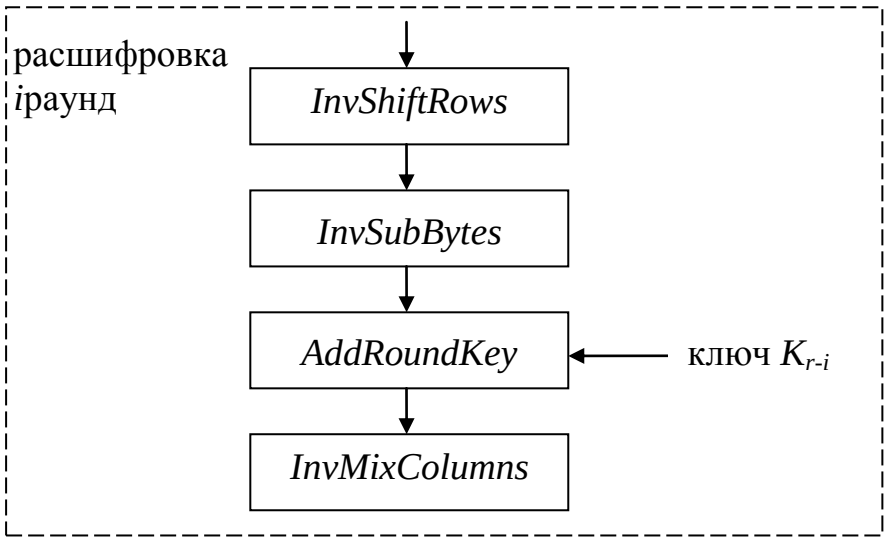


Рис. 48. Раунд расшифрования алгоритма AES

Аналогично процедуре шифрования перед первым раундом расшифрования выполняется операция *AddRoundKey*, накладывающая на шифр-текст значения ключа последнего (*r*) раунда шифрования.Последний раунд расшифровки не содержит операцию *InvMixColumns*.

Аналогично процедуре шифрования перед первым раундом расшифрования выполняется операция *AddRoundKey*, накладывающая на шифр-текст значения ключа последнего (*r*) раунда шифрования.Последний раунд расшифровки не содержит операцию *InvMixColumns*.

Операция *InvShiftRows*производит циклический сдвиг вправо трех последних строк массива данных на то же количество байтов, на которое выполнялся сдвиг операцией *ShiftRows*при шифровании.

Операция *InvSubBytes*производит побайтно обратную *SubBytes*табличную замену в соответствие с таблицей 24.

Таблица 24

Таблица замен операции *InvSubBytes*

	0	**1**	**2**	**3**	**4**	**5**	**6**	**7**	**8**	**9**	**A**	**B**	**C**	**D**	**E**	**F**
0	52	09	6A	D5	30	36	A5	38	BF	40	A3	9E	81	F3	D7	FB
1	7C	E3	39	82	9B	2F	FF	87	34	8E	43	44	C4	DE	E9	CB
2	54	7B	94	32	A6	C2	23	3D	EE	4C	95	0B	42	FA	C3	4E
3	08	2E	A1	66	28	D9	24	B2	76	5B	A2	49	6D	8B	D1	25
4	72	F8	F6	64	86	68	98	16	D4	A4	5C	CC	5D	65	B6	92
5	6C	70	48	50	FD	ED	B9	DA	5E	15	46	57	A7	8D	9D	84
6	90	D8	AB	00	8C	BC	D3	0A	F7	E4	58	05	B8	B3	45	06
7	D0	2C	1E	8F	CA	3F	0F	02	C1	AF	BD	03	01	13	8A	6B
8	3A	91	11	41	4F	67	DC	EA	97	F2	CF	CE	F0	B4	E6	73
9	96	AC	74	22	E7	AD	35	85	E2	F9	37	E8	1C	75	DF	6E
A	47	F1	1A	71	1D	29	C5	89	6F	B7	62	0E	AA	18	BE	1B
B	FC	56	3E	4B	C6	D2	79	20	9A	DB	C0	FE	78	CD	5A	F4
C	1F	DD	A8	33	88	07	C7	31	B1	12	10	59	27	80	EC	5F
D	60	51	7F	A9	19	B5	4A	0D	2D	E5	7A	9F	93	C9	9C	EF
E	A0	E0	3B	4D	AE	2A	F5	B0	C8	EB	BB	3C	83	53	99	61
F	17	2B	04	7E	BA	77	D6	26	E1	69	14	63	55	21	0C	7D

Операция *AddRoundKey* выполняет наложение на массив данных ключа раунда, однако использование ключей раундов при расшифровке производится в обратную сторону (от *r*-1до 0). Таким образом, в *i*раунде расшифрования используется ключ *r-i*раунда шифрования *–Kr-i*.

Операция *InvMixColumns*выполняет умножение каждого столбца массива данных аналогично прямой операции *MixColumns* на полином $g^{-1}(x) = Bx^3 + Dx^2 + 9x + E$.

Задание

A. Выполнить «в ручную» операцию *MixColumns*для заданного столбца байтов. Выбор столбца байтов для преобразования производится из таблицы 25 в соответствии с номером варианта.

B. Зашифровать с помощью алгоритма AES-128заданный фрагмент на заданном ключе.

C. Дешифровать заданную криптограмму, полученную шифром AES-128 на ключе из задания ***B***, получить открытый текст сообщения.

Выбор блока открытого текста для шифрования, ключа и криптограммы для расшифровывания производится из таблицы 25 в соответствии с номером варианта.

Таблица 25

Варианты задания

1.	Столбец байтов AD 41 87 AC	Блок текста: 38 AD C5 0F AC 3F C1 1B 4C 8E B2 80 57 90 23 2C Ключ: A4 83 01 77 CA 0F 68 EE AF 66 AB 45 A7 7B 89 08 Криптограмма: AB 0A 78 15 33 CC 17 49 18 74 F4 AA 2C 92 9F 07
2.	Столбец байтов 47 33 8D E5	Блок текста: 73 46 8E DE 88 B0 36 95 56 D3 59 B9 00 54 FB 89 Ключ: 87 24 31 2B 4D 2B 59 C5 E2 4D F2 80 45 36 7B 88 Криптограмма: E3 9A 65 4D 83 01 94 DE A9 D5 4F BE 20 13 37 9A
3.	Столбец байтов 24 C6 24 0F	Блок текста: DC 9F 26 D8 66 2F C2 C1 C8 BD 2F 25 3E B8 B2 DE Ключ: 86 05 F5 45 CB 2E AC 80 29 63 5E 00 6C 55 25 88 Криптограмма: AF 01 8D DD B8 BF 03 D6 51 00 BB BA 25 96 C2 5E
4.	Столбец байтов BD 8C 58 3A	Блоктекста: A6 8B 6B EE 75 D1 28 5A D9 29 A7 48 7F 1A 47 C5 Ключ: 72 3A 31 15 B9 14 9D 95 90 77 C3 95 FC 22 E6 1D Криптограмма: 5F A4 49 D6 02 F0 20 87 F6 90 D3 A8 13 1A F3 4B
5.	Столбец байтов 00 41 87 AC	Блок текста: 82 20 62 4C E4 0B 86 7C C6 22 73 70 62 84 97 DD Ключ: F1 84 95 A5 48 A0 08 30 D8 D7 CB A5 24 F5 2D B8 Криптограмма: C9 5A DB 3B 19 43 E6 0D 2E 27 F1 41 D9 47 5C 9C

6.	Столбец байтов 29 33 8D E5	Блок текста: E4 BA F0 AD 95 5E 82 C2 F0 28 5F B7 BC B7 4B 0C Ключ: 37 6C F9 93 7F CC F1 A3 A7 1B 3A 06 83 EE 17 BE Криптограмма: FB D4 F2 68 43 D6 F8 08 AB F9 B3 5D CA C3 8E F0
7.	Столбец байтов 2A C6 24 F0	Блоктекста: 3C 01 54 58 51 D5 36 6B ED 74 73 E6 F4 E4 40 BF Ключ: 5F 9C 57 7F 20 50 A6 DC 87 4B 9C DA 04 A5 8B 64 Криптограмма: 36 FF F9 82 E2 BC 3E DB 86 C1 99 CB B8 67 9D 4A
8.	Столбец байтов E9 8C 85 CA	Блок текста: 10 F3 A2 C5 57 CF 49 FB C9 D3 61 92 6E 63 CB C0 Ключ: D9 A1 14 8D F9 F1 B2 51 7E BA 2E 8B 7A 1F A5 EF Криптограмма: 2D 26 DF 69 B4 01 66 43 A6 B7 B8 27 D4 A3 1C 24
9.	Столбец байтов 14 9F 7D DE	Блок текста: 86 F4 44 C2 5C E1 40 92 FC CB 6D 28 3C 98 90 FD Ключ: 19 A6 CB 57 E0 57 79 06 9E ED 57 8D E4 F2 F2 62 Криптограмма: D3 70 BA D5 8B 86 3F 46 54 A3 C3 D5 FE 08 53 93
10.	Столбец байтов 35 66 8B 3F	Блок текста: 98 4C FA B5 40 88 61 C2 DA 2E F9 FE 93 D3 D6 A8 Ключ: CF 5C 09 49 4A 06 68 CE D7 47 94 A5 FE F2 C7 CE Криптограмма: 96 62 59 51 53 34 06 A7 99 3F 54 3A 33 F3 E2 10
11.	Столбец байтов A1 7B E9 89	Блоктекста: 4F FB FF 41 28 B9 C3 A3 DB 8E 90 5D 72 ED 21 1A Ключ: 44 9A 82 F2 0E 9C EA 3C D9 DB 7E 99 27 29 B9 57 Криптограмма: CE 6F 00 C6 4A 36 FF B8 E7 D3 E7 A7 A7 09 46 80

12.	Столбец байтов 05 A3 D3 62	Блок текста: 6F B0 6D 0C 33 05 B8 99 53 F8 A0 1E D4 49 7E 2E Ключ: E5 CC D9 3E EB 50 33 02 32 8B 4D 9B 15 A2 F4 CC Криптограмма: 71 6C 85 E2 21 8A 62 22 8D 12 37 34 63 BA 3A 12
13.	Столбец байтов 95 9F D7 ED	Блоктекста: C2 B8 92 34 B8 E1 55 09 6C BA CA 77 A9 F9 15 7B Ключ: D7 73 92 67 3C 23 A1 65 0E A8 EC FE 1B 0A 18 32 Криптограмма: 5D 07 C0 8A CD A7 4F B3 5F 1B 39 8C E9 F0 FA CD
14.	Столбец байтов 05 66 B8 F3	Блоктекста: DB 00 C4 C6 A2 4F A3 4C 50 01 B8 DA 1B EB 40 3D Ключ: A0 DE B1 CB 9C FD 10 AD 92 55 FC 53 89 5F E4 61 Криптограмма: AF 91 26 B5 6D BE 5E D2 9E F2 62 17 61 31 85 B2
15.	Столбец байтов 30 7B 0E 98	Блоктекста: 15 E7 3D BE D1 90 83 E5 21 C2 05 01 34 7F C5 4C Ключ: 4F 87 5E 6F D3 4A 4E C2 41 1F B2 91 CB 40 56 F0 Криптограмма: DB AE 22 2E 3D AC 5C F8 DE 46 2A BF DD 8B E4 D8
16.	Столбец байтов F2 A3 3D 26	Блоктекста: A4 83 01 77 CA 0F 68 EE AF 66 AB 45 A7 7B 89 08 Ключ: E6 6E E7 1F E8 03 32 D3 33 CA 38 DE C8 B1 93 51 Криптограмма: 30 63 8A EB 86 86 93 91 18 C2 21 66 CD 38 10 FA
17.	Столбец байтов C9 80 2E 8C	Блок текста: 87 24 31 2B 4D 2B 59 C5 E2 4D F2 80 45 36 7B 88 Ключ: 6E 70 D9 89 05 87 8F 66 BB D9 4F 8B 75 26 54 8C Криптограмма: 08 75 94 2C 3C 2C C5 C4 7A 93 4D 02 0F 1D C3 C5

18.	Столбец байтов 03 2D 89 2B	Блок текста: 86 05 F5 45 CB 2E AC 80 29 63 5E 00 6C 55 25 88 Ключ: 43 EB E9 A5 44 1A AB 53 A4 E6 6D B2 0F 07 A2 FB Криптограмма: 96 6B 6E 3B EA FC 95 20 F3 AE 8C D1 EE 0C BB 92
19.	Столбец байтов 29 D5 F5 06	Блок текста: 72 3A 31 15 B9 14 9D 95 90 77 C3 95 FC 22 E6 1D Ключ: D4 F2 93 9A CD 05 63 95 03 13 06 24 BF 0B F5 23 Криптограмма: BE E6 73 E3 7C B4 86 C7 0C 3A 00 0F 96 57 F7 73
20.	Столбец байтов B5 7D 0D 16	Блоктекста: F1 84 95 A5 48 A0 08 30 D8 D7 CB A5 24 F5 2D B8 Ключ: C5 C9 F4 94 7C 32 63 A7 13 75 E2 0A ED 7B 06 A7 Криптограмма: 08 1D B4 55 80 1B ED AF 21 4C 34 5A 7B EA 93 EC
21.	Столбец байтов 2D 80 E9 C8	Блоктекста: 37 6C F9 93 7F CC F1 A3 A7 1B 3A 06 83 EE 17 BE Ключ: 61 C3 8B 03 CE D6 D4 F1 A6 43 9C 5A B1 77 E7 8F Криптограмма: 2C 97 CC 7E A3 3E 7E 98 9C B0 35 19 40 7A 95 6D
22.	Столбец байтов EA 2D 19 B5	Блоктекста: 5F 9C 57 7F 20 50 A6 DC 87 4B 9C DA 04 A5 8B 64 Ключ: BB 1C A2 D6 7A 7C 99 66 AC 9C 58 97 30 87 8E AC Криптограмма: F1 00 63 F8 4B DB 3F CE 14 28 3D AF BC 62 B0 52
23.	Столбец байтов EE F5 3E 60	Блоктекста: D9 A1 14 8D F9 F1 B2 51 7E BA 2E 8B 7A 1F A5 EF Ключ: 45 64 6A EA 4E 12 9D 9A A5 62 8C E2 54 3D 93 A6 Криптограмма: 56 09 61 C6 9D B3 75 F2 DC 14 F9 5A B5 EA 61 1B

24.	Столбец байтов 9B D7 0D 51	Блоктекста: 19 A6 CB 57 E0 57 79 06 9E ED 57 8D E4 F2 F2 62 Ключ: E6 DD 69 0A 7A F2 E6 FE 17 38 70 C3 AC C1 DE 3E Криптограмма: B1 0A 28 5F CD 15 04 9A 54 31 F8 F4 41 58 52 B8
25.	Столбец байтов 92 39 2C 17	Блоктекста: CF 5C 09 49 4A 06 68 CE D7 47 94 A5 FE F2 C7 CE Ключ: 20 44 A6 F1 AA 01 E7 91 A9 BD B6 D8 E0 B1 8A 2B Криптограмма: 2E AF 76 93 A0 E7 52 66 19 19 0D 77 32 F8 BF 44

Указания к выполнению практической работы

Для выполнения практической работы рекомендуется использовать файл *AES.xlsm*.

Технология выполнения задания

1. Изучить описание алгоритма AES, рекомендуется использовать презентацию алгоритма (файл *rij.exe*).

Задание А. Выполнить операцию *MixColumns*для заданного столбца байтов аналогично рассмотренному примеру.

Пример. Пусть задан столбец алгоритма AES, содержащий байты, представленные шестнадцатеричными числами: A1, BF, 5D, 30. Выполнить операцию *MixColumns*над заданным столбцом байтов.

2. Выполнить операцию *MixColumns* как действия с полиномами в конечном поле Галуа $GF(2^8)$.Элементы столбца определяются как полиномы в $GF(2^8)$:

- Преобразовать элементы столбца в полиномы в конечном поле Галуа $GF(2^8)$, для чего сначала перевести шестнадцатеричное число в двоичный вид с помощью КалькулятораWindows (*Инженерный режим*)или функцией MSExcel**ШЕСТН.В.ДВ**(группа *Инженерные*), а затем битовую строку – в полином.

Для рассматриваемого примера имеем:

a_1 = $A1_{16}$ = 10100001_2,соответствующий полином в поле Галуа имеет вид: x^7+x^5+1;

a_2 = BF_{16}= 10111111_2, $x^7+x^5+x^4+x^3+x^2+x+1$;

a_3 = $5D_{16}$= 01011101_2, $x^6+x^4+x^3+x^2+1$;

a_4 = 30_{16}= 00110000_2,x^5+x^4.

3. Провестивычисление, используя $b_1 = 02 \bullet a_1 \oplus 03 \bullet a_2 \oplus a_3 \oplus a_4$, умножение полиномов производится по модулю ($x^8+x^4+x^3+x+1$).

ЗАМЕЧЕНИЕ: Значениям 02_{16}=00000010_2 и 03_{16}=00000011_2 соответствуют полиномы x и x+1 в конечном поле Галуа$GF(2^8)$.

В примере получаем:

$b_1=(x^7+x^5+1)\cdot x+(x^7+x^5+x^4+x^3+x^2+x+1)\cdot(x+1)+(x^6+x^4+x^3+x^2+1)+$
$+(x^5+x^4)= x^8+x^6+x+x^8+x^6+x^5+x^4+x^3+x^2+x+x^7+x^5+x^4+x^3+x^2+x+1+$
$+x^6+x^3+x^2+1+x^5 = x^7+ x^6+x^5+x^3+x^2+x.$

(заливкой выделены сокращаемые слагаемые, согласно определению операции сложения в $GF(2^8)$как операции побитового XOR коэффициентов при одинаковых степенях)

Поскольку старшая степень результирующего полинома не превышает 7, приведение по модулю можно не проводить.

- Преобразовать результат в двузначное шестнадцатеричное число (воспользоваться Калькулятором Windowsили инженерной функцией MSExcel**ДВ.В.ШЕСТН**): b_1= = 11101110_2 = EE_{16}.

4. Провестивычисление$b_2 = a_1 \oplus 02 \bullet a_2 \oplus 03 \bullet a_3 \oplus a_4$.

В примере получаем:

$b_2 = (x^7+x^5+1)+(x^7+x^5+x^4+x^3+x^2+x+1)\cdot x+$
$(x^6+x^4+x^3+x^2+1)\cdot(x+1)+(x^5+x^4) =$
$x^7+1+x^8+x^6+x^5+x^4+x^3+x^2+x+x^7+x^5+x^4+x^3+x+x^6+x^4+x^3+x^2+1+x^4=$
x^8+x^3.

Поскольку старшая степень полинома равна 8, следует привести результат по модулю ($x^8+x^4+x^3+x+1$), что в данном случае означает сложение с этим полиномом:

$x^8+x^3 \bmod (x^8+x^4+x^3+x+1)= (x^8+x^4+x^3+x+1)+x^8+x^3= x^4+x+1$.

Окончательно, $b_2 = 00010011_2 = 13_{16}$.

5. Провести вычисление$b_3 = a_1 \oplus a_2 \oplus 02 \bullet a_3 \oplus 03 \bullet a_4$.

В примере получаем:

$b_3 = (x^7+x^5+1)+(x^7+x^5+x^4+x^3+x^2+x+1)(x^6+x^4+x^3+x^2+1)\cdot x+$
$(x^5+x^4)\cdot(x+1) = x^4+x^3+x^2+x+x^7+x^5+x^4+x^3+x+x^6+x^5+x^5+x^4 =$

$x^7+x^6+x^5+x^4+x^2$.

$b_3 = 11110100_2=F4_{16}$.

6. Провестивычисление$b_4 = 03 \bullet a_1 \oplus a_2 \oplus a_3 \oplus 02 \bullet a_4$.

В рассматриваемом примере:

$b_4 = (x^7+x^5+1)\cdot(x+1)+(x^7+x^5+x^4+x^3+x^2+x+1)+$
$(x^6+x^4+x^3+x^2+1)+(x^5+x^4)\cdot x =$
$= x^8+x^6+x+x^7+x^5+1+x^7+x^5+x+x^6+x^6+x^5 = x^8+x^6+x^5+1.$

Приведение по модулю:

$(x^8+x^6+x^5+1) \bmod (x^8+x^4+x^3+x+1) =(x^8+x^4+x^3+x+1)+x^8+x^6+x^5+1=$
$x^6+x^5+x^4+x^3+x.$

$b_4= 01111010_2=7A_{16}$.

Результатом выполнения операции *MixColumns*над столбцом байтов A1, BF, 5D, 30 является столбец EE, 13, F4,7A.

7. Выполнить операцию *MixColumns*как действия с двоичными разрядами.

ЗАМЕЧАНИЕ: В формулах для вычисления *bi* умножение на значение 02_{16} (00000010_2) можно рассматривать как сдвиг двоичного числа на один разряд влево, умножение на 03_{16} (00000011_2) – как сдвиг числана один разряд влево с последующим сложением (XOR) сисходным числом. Приведение по модулю: $(x^8+x^4+x^3+x+1)$ – сложение (XOR) с 100011011_2.

- Представить элементы исходного столбца в двоичном виде.

Впримере:$a_1 = 10100001_2$, $a_2 = 10111111_2$, $a_3 = 01011101_2$, $a_4 = 00110000_2$.

- Вычислитьb_1.

Для рассматриваемого примера получаем:

$02 \bullet a_1$= 101000010,

$03 \bullet a_2$ =101111110 XOR10111111= 111000001.

b_1=	1	0	1	0	0	0	0	1	0
	1	1	1	0	0	0	0	0	1
		0	1	0	1	1	1	0	1
XOR		0	0	1	1	0	0	0	0
	0	1	1	1	0	1	1	1	0

$b_1 = 11101110_2=EE_{16}$.

- Вычислитьb_2.

В примере имеем:

02•a_2 =101111110,
03•a_3 =010111010 XOR01011101=011100111.

b_2=	1	0	1	0	0	0	0	1
	1	0	1	1	1	1	1	0
	0	1	1	1	0	0	1	1
XOR	0	0	1	1	0	0	0	0
	1	0	0	0	0	1	0	0
приведение, XOR	1	0	0	0	1	1	0	1	1
	0	0	0	0	1	0	0	1	1

$b_2 = 00010011_2=13_{16}$

- Вычислитьb_3.

В примере:
02•a_3=010111010,
03•a_4 =001100000XOR00110000= 001010000.

b_3=		1	0	1	0	0	0	0	1
		1	0	1	1	1	1	1	1
	0	1	0	1	1	1	0	1	0
XOR	0	0	1	0	1	0	0	0	0
	0	1	1	1	1	0	1	0	0

$b_3 = 11110100_2=F4_{16}$

- Вычислитьb_4.

В примере:
03•a_1 =101000010XOR10100001= 111100011.
02•a_4=001100000,

b_4=	1	1	1	1	0	0	0	1	1
		1	0	1	1	1	1	1	1
		0	1	0	1	1	1	0	1
XOR	0	0	1	1	0	0	0	0	0
	1	0	1	1	0	0	0	0	1
приведение, XOR	1	0	0	0	1	1	0	1	1
	0	0	1	1	1	1	0	1	0

$b_4 = 01111010_2= 7A_{16}$
Результат – столбец EE, 13, F4,7A.

Задание В. Выполнить шифрование заданного блока текста аналогично рассмотренному примеру.

Пример. Пусть задан 128-битовый фрагмент текста«3243F6A8885A308D313198A2E0370734» и 128-битовый ключ«2B7E151628AED2A6ABF7158809CF4F3C». Требуется зашифровать текст с помощью алгоритма AES.Для шифрования рекомендуется использовать книгу *AES.xlsx*.

8. Выбрать значения блока текста и ключа шифрования из таблицы 25 в соответствии с номером варианта.
9. Открыть книгу *AES.xlsx*. Занести значения текста и ключа побайтно в ячейки диапазонов **B3:Q3** и **S3:AH3**листа *Данные шифр-е* книги *AES.xlsx*. Числовые значения следует вводить в текстовом формате, то есть предварять символом одинарной кавычки (‘). Результат предварительного (нулевого) раунда отобразится в диапазоне **S5:V8**листа *Данные шифр-е*.

Для рассматриваемого примера:

Данные

32	88	31	E0
43	5A	31	37
F6	30	98	07
A8	8D	A2	34

Ключ 0

2B	28	AB	09
7E	AE	F7	CF
15	D2	15	4F
16	A6	88	3C

Результат 0 раунда

19	A0	9A	E9
3D	F4	C6	F8
E3	E2	8D	48
BE	2B	2A	08

10. Вычислить ключ 1 раунда шифрования:

- Перейти на лист *Расширение ключа*, в ячейке **A11**установить значение **1**.
- Скопировать данные из диапазона **K5:N8**листа *Данные шифр-е*, перейти на лист *Расширение ключа* и вставить значения в диапазон **F11:I14**командой **Вставить/Специальная вставка/Значения**.
- В диапазоне ячеек **A15:D18**листа *Расширение ключа* получен ключ 1 раунда.

В рассматриваемом примере имеем:

Результат (ключ 1 раунда):

A0	88	23	2A
FA	54	A3	6C
FE	2C	39	76
17	B1	39	05

- Скопировать значения ключа 1 раунда в диапазон ячеек **K10:N13**листа *Данные шифр-е*(**Вставить/Специальная вставка/Значения**).

11. Выполнить первый раунд шифрования:

- На листе *Данные шифр-е* автоматически заполнен диапазон **D10:G13** исходных данных 1 раунда шифрования. Скопировать значения из диапазона **D10:G13** в диапазон **C8:F11**листа *Шифрование*(**Вставить/Специальная вставка/Значения**).
- Аналогичным образом скопировать значения из диапазона **K10:N13**листа *Данные шифр-е* в диапазон ячеек **H8:K11** листа *Шифрование*.
- На листе *Шифрование* приведены результаты выполнения операций раунда.

В примере:

SubBytes

D4	E0	B8	1E
27	BF	B4	41
11	98	5D	52
AE	F1	E5	30

ShiftRows

D4	E0	B8	1E
BF	B4	41	27
5D	52	11	98
30	AE	F1	E5

MixColumns

04	E0	48	28
66	CB	F8	06
81	19	D3	26
E5	9A	7A	4C

AddRoundKey

A4	68	6B	02
9C	9F	5B	6A
7F	35	EA	50
F2	2B	43	49

- Скопировать результат выполнения последней операции раунда (данные диапазона **C53:F56**листа *Шифрование*) в диапазон **S10:V13** листа *Данные шифр-е*.

12. Повторить пункты 10-11 для всех раундов шифрования (со 2 по 9).

В примере будут получены следующие результаты:

раунд 2

текст

A4	68	6B	02
9C	9F	5B	6A
7F	35	EA	50
F2	2B	43	49

ключ 2

F2	7A	59	73
C2	96	35	59
95	B9	80	F6
F2	43	7A	7F

результат раунда

AA	61	82	68
8F	DD	D2	32
5F	E3	4A	46
03	EF	D2	9A

операции раунда

SubBytes

49	45	7F	77
DE	DB	39	02
D2	96	87	53
89	F1	1A	3B

ShiftRows

49	45	7F	77
DB	39	02	DE
87	53	D2	96
3B	89	F1	1A

MixColumns

58	1B	DB	1B
4D	4B	E7	6B
CA	5A	CA	B0
F1	AC	A8	E5

AddRoundKey

AA	61	82	68
8F	DD	D2	32
5F	E3	4A	46
03	EF	D2	9A

раунд 3

текст

AA	61	82	68
8F	DD	D2	32
5F	E3	4A	46
03	EF	D2	9A

ключ 3

3D	47	1E	6D
80	16	23	7A
47	FE	7E	88
7D	3E	44	3B

результат раунда

48	67	4D	D6
6C	1D	E3	5F
4E	9D	B1	58
EE	0D	38	E7

операции раунда

SubBytes

AC	EF	13	45
73	C1	B5	23
CF	11	D6	5A
7B	DF	B5	B8

ShiftRows

AC	EF	13	45
C1	B5	23	73
D6	5A	CF	11
B8	7B	DF	B5

MixColumns

75	20	53	BB
EC	0B	C0	25
09	63	CF	D0
93	33	7C	DC

AddRoundKey

48	67	4D	D6
6C	1D	E3	5F
4E	9D	B1	58
EE	0D	38	E7

раунд 4

текст

48	67	4D	D6
6C	1D	E3	5F
4E	9D	B1	58
EE	0D	38	E7

ключ 4

EF	A8	B6	DB
44	52	71	0B
A5	5B	25	AD
41	7F	3B	00

результат раунда

E0	C8	D9	85
92	63	B1	B8
7F	63	35	BE
E8	C0	50	01

операции раунда

SubBytes

52	85	E3	F6
50	A4	11	CF
2F	5E	C8	6A
28	D7	07	94

ShiftRows

52	85	E3	F6
A4	11	CF	50
C8	6A	2F	5E
94	28	D7	07

MixColumns

0F	60	6F	5E
D6	31	C0	B3
DA	38	10	13
A9	BF	6B	01

AddRoundKey

E0	C8	D9	85
92	63	B1	B8
7F	63	35	BE
E8	C0	50	01

раунд 5

текст

E0	C8	D9	85
92	63	B1	B8
7F	63	35	BE
E8	C0	50	01

ключ 5

D4	7C	CA	11
D1	83	F2	F9
C6	9D	B8	15
F8	87	BC	BC

результат раунда

F1	C1	7C	5D
00	92	C8	B5
6F	4C	8B	D5
55	EF	32	0C

операции раунда

SubBytes

E1	E8	35	97
4F	FB	C8	6C
D2	FB	96	AE
9B	BA	53	7C

ShiftRows

E1	E8	35	97
FB	C8	6C	4F
96	AE	D2	FB
7C	9B	BA	53

MixColumns

25	BD	B6	4C
D1	11	3A	4C
A9	D1	33	C0
AD	68	8E	B0

AddRoundKey

F1	C1	7C	5D
00	92	C8	B5
6F	4C	8B	D5
55	EF	32	0C

раунд 6

текст

F1	C1	7C	5D
00	92	C8	B5
6F	4C	8B	D5
55	EF	32	0C

ключ 6

6D	11	DB	CA
88	0B	F9	00
A3	3E	86	93
7A	FD	41	FD

результат раунда

26	3D	E8	FD
0E	41	64	D2
2E	B7	72	8B
17	7D	A9	25

операции раунда

SubBytes

A1	78	10	4C
63	4F	E8	D5
A8	29	3D	03
FC	DF	23	FE

ShiftRows

A1	78	10	4C
4F	E8	D5	63
3D	03	A8	29
FE	FC	DF	23

MixColumns

4B	2C	33	37
86	4A	9D	D2
8D	89	F4	18
6D	80	E8	D8

AddRoundKey

26	3D	E8	FD
0E	41	64	D2
2E	B7	72	8B
17	7D	A9	25

раунд 7

текст

26	3D	E8	FD
0E	41	64	D2
2E	B7	72	8B
17	7D	A9	25

ключ7

4E	5F	84	4E
54	5F	A6	A6
F7	C9	4F	DC
0E	F3	B2	4F

результат раунда

5A	19	A3	7A
41	49	E0	8C
42	DC	19	04
B1	1F	65	0C

операции раунда

SubBytes

F7	27	9B	54
AB	83	43	B5
31	A9	40	3D
F0	FF	D3	3F

ShiftRows

F7	27	9B	54
83	43	B5	AB
40	3D	31	A9
3F	F0	FF	D3

MixColumns

14	46	27	34
15	16	46	2A
B5	15	56	D8
BF	EC	D7	43

AddRoundKey

5A	19	A3	7A
41	49	E0	8C
42	DC	19	04
B1	1F	65	0C

раунд 8

текст

5A	19	A3	7A
41	49	E0	8C
42	DC	19	04
B1	1F	65	0C

ключ 8

EA	B5	31	7F
D2	8D	2B	8D
73	BA	F5	29
21	D2	60	2F

результат раунда

EA	04	65	85
83	45	5D	96
5C	33	98	B0
F0	2D	AD	C5

операции раунда

SubBytes

BE	D4	0A	DA
83	3B	E1	64
2C	86	D4	F2
C8	C0	4D	FE

ShiftRows

BE	D4	0A	DA
3B	E1	64	83
D4	F2	2C	86
FE	C8	C0	4D

MixColumns

00	B1	54	FA
51	C8	76	1B
2F	89	6D	99
D1	FF	CD	EA

AddRoundKey

EA	04	65	85
83	45	5D	96
5C	33	98	B0
F0	2D	AD	C5

раунд 9

текст			
EA	04	65	85
83	45	5D	96
5C	33	98	B0
F0	2D	AD	C5

ключ 9			
AC	19	28	57
77	FA	D1	5C
66	DC	29	00
F3	21	41	6E

результат раунда			
EB	59	8B	1B
40	2E	A1	C3
F2	38	13	42
1E	84	E7	D2

операции раунда

SubBytes			
87	F2	4D	97
EC	6E	4C	90
4A	C3	46	E7
8C	D8	95	A6

ShiftRows			
87	F2	4D	97
6E	4C	90	EC
46	E7	4A	C3
A6	8C	D8	95

MixColumns			
47	40	A3	4C
37	D4	70	9F
94	E4	3A	42
ED	A5	A6	BC

AddRoundKey			
EB	59	8B	1B
40	2E	A1	C3
F2	38	13	42
1E	84	E7	D2

13. Аналогично пункту 10 сформировать ключ завершающего (10) раунда.
14. Поскольку завершающий раунд шифрования имеет сокращенное число операций, скопировать значения текста и ключа в диапазоны ячеек **C59:F62**и **H59:K62**соответственно листа *Шифрование*. Результат шифрования отобразится в диапазоне **C75:F78**листа *Шифрование*. Скопировать значения диапазона **C75:F78** в диапазон ячеек **S55:V58**листа *Данные шифр-е*.

Для рассматриваемого примера получили:

заключит. раунд

текст			
EB	59	8B	1B
40	2E	A1	C3
F2	38	13	42
1E	84	E7	D2

ключ 10			
D0	C9	E1	B6
14	EE	3F	63
F9	25	0C	0C
A8	89	C8	A6

результат шифрования

39	02	DC	19
25	DC	11	6A
84	09	85	0B
1D	FB	97	32

операции раунда

SubBytes			
E9	CB	3D	AF
09	31	32	2E
89	07	7D	2C
72	5F	94	B5

ShiftRows			
E9	CB	3D	AF
31	32	2E	09
7D	2C	89	07
B5	72	5F	94

AddRoundKey			
39	02	DC	19
25	DC	11	6A
84	09	85	0B
1D	FB	97	32

Результат шифрования – криптограмма «3925841D02DC09FBDC118597196A0B32».

Задание С. Выполнить расшифрованиезаданного блока аналогично рассмотренному примеру.

Пример. Пусть задан 128-битовый фрагмент текста «E20E5F3C947E69D0D78B8079F4E2695B». Требуется расшифровать текст с помощью алгоритма AES с помощью ключа из предыдущего задания «2B7E151628AED2A6ABF7158809CF4F3C».

При расшифровании используются те же раундовые ключи, что и при шифровании данных, но в обратном порядке. Поскольку заданный шифр-текст получен на том же ключе шифрования, что и в предыдущем задании, ключи для расшифровки уже вычислены.Для расшифрования рекомендуется использовать книгу *AES.xlsx*.

15. Выбрать значение криптограммы из таблицы 25 в соответствии с номером варианта.
16. Занести значение криптограммы побайтно в ячейки диапазона **B3:Q3** листа *Данные расшифр-ка* книги *AES.xlsx*. Числовые значения следует предварять знаком одинарной кавычки «’». В ячейки диапазона **K5:N8** листа *Данные расшифр-ка* скопировать значения байтов ключа заключительного раунда шифрования из диапазона **K55:N58** листа *Данные шифр-е*. Результат предварительного (нулевого) раунда расшифровки отобразится в диапазоне **S5:V8** листа *Данные расшифровка*.

В примере имеем:

раунд 0

текст

E2	94	D7	F4
0E	7E	8B	E2
5F	69	80	69
3C	D0	79	5B

ключ 10

D0	C9	E1	B6
14	EE	3F	63
F9	25	0C	0C
A8	89	C8	A6

результат раунда

32	5D	36	42
1A	90	B4	81
A6	4C	8C	65
94	59	B1	FD

17. Выполнить первый раунд шифрования:

- Скопировать значения ключа шифрования 9 раунда с листа *Данные шифр-е* в диапазон ячеек **K10:N13**листа*Данные расшифр-ка*.
- На листе *Данные расшифр-ка* автоматически заполнен диапазон **D10:G13** исходных данных 1 раунда расшифровки. Скопировать значения из диапазона **D10:G13** в диапазон **C8:F11**листа *Расшифровка* (**Вставить/Специальная вставка/значения**).

- Аналогичным образом скопировать данные из диапазона **K10:N13**листа *Данные расшифр-ка* в диапазон ячеек **H8:K11** листа *Расшифровка*.
- На листе *Расшифровка* приведены результаты выполнения операций раунда расшифрования.

  В примере:

InvShiftRows

32	5D	36	42
81	1A	90	B4
8C	65	A6	4C
59	B1	FD	94

InvSubBytes

A1	8D	24	F6
91	43	96	C6
F0	BC	C5	5D
15	56	21	E7

AddRoundKey

0D	94	0C	A1
E6	B9	47	9A
96	60	EC	5D
E6	77	60	89

InvMixColumns

B5	C2	92	DC
29	F4	33	95
03	42	E7	E5
04	4E	81	43

- Скопировать результат выполнения последней операции раунда (данные диапазона **C73:F76**листа *Расшифровка*) в диапазон **S10:V13** листа *Данные расшифр-ка*.

18. Повторить пункт 17 для всех раундов расшифровки (со 2 по 9).

    В примере будут получены следующие результаты:

раунд 2

текст

B5	C2	92	DC
29	F4	33	95
03	42	E7	E5
04	4E	81	43

ключ 8

EA	B5	31	7F
D2	8D	2B	8D
73	BA	F5	29
21	D2	60	2F

результат раунда

FC	CB	48	8B
1A	2A	BB	DB
21	58	D6	2D
D4	B6	D5	BA

операции раунда

InvShiftRows

B5	C2	92	DC
95	29	F4	33
E7	E5	03	42
4E	81	43	04

InvSubBytes

D2	A8	74	93
AD	4C	BA	66
B0	2A	D5	F6
B6	91	64	30

AddRoundKey

38	1D	45	EC
7F	C1	91	EB
C3	90	20	DF
97	43	04	1F

InvMixColumns

FC	CB	48	8B
1A	2A	BB	DB
21	58	D6	2D
D4	B6	D5	BA

раунд 3

текст

FC	CB	48	8B
1A	2A	BB	DB
21	58	D6	2D
D4	B6	D5	BA

ключ 7

4E	5F	84	4E
54	5F	A6	A6
F7	C9	4F	DC
0E	F3	B2	4F

результат раунда

C4	DC	0B	4F
2B	0B	34	A3
56	37	25	55
A3	8F	3F	B5

операции раунда

InvShiftRows

FC	CB	48	8B
DB	1A	2A	BB

InvSubBytes

55	59	D4	CE
9F	43	95	FE

AddRoundKey

1B	06	50	80
CB	1C	33	58

InvMixColumns

C4	DC	0B	4F
2B	0B	34	A3

D6	2D	21	58
B6	D5	BA	D4

4A	FA	7B	5E
79	B5	C0	19

BD	33	34	82
77	46	72	56

56	37	25	55
A3	8F	3F	B5

раунд 4

текст

C4	DC	0B	4F
2B	0B	34	A3
56	37	25	55
A3	8F	3F	B5

ключ6

6D	11	DB	CA
88	0B	F9	00
A3	3E	86	93
7A	FD	41	FD

результат раунда

02	6F	60	28
C6	5D	B8	F3
6E	37	1D	F0
DE	8C	4B	F6

операции раунда

InvShiftRows

C4	DC	0B	4F
A3	2B	0B	34
25	55	56	37
8F	3F	B5	A3

InvSubBytes

88	93	9E	92
71	0B	9E	28
C2	ED	B9	B2
73	25	D2	71

AddRoundKey

E5	82	45	58
F9	00	67	28
61	D3	3F	21
09	D8	93	8C

InvMixColumns

02	6F	60	28
C6	5D	B8	F3
6E	37	1D	F0
DE	8C	4B	F6

раунд 5

текст

02	6F	60	28
C6	5D	B8	F3
6E	37	1D	F0
DE	8C	4B	F6

ключ 5

D4	7C	CA	11
D1	83	F2	F9
C6	9D	B8	15
F8	87	BC	BC

результат раунда

3B	AD	EF	64
79	B9	61	24
9F	B8	37	0A
DC	53	0B	51

операции раунда

InvShiftRows

02	6F	60	28
F3	C6	5D	B8
1D	F0	6E	37
8C	4B	F6	DE

InvSubBytes

6A	06	90	EE
7E	C7	8D	9A
DE	17	45	B2
F0	CC	D6	9C

AddRoundKey

BE	7A	5A	FF
AF	44	7F	63
18	8A	FD	A7
08	4B	6A	20

InvMixColumns

3B	AD	EF	64
79	B9	61	24
9F	B8	37	0A
DC	53	0B	51

раунд 6

текст

3B	AD	EF	64
79	B9	61	24
9F	B8	37	0A
DC	53	0B	51

ключ 4

EF	A8	B6	DB
44	52	71	0B
A5	5B	25	AD
41	7F	3B	00

результат раунда

B8	D3	D3	E4
96	45	62	20
8D	33	B5	C4
E1	F1	79	20

операции раунда

InvShiftRows

3B	AD	EF	64
24	79	B9	61
37	0A	9F	B8
53	0B	51	DC

InvSubBytes

49	18	61	8C
A6	AF	DB	D8
B2	A3	6E	9A
50	9E	70	93

AddRoundKey

A6	B0	D7	57
E2	FD	AA	D3
17	F8	4B	37
11	E1	4B	93

InvMixColumns

B8	D3	D3	E4
96	45	62	20
8D	33	B5	C4
E1	F1	79	20

раунд 7

текст

B8	D3	D3	E4
96	45	62	20
8D	33	B5	C4
E1	F1	79	20

ключ 3

3D	47	1E	6D
80	16	23	7A
47	FE	7E	88
7D	3E	44	3B

результат раунда

CE	58	B6	57
2F	16	28	83
87	94	87	34
D6	F0	3F	C7

операции раунда

InvShiftRows

B8	D3	D3	E4
20	96	45	62
B5	C4	8D	33
F1	79	20	E1

InvSubBytes

9A	A9	A9	AE
54	35	68	AB
D2	88	B4	66
2B	AF	54	E0

AddRoundKey

A7	EE	B7	C3
D4	23	4B	D1
95	76	CA	EE
56	91	10	DB

InvMixColumns

CE	58	B6	57
2F	16	28	83
87	94	87	34
D6	F0	3F	C7

раунд 8

текст

CE	58	B6	57
2F	16	28	83
87	94	87	34
D6	F0	3F	C7

ключ 2

F2	7A	59	73
C2	96	35	59
95	B9	80	F6
F2	43	7A	7F

результат раунда

9F	76	15	B2
DC	D7	6A	2F
F0	D5	D2	7E
B4	7F	66	D9

операции раунда

InvShiftRows

CE	58	B6	57
83	2F	16	28
87	34	87	94
F0	3F	C7	D6

InvSubBytes

EC	5E	79	DA
41	4E	FF	EE
EA	28	EA	E7
17	25	31	4A

AddRoundKey

1E	24	20	A9
83	D8	CA	B7
7F	91	6A	11
E5	66	4B	35

InvMixColumns

9F	76	15	B2
DC	D7	6A	2F
F0	D5	D2	7E
B4	7F	66	D9

раунд 9

текст

9F	76	15	B2
DC	D7	6A	2F
F0	D5	D2	7E
B4	7F	66	D9

ключ 1

A0	88	23	2A
FA	54	A3	6C
FE	2C	39	76
17	B1	39	05

результат раунда

CE	4B	3D	1E
00	6F	80	0B
94	79	BF	89
DD	D9	52	BC

операции раунда

InvShiftRows

9F	76	15	B2
2F	DC	D7	6A
D2	7E	F0	D5
7F	66	D9	B4

InvSubBytes

6E	0F	2F	3E
4E	93	0D	58
7F	8A	17	B5
6B	D3	E5	C6

AddRoundKey

CE	87	0C	14
B4	C7	AE	34
81	A6	2E	C3
7C	62	DC	C3

InvMixColumns

CE	4B	3D	1E
00	6F	80	0B
94	79	BF	89
DD	D9	52	BC

19. Выполнить заключительный раунд расшифровки:

- Скопировать значения ключа 0 раунда шифрования (исходного ключа шифрования) с листа *Данные шифр-е* в диапазон ячеек **K55:N58**листа *Данные расшифр-ка*.
- Скопировать значения текста и ключа заключительного раунда расшифровки в диапазоны ячеек **C79:F82**и **H79:K82**листа *Расшифровка*. Результат расшифрования отобразится в диапазоне **C95:F98**листа *Расшифровка*.

В примере получим:

заключит. раунд

текст			
CE	4B	3D	1E
00	6F	80	0B
94	79	BF	89
DD	D9	52	BC

ключ 0			
2B	28	AB	09
7E	AE	F7	CF
15	D2	15	4F
16	A6	88	3C

открытый текст			
C7	E4	20	E0
E0	FC	F1	F5
E1	20	F2	E0
F3	EE	F0	F5

операции раунда

InvSubBytes			
EC	CC	8B	E9
52	06	3A	9E
E7	AF	F4	F2
C9	E5	48	78

InvShiftRows			
EC	CC	8B	E9
9E	52	06	3A
F4	F2	E7	AF
E5	48	78	C9

AddRoundKey			
C7	E4	20	E0
E0	FC	F1	F5
E1	20	F2	E0
F3	EE	F0	F5

- Скопировать значения диапазона **C95:F98** в диапазон ячеек **S55:V58**листа *Данные расшифр-ка*. Данные значения представляют открытый текст в шестнадцатеричном представлении.
- В диапазоне **B63:Q63**листа *Данные расшифр-ка* приведено десятеричное представление открытого текста, которое трактуется как ASCII-коды текстовых символов. Диапазон **B65:Q65**листа *Данные расшифр-ка* содержит символьное представление открытого текста. Критерием правильности выполнения задания является получение осмысленного текста.

В рассматриваемом примере будет получен открытый текст «Забудь о страхах».

ТЕМА 3. ПОТОКОВЫЕ СИСТЕМЫ ШИФРОВАНИЯ

Потоковые шифры преобразуют открытый текст в шифртекст последовательно, бит за битом. Фактически они являются шифром гаммирования и различаются только методами генерации ключевой последовательности – *гаммы* $\gamma_1(k),\gamma_2(k), ..., \gamma_i(k), ...$, зависящей от ключа k. Шифрование производится наложением гаммы на открытый текст: $y_i = x_i \oplus \gamma_i(k)$, арасшифрование – повторным наложением гаммы $x_i = y_i \oplus \gamma_i(k) = x_i \oplus \gamma_i(k) \oplus \gamma_i(k)$.

Сама гамма должна быть непредсказуемой, то есть нарушитель, зная любой коль угодно длинный ее фрагмент, не должен иметь возможности предсказать следующий бит (биты) гаммы. Поэтому в качестве генераторов гаммы должны использоваться криптографически сильные генераторы псевдослучайных чисел. К таким генераторам относятся, например, режимы гаммирования блочных шифров в предположении стойкости алгоритма блочного шифрования.

Кроме того, важна и эффективность (высокая скорость работы) генератора. Криптографически сильные генераторы, как правило, гораздо медленнее традиционных методов генерации псевдослучайных чисел, встроенных в инструментальные средства разработки программных систем и высокоуровневые языки программирования.

Одним из наиболее эффективных на сегодняшний день генераторов криптографически сильных псевдослучайных последовательностей является генератор Блюм-Блюма-Шуба (BBS-генератор), являющийся асимметричной криптосистемой. Шифр гаммирования, использующий этот генератор, был предложен в 1984 году и получил название криптосистемы Блюма – Гольдвассер по именам авторов.

Практическая работа №8. Изучениепотоковой криптосистемы Блюма – Гольдвассер

Описание метода шифрования

Система вероятностного шифрования Блюма-Гольдвассер основана на применении криптографически сильного генератора

псевдослучайных чисел – BBS-генератора. Параметрами генератора являются два случайных больших простых числа pи q, такие, что $p \equiv q \equiv 3 \pmod 4$. Числа pи qдержатся в секрете, а число Блюма $n = pq$является общим открытым параметром и может публиковаться свободно.

Отправитель сообщения Mпредставляет его в виде битовой последовательностидлины m, выбирает случайное число s,взаимно простое с n, $1 < s < n$, и генерирует псевдослучайную битовую последовательность $ps = b_0 b_1 b_2 \ldots b_{m-1}$длины m, пользуясь формулами:

$x_0 = s^2 \bmod n$, $x_i = x_{i-1}^2 \bmod n$, $b_i = x_i \bmod 2$, $i = 0, 1, \ldots, m-1$.

Для шифрования сообщения M на него накладывается (с помощью побитового XOR) полученная псевдослучайная битовая последовательность накладывается на сообщение $M \oplus ps$. Результат отправляется получателю вместе с подсказкой – значениемследующего члена ряда x_i, то есть x_m. Таким образом, в качестве криптограммы Cвыступает пара $(x_m, M \oplus ps)$, причемчисло $\boldsymbol{x}_m$не участвовало в формировании последовательности ps.

Получатель должен восстановить последовательность ps, а затем наложить ее на C: $C \oplus ps = M \oplus ps \oplus ps = M$.

Стойкость криптосистемы Блюма-Гольдвассер базируется на непредсказуемости влево BBS-генератора, определяемой однонаправленностью функции $f(x) = x^2 \bmod n$, где n – число Блюма, в предположении трудности факторизации числа n.

Законный получатель сообщения, зная значения pи q,может легко восстановить последовательность ps.

Для этого сначала с помощью расширенного алгоритма Евклидаон получает целые числа aи b, такие, что $ap + bq = 1$.

Затем вычисляет:

$$\alpha = \left(\frac{p+1}{4} \right)^m \bmod (p-1),$$

$$\beta = \left(\frac{q+1}{4} \right)^m \bmod (q-1),$$

$r = (x_m \bmod p)^{\alpha} \bmod p$,

$t = (x_m \bmod q)^{\beta} \bmod q$,

$x_0 = (apt + bqr) \bmod n$.

Значениеx_0позволяет вычислить любой член последовательности x_iс той же эффективностью, как это может сделать отправитель.

Быстродействие криптосистемы Блюма-Гольдвассер может быть повышено за счет использования не одного, а не более $\log_2\eta$младших битов чисел последовательности x_i,где η– количество двоичных разрядов числа Блюма n (то есть $\eta\approx\log_2\log_2 n$). Это не ослабит результирующую последовательность *ps*, а само шифрование будет эффективнее в $\log_2\eta$раз.

Задание

Изучить процедуры генерации случайных чисел методом Блюма-Блюма-Шуба, шифрования и расшифрования в криптосистеме Блюма-Гольдвассер.

Технология выполнения задания

Задание А. Зашифровать клавиатурный символ с помощью криптосистемы Блюма-Гольдвассер, сгенерировав 8-битовую псевдослучайную последовательность.

1. Из таблицы 26 выбрать,в соответствии с номером варианта, значения параметров BBS-генератора *p*, *q*, случайное число *s* и подлежащий зашифрованию символ*M* (все символы – русскоязычные).

Таблица 26

Варианты задания

№	*p*	*q*	*s*	Открытый текст ***M***	№	*p*	*q*	*s*	Открытый текст ***M***
1	491	191	86584	А	**14**	883	367	65486	О
2	967	211	199217	Б	**15**	719	127	24904	П
3	787	167	126295	В	**16**	431	607	232989	р
4	859	307	40176	Г	**17**	359	523	76520	с
5	547	239	113114	Д	**18**	947	331	127471	т
6	811	443	201939	е	**19**	167	839	6960	у
7	607	499	38453	ж	**20**	523	419	160052	ф
8	419	631	178911	з	**21**	239	919	33449	Х
9	331	727	178999	и	**22**	571	227	41449	Ц

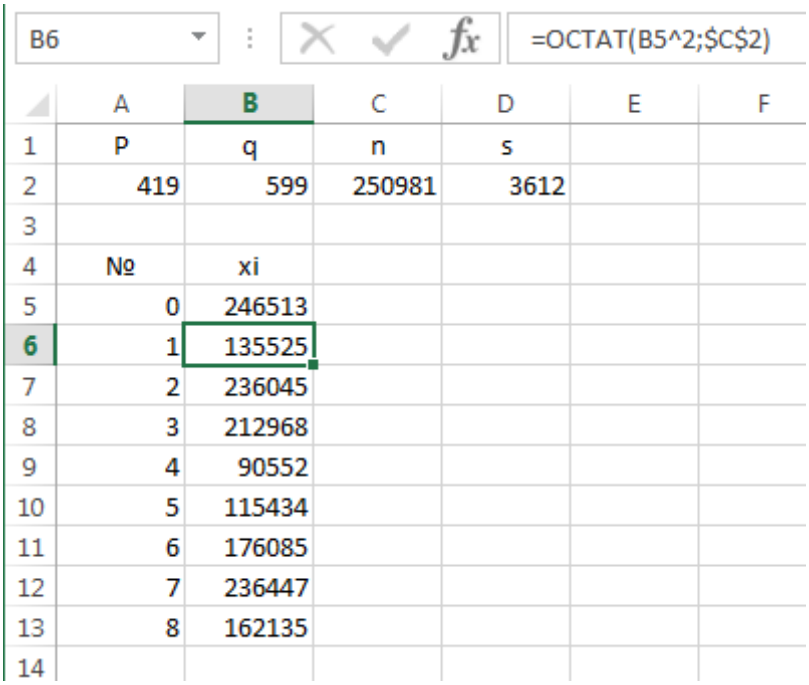
10	311	563	124332	к	**23**	191	823	102516	Ч
11	227	751	141201	Л	**24**	127	827	74957	Ш
12	659	491	47136	М	**25**	463	371	97069	Щ
13	439	523	96423	Н					

Сформировать псевдослучайную последовательность *ps*и зашифровать символ *М*аналогично рассмотренному ниже примеру.

Пример. BBS-генератор имеет следующие параметры: p = 419, q = 599, выбрано случайное число s = 3612. Сформировать псевдослучайную 8-битовую последовательность, используя один младший бит чисел x_i, формируемых BBS-генератором. Зашифровать символ «я».

2. В приложении MSExcel создать новую книгу, на первом листе ввести значения p, q, вычислить число Блюма n как их произведение. Ввести значение случайного числа s.
3. Рассчитать элементы ряда x_i(рис.49):

- Пронумеровать ячейки первого столбца от 0 до 8 (поскольку требуется сформировать 8 бит последовательности *ps*для шифрования и еще одно число-подсказку).
- В первую ячейку второго столбца ввести формулу для вычисления x_0по формуле $x_0 = s^2 \bmod n$, например, **=ОСТАТ(D2^2;$C$2)**.
- Во вторую ячейку второго столбца ввести формулу для вычисления x_1 ($x_1 = x_0^2 \bmod n$), например, **=ОСТАТ(B5^2;$C$2)**. Скопировать эту формулу на оставшиеся ячейки рядаx_i.

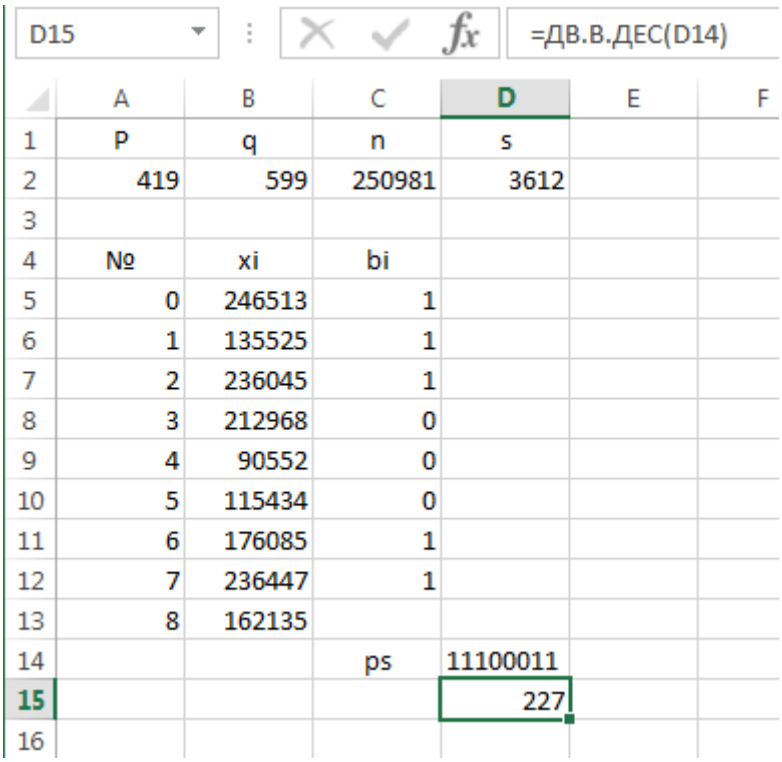


	A	B	C	D	E	F
1	P	q	n	s		
2	419	599	250981	3612		
3						
4	№	xi				
5	0	246513				
6	1	135525				
7	2	236045				
8	3	212968				
9	4	90552				
10	5	115434				
11	6	176085				
12	7	236447				
13	8	162135				
14						

Рис. 49.Вычисление последовательности x_iBBS-генератора

4. Вычислить младшие биты b_i чисел x_i. Значение младшего бита определяется остатком от деления числа на 2, поэтому для вычисления можно использовать функцию **ОСТАТ** (рис. 50), например, **=ОСТАТ(B5;2)** для числа x_0. Скопировать формулу на все ячейки ряда b_i, кроме последней (последнее число x_8не предназначено для формирования битовой последовательности, это – число-подсказка).
5. Сформировать результирующую битовую псевдослучайную последовательность с помощью операции **&**, например, **=C5&C6&C7&C8&C9&C10&C11&C12**, или функции **СЦЕПИТЬ** из группы *Текстовые*, например,**=СЦЕПИТЬ(C5;C6;C7;C8;C9;C10;C11;C12)**.

Значение результирующей последовательности: 11100011 (рис. 50).



	A	B	C	D	E	F
1	P	q	n	s		
2	419	599	250981	3612		
3						
4	№	xi	bi			
5	0	246513	1			
6	1	135525	1			
7	2	236045	1			
8	3	212968	0			
9	4	90552	0			
10	5	115434	0			
11	6	176085	1			
12	7	236447	1			
13	8	162135				
14			ps	11100011		
15				227		
16						

Рис. 50. Вычисление псевдослучайной последовательности ps

6. Перевести битовую последовательность *ps*в десятеричное число с помощью функции **ДВ.В.ДЕС** группы *Инженерные*.
7. Зашифровать символ в криптосистеме Блюма-Гольдвассер (рис. 51):

- Занести шифруемый символ *M* на лист MSExcel. Получить десятичный (ASCII) код символа с помощью функции **КОДСИМВ** группы *Текстовые*.
- Получить значение *M*⊕*ps* (на основе десятичных значений кода символа и последовательности *ps*) с помощью функции **БИТ.ИСКЛИЛИ** (в MSExcel 2013) или операции *Xor*в стандартном приложенииMSWindows Калькулятор, режим (вид) *Программист*.

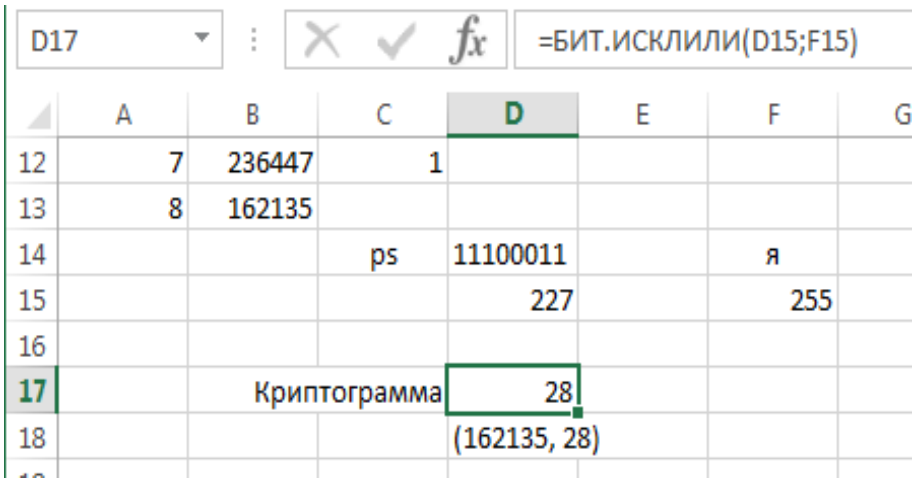


Рис. 51. Зашифрование символа в криптосистеме Блюма-Гольдвассер

- Сформировать криптограмму C с подсказкой вида $(x_8, M \oplus ps)$.

В рассматриваемом примере получили: $M \oplus ps = 28$; $C = (162135, 28)$.

Задание В. Расшифровать криптограмму, полученную в криптосистеме Блюма-Гольдвассер. Известно, что использована эффективная реализация BBS-генератора с максимально допустимым числом младших битов.

8. В соответствии с номером варианта выбрать из таблицы 27значения секретного ключа: чисел pи q, криптограммуC, состоящую из числа-подсказки x_6и последовательности ASCII-кодов c_iсимволов зашифрованного текста.

Провести расшифрование (получить открытый текст) аналогично рассмотренному ниже примеру.

Пример. Известен общий секретный ключ абонентов – числа $p = 419$ и $q = 599$. Получена криптограмма, представленная последовательностью ASCII-кодов 71;228;136 с проверочным числом $x_6 = 3600$. Известно, что при формировании псевдослучайной последовательности BBS-генератора использовано максимально возможное число младших битов чисел x_i, не нарушающее стойкости последовательности.

Таблица 27

Варианты задания

№	*p*	*q*	Криптограмма*C*		№	*p*	*q*	Криптограмма*C*	
			x_6	c_i				x_6	c_i
1	439	491	123530	130;222;119	**14**	751	359	155824	52;188;154
2	883	227	90864	142;179;227	**15**	919	307	87447	245;152;205
3	719	787	1969	191;6;52	**16**	443	499	114407	245;33;110
4	431	859	365061	185;255;104	**17**	367	631	61651	0;250;25
5	359	547	21860	32;225;68	**18**	211	823	10088	211;28;89
6	947	811	333274	78;119;23	**19**	311	827	106599	229;47;240
7	167	607	10940	43;233;19	**20**	307	839	102273	108;251;47
8	523	419	32720	245;222;181	**21**	499	523	186727	59;132;91
9	239	631	136689	17;103;9	**22**	631	239	28164	100;183;157
10	571	311	36743	135;142;186	**23**	331	571	55710	247;40;158
11	191	967	132562	158;52;200	**24**	727	311	81985	222;79;20
12	127	659	57634	48;202;24	**25**	563	439	64930	53;81;109
13	463	431	113045	204;84;79					

9. Определить максимально допустимое для использования в последовательности *ps*число младших битов чисел x_i (рис. 52):

- Занести на новый лист MSExcelзначения *p* и *q*, вычислить *n* = *pq*. Получили *n* = 250981.
- Определить минимальное число битов, необходимое для кодирования *n*. Рядом со значением*n* вычислить двоичный логарифм значения *n* + 1. Для этого следует использовать функцию **LOG**, задав значение второго параметра равным 2, например, **=LOG(C2+1;2)**. Полученное значение округлить вверх до целого, для чего следует использовать функцию **ОКРУГЛВВЕРХ**, задав число десятичных разрядов равным 0, например, **=ОКРУГЛВВЕРХ(LOG(C2+1;2);0)**. Получили значение 18, таким образом, для кодирования числа *n* = 250981 требуется не менее 18 двоичных разрядов.

ЗАМЕЧАНИЕ: Округление вверх можно произвести также с помощью функций **ОКРВВЕРХ** или **ОКРВВЕРХ.ТОЧН**, в этом случае значение второго параметра (точность) следует установить равным 1.

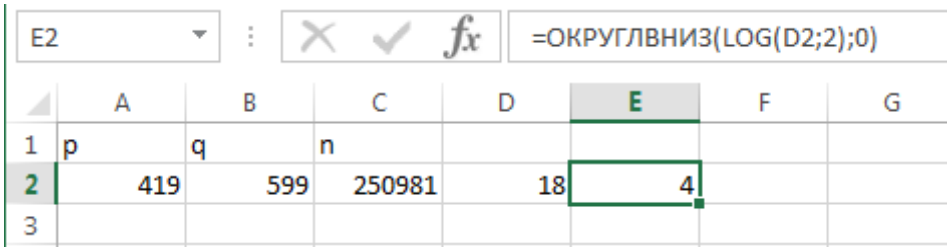


Рис. 52. Расчет максимально допустимого числа младших битов

- Взять двоичный логарифм от полученного значения, например, **=LOG(D2;2)**. Округлить полученное значение вниз с помощью функции **ОКРУГЛВНИЗ**, задав число десятичных разрядов равным 0, например, **=ОКРУГЛВНИЗ(LOG(D2;2);0)**. Получили 4, таким образом, в BBS-генераторе допустимо использовать не более 4 младших битов.

ЗАМЕЧАНИЕ: Округление вниз можно также произвести с помощью функций **ОКРВНИЗ** или **ОКРВНИЗ.ТОЧН**, в этом случае значение второго параметра (точность) следует установить равным 1.

10. С помощью значения-подсказки, восстановить значение x_0, использованное для генерации последовательности *ps*при шифровании. Сначала с помощью расширенного алгоритма Евклида следует найти значения *a* и*b*, такие что $ap + bq = 1$. Значения *a*и *b*существуют, так как числа *p* и *q*–простые, а значит, взаимно просты.Реализовать расширенный алгоритм Евклида (рис. 53):

- Сформировать первую строку алгоритма как: *max*(*p*,*q*);1; 0.
- Сформировать первую строку алгоритма как: *min*(*p*,*q*); 0; 1.
- Теперь следует вычислить значения в третьей строке алгоритма. В качестве первого элемента строки вычислить значение *max*(*p*,*q*)mod*min*(*p*,*q*) с помощью функции **ОСТАТ**, например, **=ОСТАТ(A4;A5)**для рис. 53.
- Вычислить четвертое значение в третьей строке как результат целочисленного деления *max*(*p*,*q*) на *min*(*p*,*q*) с помощью функции **ЧАСТНОЕ**. Например, для рис. 53 функция примет вид =**ЧАСТНОЕ(A4;A5)**.
- Второе и третье значения в строке вычисляются как разность соответствующего значения из первой строки и значения из

второй строки, помноженного на результат целочисленного деления. Например, в ячейку **B6**на рис. 53 будет занесена формула **=B4-B5*D6**, а в ячейку **C7** – формула **=C4-C5*D6**.

- Скопировать строку 3 на нижележащий диапазон ячеек, пока не будут получены значения #ДЕЛ/0!.
- Результаты вычисления (*a* и *b*) находятся во второй и третьей ячейках строки, начинающейся с 1.При этом меньшее по модулю значение соответствует большему из чисел *p* и*q*. В случае получения отрицательных значений*a* или *b*, их дальнейшее преобразование проводитьне надо.

  Для рассматриваемого примера получили: *a* = -203, *b* = 142.
- Провести проверку равенства *ap* + *bq* = 1.

  В примере получаем: -203 * 419 + 142 * 599 = 1, значит числа *a* и *b* определены правильно.

B10 | =B8-B9*D10

	A	B	C	D	E
1	p	q	n		
2	419	599	250981	18	4
3					
4	599	1	0		
5	419	0	1		
6	180	1	-1	1	
7	59	-2	3	2	
8	3	7	-10	3	
9	2	-135	193	19	
10	1	142	-203	1	
11	0	-419	599	2	
12	#ДЕЛ/0!	#ДЕЛ/0!	#ДЕЛ/0!	#ДЕЛ/0!	
13	#ДЕЛ/0!	#ДЕЛ/0!	#ДЕЛ/0!	#ДЕЛ/0!	
14					
15	1				

Рис. 53. Определение значений a и b с помощью расширенного алгоритма Евклида

- Вычислить значения α и β, воспользовавшись формулами: $\alpha = \left(\frac{p+1}{4}\right)^m \bmod(p-1)$, $\beta = \left(\frac{q+1}{4}\right)^m \bmod(q-1)$, где m – номер члена ряда x_i, переданного в качестве значения-подсказки.

В рассматриваемом примере $m = 6$. Поскольку показатель степени невелик, для вычисления α и β можно использовать последовательное умножение по модулю числа на само себя (рис. 54). Например, пронумеровать ячейки диапазона **G4:G9** от 1 до 6, вычислить в ячейке **H4** значение $(p + 1)/4$, в ячейку **H5** занести формулу **=ОСТАТ(H4*H$4;A$2-1)**, затем скопировать формулу на оставшиеся ячейки диапазона **H5:H9**. Ячейка **H9** содержит значение α ($\alpha = 49$ для рассматриваемого примера). Аналогичным образом вычислить значение β: в ячейке **I4** вычислить значение $(q + 1)/4$, скопировать формулу из ячейки **H5** на диапазон **I5:I9** (в примере $\beta = 584$).

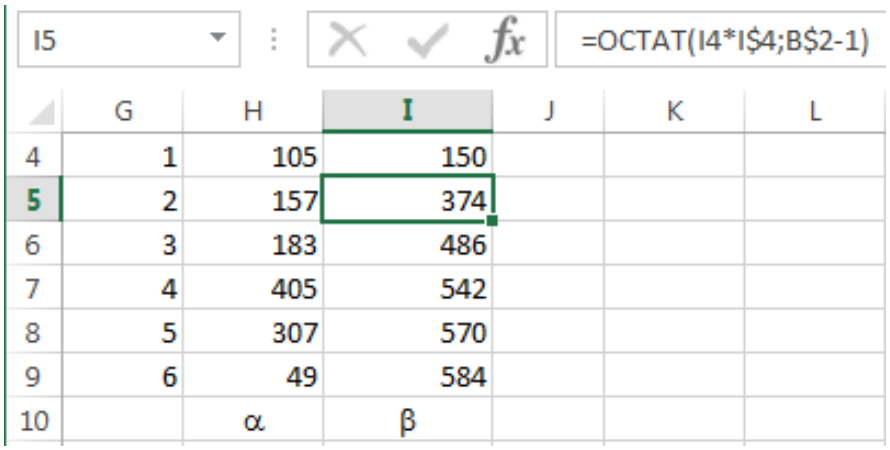


Рис. 54. Вычисление значений α и β

- Вычислитьзначения*r*и*t*, воспользовавшисьформулами:$r = (x_m \bmod p)^{\alpha} \bmod p$, $t = (x_m \bmod q)^{\beta} \bmod q$. Занести на лист MSExcelзначение-подсказку $x_m = x_6$. Для проведения вычислений реализовать быстрый алгоритм возведения в степень по модулю аналогично пункту 3 лабораторной работы №6 (Изучение шифра RSA). Для рассматриваемого примера получили: $r = 215$, $t = 54$ (рис. 55).

P22 =OCTAT(P21*O22;$B$2)

	G	H	I	J	K	L	M	N	O	P
10		α	β		x6					
11		110001	1001001000		3600					
12	n	6	10							
13	0	1	248	248	248		0	6	1	1
14	1	0	330	1	248		0	36	1	1
15	2	0	379	1	248		0	98	1	1
16	3	0	343	1	248		1	20	20	20
17	4	1	329	329	306		0	400	1	20
18	5	1	139	139	215		0	67	1	20
19	6				*r*		1	296	296	529
20	7						0	162	1	529
21	8						0	487	1	529
22	9						1	564	564	54
23										*t*
24					x0	141418				

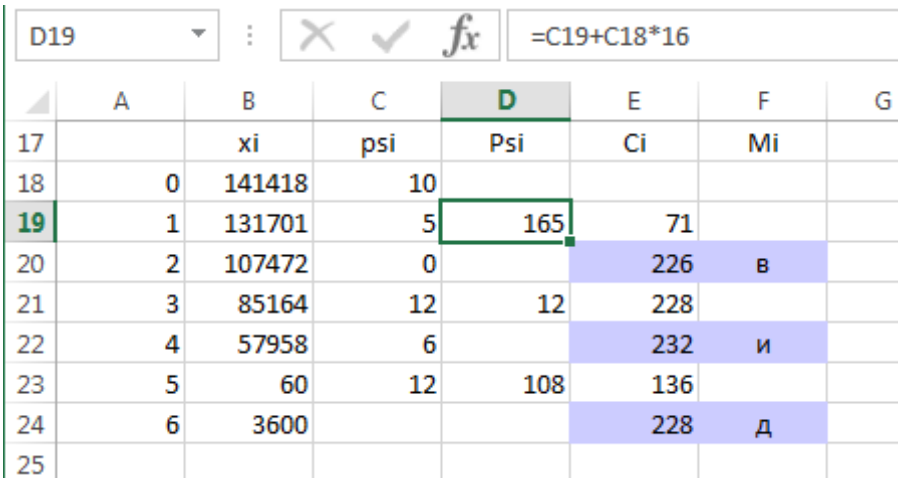
Рис. 55. Вычисление значений r и t

- Вычислить значение x_0, воспользовавшись формулой $x_0 = (apt + bqr) \bmod n$. Для вычислений использовать функцию **ОСТАТ**. В примере получили: $x_0 = 141418$.

11. Зная значения x_0 и n, восстановить элементы исходной последовательности *ps* и расшифровать криптограмму (рис. 56):

- Определить число членов ряда x_i, необходимых для формирования псевдослучайной последовательности достаточной для шифрования/расшифрования длины. Для этого число ASCII-кодов, задающих шифртекст, следует умножить на 8 и разделить на полученное максимально допустимое число младших битов. Для рассматриваемого примера получаем: 3·8/4 = 6, то есть требуется сформировать 6 чисел ряда x_i.
- Пронумеровать ячейки первого столбца числами от 0 до 6. В первую ячейку второго столбца занести значение x_0, в следующей вычислить x_1 по формуле $x_1 = x_0^2 \bmod n$, используя функцию **ОСТАТ** (аналогично пункту 3). Например, **=ОСТАТ(B18^2;$C$2)** для ячейки **B19**. Проверить, что полученное значение x_6 совпало с присланным значением-подсказкой.
- Во втором столбце сформировать фрагменты последовательности *ps*, соответствующие значениям ряда $\boldsymbol{x}_0 - \boldsymbol{x}_5$ (число-подсказка x_6 не участвует в формировании последовательности *ps*). Поскольку ис-

пользованы 4 младших бита чисел x_i, в десятичном виде фрагменты *ps* можно получить в виде остатка от целочисленного деления на 2^4 = 16. Например, **=ОСТАТ(B18;16)** для ячейки **C18**.



	A	B	C	D	E	F	G
17		xi	psi	Psi	Ci	Mi	
18	0	141418	10				
19	1	131701	5	165	71		
20	2	107472	0		226	в	
21	3	85164	12	12	228		
22	4	57958	6		232	и	
23	5	60	12	108	136		
24	6	3600			228	д	
25							

Рис. 56. Расшифрование сообщения

- Поскольку шифрованию подвергались 8-битовые значения (ASCII-коды символов сообщения), сформировать 8-битовые фрагменты последовательности *ps*, сгруппировав полученные 4-битовые фрагменты по 2. В десятичном виде это можно сделать, умножив первое значение на 16 и добавив к нему второе. Например, **=C19+C18*16** для ячейки **D19**.
- Занести на лист MSExcel последовательность кодов криптограммы. Выполнить операцию побитового Xor соответствующих 8-битовых фрагментов *ps* и кодов криптограммы. Для этих целей можно воспользоваться функцией **БИТ.ИСКЛИЛИ** (в MSExcel 2013) или операцией *Xor* в режиме Программист стандартного Калькулятора MSWindows. Например, **=БИТ.ИСКЛИЛИ(D19;E19)** для ячейки **E20**.
- Перевести полученные ASCII-коды в символы открытого текста с помощью функции **СИМВОЛ** группы *Текстовые*. Например, **=СИМВОЛ(E20)** для ячейки **F20**. Получение осмысленного текста является критерием правильности расшифрования сообщения.

  В примере получен текст «вид».

12. Продемонстрировать результаты выполнения практической работы преподавателю.

ТЕМА 4. КРИПТОСИСТЕМЫ С ОТКРЫТЫМ КЛЮЧОМ

Концепция криптографии с открытым ключом была предложена УитфилдомДиффи (WhitfieldDiffie) и Мартином Хеллманом (MartinHellman), и, независимо от них, Ральфом Мерклом (RalphMerkle). Основная идея заключается в том, чтобы использовать ключи парами, состоящими из ключа шифрования и ключа расшифрования, которые невозможно вычислить один из другого.

Алгоритм является общедоступным, нет необходимости в секретных каналах связи. Общая схема выглядит следующим образом:

1. Каждый пользователь генерирует пару ключей: один для шифрования (открытый ключ), другой для расшифрования (личный ключ).

2. Каждый пользователь публикует свой ключ шифрования, размещает его в открытом для всех доступе. Второй ключ, парный открытому – это личный ключ, он сохраняется в секрете.

3. Если пользователь А собирается послать сообщение пользователю В, он шифрует сообщение открытым ключом пользователя В.

4. Когда пользователь В получает криптограмму, он расшифровывает ее с помощью своего личного (секретного) ключа. Другой получатель не сможет дешифровать сообщение, поскольку личный ключ В известен только абоненту В.

Наиболее широкое распространение получила Схема Райвеста–Шамира–Адлемана (RSA).

Асимметричные криптосистемы (и, в частности, шифр RSA) могут быть использованы и для подтверждения авторства (подписания сообщений). В этом случае:

1. Если пользователь А собирается послать подписанное сообщение пользователю В, он шифрует сообщение своимличным ключом.

2. Теперь любой, в том числе и пользователь В сможет удостовериться в авторстве и неизменности сообщения, расшифровавприсланную с ним криптограмму с помощью открытого ключа отправителя А и сравнив результат с открытым текстом.

Совпадение открытого и расшифрованного текстов свидетельствует о подлинности авторства и неизменности переданного сообщения. Никто другой не сможет подписать сообщение от лица А, поскольку личный ключ известен только абоненту А.

Практическая работа №9. Изучение шифра RSA

Описание алгоритма шифрования

Перед началом процесса шифрованияисходный текст должен быть переведен в числовую форму (с помощью таблицы замен), этот метод считается известным. В результате текст представляется в виде одного большого числа. Затем полученное число разбивается на части (блоки) так, чтобы каждая из них была числом в промежутке от 0 до $N-1$, (о выборе числа Nбудет рассказано далее). Процесс шифрования одинаков для каждого блока. Поэтому можно считать, что блок исходного текста представлен числом x, $0 \le x \le N-1$.

Конечно, выбор блоков неоднозначен, но и не совсем произволен. Например, во избежание двусмысленностей, не следует выделять блоки, начинающиеся с нуля.

Разбиение числа на блоки можно произвести различными способами. При этом промежуточные результаты зависят от способа разбиения, однако конечный результат – не зависит.

При расшифровании, наоборот, полученная последовательность блоков соединяется вместе и получаетсябольшое число. После этого числа заменяют буквами в соответствии с таблицей замен для получения исходного сообщения.

Опишем процесс шифрования. Каждый абонент вырабатывает свою пару ключей. Для этого он генерирует два больших простых числа p и q, вычисляет произведение $N=p \cdot q$. Затем он вырабатывает случайное число e, взаимно простое со значением функции Эйлера $\varphi(N)$ от числа N: $\varphi(N)=(p-1)\cdot(q-1)$, и находит число d из условия $e \cdot d = 1 (\mathrm{mod}\, \varphi(N))$. Так как eи $\varphi(N)$– взаимно простые:НОД$(e,\varphi(N))=1$, то такое число d существует и оно единственно.

Пара (N, e) объявляется открытым ключом абонента и помещается в открытый доступ. Пара (N, d) является личным (сек-

ретным) ключом. Для расшифрования достаточно знать секретный ключ. Числа p, q, $\varphi(N)$ в дальнейшем не нужны, поэтому их можно уничтожить.

Пользователь А, отправляющий сообщение x абоненту В, выбирает из открытого каталога пару (N, e) абонента В и вычисляет шифрованное сообщение $y=x^e(\mathrm{mod}N)$.

Чтобы получить исходный текст, абонент В вычисляет $y^{d-}\mathrm{mod}N$.

Пример. Пусть p=7, q=17. Тогда N=7·17=119, $\varphi(N)$=6·16=96. Выбираем значение e: e<96, НОД(e,96)=1. Пусть выбрано e=5. Находимd: $e\cdot d=1(\mathrm{mod}\varphi(N))$, $d=e^{-1}(\mathrm{mod}\varphi(N))$. С помощью расширенного алгоритма Евклида получаем d=77 (77·5=4·96+1).

Открытый ключ (119,5), личный ключ (119,77). Пусть теперь x=19. Для зашифрования число 19 возводим в 5-ю степень по модулю 119, тогда имеем 19^5=2 476 099 и остаток от целочисленного деления этого значения на 119 равен 66. Итак, $y=19^5\mathrm{mod}119=66$. При расшифровании же получим:$x=66^{77}\mathrm{mod}119=19$.

Упрощение вычислений

Как шифрование, так и расшифрование в RSA предполагают использование операции возведения целого числа в целую степень по модулю p. Если возведение в степень выполнять непосредственно с целыми числами и только потом проводить сравнение по модулю p, то промежуточные значения окажутся огромными. Здесь можно воспользоваться свойствами арифметики в классах вычетов $a\cdot b\mathrm{mod}p = ((a\mathrm{mod}p)\cdot b)\mathrm{mod}p=((a\mathrm{mod}p)\cdot(b\mathrm{mod}p))\mathrm{mod}p$. Таким образом, можно рассмотреть промежуточные результаты по модулю p. Это позволяет получить значение большой степени по модулюс помощью итерационных вычислений. Итерационный алгоритм будет иметь линейную сложность относительно показателя степени.

Например, длявычисления 88^3mod 23, можно выполнить следующее преобразование:

$88^3\mathrm{mod}23=((88\mathrm{mod}23)\cdot 88\mathrm{mod}\ 23)\cdot 88\mathrm{mod}23=$

$=((19\cdot 88)\mathrm{mod}23)\cdot 88\mathrm{mod}23=(1672\mathrm{mod}23)\cdot 88\mathrm{mod}23=$

$16\cdot 88\mathrm{mod}23=1408\mathrm{mod}23=5$.

Существует и более эффективный алгоритм вычисления большой степени числа, основанный на возведении в квадрат по модулю p.Степень xпри вычислении значения a^xпредставляется в виде последовательности операций умножения на 2 и сложения с 1. Пусть, например, требуется вычислить $a^{100}\mathrm{mod}p$. Представим степень как $100=2(2(1+2\cdot2\cdot2(1+2)))$. Тогдавозведениевстепень$a^{100}=(((((a^2\cdot a)^2)^2)^2\cdot a)^2)^2$, $a^{100}\mathrm{mod}p=(((((((a^2\mathrm{mod}p)\cdot(a\mathrm{mod}p))^2\mathrm{mod}p)^2\mathrm{mod}p)^2\mathrm{mod}p)\cdot (a\mathrm{mod}p))^2\mathrm{mod}p)^2\mathrm{mod}p$.

Вычислим $7^{100}\mathrm{mod}23$, получаем 16 (табл. 28).

Таблица 28

Пример быстрого вычисления степени по модулю

	7^2 mod 23	$x\cdot7$ mod 23	x^2 mod 23	x^2 mod 23	x^2 mod 23	$x\cdot7$ mod 23	x^2 mod 23	x^2 mod 23
x	3	21	4	16	3	21	4	16

Такимобразом, возведение в степень 100 производится путем 2 умножений и 6 возведений в квадрат по модулю(то есть всего 8 операций).

Количество операций умножения при вычислении a^xметодомповторного возведения в квадратне превосходит $2\log x$.

Для нахождения числа d, удовлетворяющего сравнению $e\cdot d\equiv1(\mathrm{mod}\varphi(N))$, то есть инверсии e по модулю $\varphi(N)$: $d=e^{-1}\mathrm{mod}\varphi(N)$, может быть использован расширенный алгоритм Евклида.

На вход алгоритма подаются числа $\varphi(N)$, e, $\varphi(N)>e$.

1. Формируются строки: $U=\{u_1,u_2\}\leftarrow\{\varphi(N),0\}$;
   $V=\{v_1,v_2\}\leftarrow\{e,1\}$.
2. ПОКА $v_1\neq0$:
   3. $k\leftarrow u_1 div v_1$
   4. $T=\{t_1; t_2\}\leftarrow\{u_1 mod v_1; u_2-k\cdot v_2\}$
   5. $U\leftarrow V$, $V\leftarrow T$
6. РЕЗУЛЬТАТ$U=\{u_1; u_2\}=\{НОД(\varphi(N),e);d\}$

Пусть, например, e=19, $\varphi(N)=28$, требуется найти значение $d=e^{-1}(\mathrm{mod}\varphi(N))$.

Вычисления с помощью расширенного алгоритма Евклида представлены на рис. 57.

В начале в строку Uзаписываются значения {28,0}, а в строку V–{19,1} (это две первые строки в схеме). Вычисляется T (третья строка). После этого в качестве Uберется вторая, а в качестве V–третья строка в схеме, и вычисляется новое значение T (четвертая строка). Этот процесс продолжается до тех пор, пока первый элемент строки Vне окажется равным 0. Тогда строка U (предпоследняя в схеме) содержит ответ.

шаг	1	2	3	результат	строки		k
	U				28	0	
	V	U			19	1	
1	T	V	U		9	-1	1
2		T	V	U	1	3	2
3			T	V	0	-28	9

Рис. 57. Пример вычисления числа, обратного по модулю, с помощью расширенного алгоритма Евклида

В рассматриваемом примере получаем: НОД(28,19)=1, $d = 3$.

Задание

Выполнить шифрование, проверку аутентичности и дешифрование по алгоритму RSA, зная только открытые ключиабонентов криптосистемы RSA.

Технология выполнения задания

ЗаданиеА.Известны открытые ключи (N, e) абонентов криптосистемы RSA (табл.29).Кодирование символов сообщения осуществляется с помощью таблицы 30 (буквы «е» и «ё» не различаются). Найти значение передаваемого между абонентами шифртекстаY.

Таблица 29

Справочник открытых ключей абонентов криптосистемы RSA

Абонент	Ключ (N, e)	Абонент	Ключ (N, e)	Абонент	Ключ (N, e)
A	(5017, 251)	F	(8809,307)	K	(4553, 241)
B	(8471, 125)	G	(6077,619)	L	(6757, 233)
C	(4559, 311)	H	(5513,607)	P	(8413, 507)
D	(3403, 211)	I	(7747, 353)	Q	(6313, 749)
E	(5177, 179)	J	(5561, 433)	R	(9301, 387)

Таблица 30

Таблица кодирования символов открытого текста

Символ	а	б	в	г	д	е	ж	з	и	й	к	л	м	н	о	п
код	11	12	13	14	15	16	17	18	19	21	22	23	24	25	26	27
Символ	р	с	т	у	ф	х	ц	ч	ш	щ	ъ	ы	ь	э	ю	я
код	28	29	31	32	33	34	35	36	37	38	39	41	42	43	44	45

1. Выбрать параметры передачи шифртекста в системеRSAи открытый текст изтаблицы 31в соответствии с номером варианта.

Изучить теоретическое описание алгоритма RSA. Выполнить шифрование по аналогии с рассмотренным далее примером.

Пример. Пусть осуществляется передача шифртекста от абонента A1 к абоненту A2. И пусть получатель – абонент A2 имеет открытый ключ N = 2537,e = 199, требуется зашифровать с помощью алгоритмаRSA текст «зима».

Таблица 31

Варианты задания

№	Передача текста	№	Передача текста	№	Передача текста
1	A→B; заря	**10**	H→J; сани	**19**	L→D; звук
2	C→D; клуб	**11**	K→P; клан	**20**	Q→B; соло
3	E→A; небо	**12**	L → Q; лист	**21**	I → A; пара
4	B → C; высь	**13**	I → K; крен	**22**	R → G; сеть
5	F → E; зонд	**14**	Q → R; свет	**23**	H → Q; один
6	J → F; семь	**15**	D → L; звон	**24**	P → F; рост
7	P → I; дело	**16**	A → H; ключ	**25**	B → K; метр
8	R → G; пять	**17**	K → F; курс		
9	G → H; слон	**18**	E → P; байт		

2. Подготовить открытый текст к шифрованию, задав для него числовое представление.

- Занести на новый лист книги MSExcelпараметры криптосистемы RSA: числа N и e, а также открытый текст (посимвольно).
- Закодировать текст с помощью таблицы 30, занеся коды символов на лист MSExcel:

з	и	м	а
18	19	24	11

ЗАМЕЧАНИЕ: Процесс перевода текста в числовые коды можно автоматизировать, если таблицу 30 занести на лист MSExcelи использовать функцию **ГПР** (для горизонтального представления таблицы) или **ВПР** (для вертикального представления) группы *Ссылки и массивы*.

- Объединить коды символов текста в общую последовательность символов: числовое представление открытого текста X = 18192411.В MSExcelдля этого можно использовать операцию конкатенации **&**, например, **=C3&D3&E3&F3** (рис. 58).

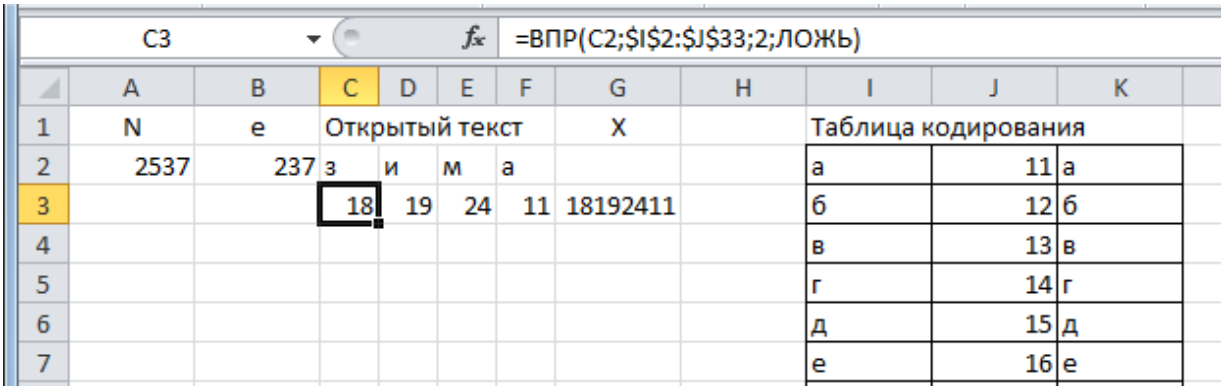


Рис. 58. Занесение исходной информации на лист MSExcel

- Разбитьпоследовательность цифр X на части так, чтобы $X_i<N$, ни одна часть не содержит ведущих нулей. Поскольку N=2537, X_i<2537:

  X_1=1819,X_2=2411.

  Занести полученные значения на лист MSExcel.

3. Зашифровать X_1 по формуле: $Y=X^e \bmod N$.Для вычислений можно использовать табличный процессор MSExcel. Подготовить

реализацию алгоритма для быстрого вычисления степени по модулю последовательным возведением в квадрат:

- Перевестизначение степени *e*в двоичное представление.В среде MSExcel для этих целей можно воспользоваться функцией **ДЕС.В.ДВ** группы *Инженерные* (например, **=ДЕС.В.ДВ(B2)**).

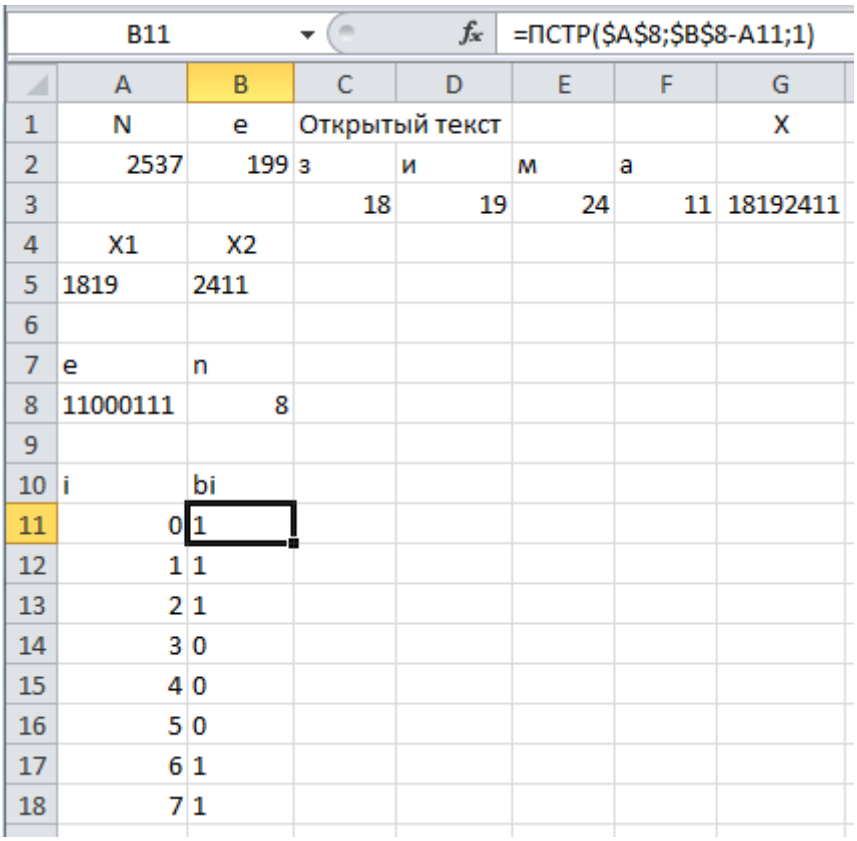
ЗАМЕЧАНИЕ: Функция **ДЕС.В.ДВ**осуществляет перевод значений только в диапазоне от -512 до 511. Если число *e* выходит за рамки указанного диапазона, следует воспользоваться стандартным приложением MSWindows Калькулятор, режим (вид) *Программист*. В этом случае следует установить переключатель системы счисления в позицию *Dec* (десятичная), ввести число *e*, а затем установить переключатель в позицию *Bin* (двоичная). Число будет переведено в двоичную систему счисления. Занести значение *e*в двоичной системе счисления на лист MSExcel.

Для рассматриваемого примера получили $e = 11000111_2$.

- Определить*n*– число разрядов двоичного представления числа *e*. В среде MSExcel для этих целей можно воспользоваться функцией **ДЛСТР** группы Текстовые. Пусть значение ***e***в двоичной системе счисления занесено в ячейку **A8**. Тогда в ячейку **A9**следует занести формулу **=ДЛСТР(A8)**.

  Для рассматриваемого примера получили *n*= 8.

- Сформировать таблицу для вычисления степени *e* по модулю *N*. В ячейки столбца **A**(ниже значений *e* и *n*) занести значения от 0 до *n*-1 (в примере – от 0 до 7), задав заголовок столбца: *i*.
- В соответствующие ячейки столбца **B** занести значения двоичных разрядов b_i(начиная с младшего разряда), для чего воспользоваться функцией **ПСТР** группы *Текстовые*, например, **=ПСТР($A$8;$B$8-A11;1)**– рис. 59.



B11 | =ПСТР($A$8;$B$8-A11;1)

	A	B	C	D	E	F	G
1	N	e	Открытый текст				X
2	2537	199	з	и	м	а	
3			18	19	24	11	18192411
4	X1	X2					
5	1819	2411					
6							
7	e	n					
8	11000111	8					
9							
10	i	bi					
11	0	1					
12	1	1					
13	2	1					
14	3	0					
15	4	0					
16	5	0					
17	6	1					
18	7	1					

Рис. 59. Выделение битов двоичного представления степени e

- В соответствующих ячейках столбца **C**вычислить значения ряда x^{2^i}, задав заголовок столбца x_i.В ячейку **C11**занести ссылку на исходное значение (которое надо будет возвести в степень, пусть оно будет помещено в ячейку **C8**), тогда ячейка **C11**должна содержать формулу **=C8**, в ячейку **C12**–формулу для вычисления квадрата по модулю *N*: **=ОСТАТ(C11^2;$A$2)**, ячейка **A2** содержит значение *N*.Скопировать формулу из **C12**на оставшийся диапазон ячеек столбца **C** (рис. 60).
- В ячейки столбца **D**занести значение 1, если соответствующее значение бита b_i = 0(из столбца**B**) или значение x^{2^i} (из столбца **C**), если b_i = 1. Для этих целей воспользоваться функцией **ЕСЛИ** группы *Логические*. Формула в ячейке **D11**имеет вид: **=ЕСЛИ(B11="0";1;C11)**. Скопировать формулу из **D11**на оставшийся диапазон ячеек столбца **D**(рис.60).
- В столбце **E**подсчитать произведение значений из столбца **D**по модулю. Для этого в ячейку **E11**ввести формулу **=D11**, в ячей-

ку **E12**–формулу **=ОСТАТ(E11*D12;$A$2)**. Скопировать формулу на оставшийся диапазон ячеек столбца **E** (рис.60).

Последняя заполненная ячейка столбца **E** (**E18** в примере) содержит результат вычисления степени по модулю. Подписать эту ячейку как *y*.

E18 =ОСТАТ(E17*D18;$A$2)

	A	B	C	D	E	F	G
7	e	n	X				
8	11000111	8	1819				
9							
10	i	bi	xi				
11	0	1	1819	1819	1819		
12	1	1	513	513	2068		
13	2	1	1858	1858	1326		
14	3	0	1844	1	1326		
15	4	0	756	1	1326		
16	5	0	711	1	1326		
17	6	1	658	658	2317		
18	7	1	1674	1674	2122		
19					y		
20	Y1						
21	2122						

Рис. 60. Результаты вычисления степени по модулю

- Занести в ячейку для исходных данных (**C8**) значение X_1=1819. Ячейка, помеченная как *y*,будет содержать значение Y_1. Скопировать полученное значение (использовать вставку только значений), подписав его (рис.60).

В рассматриваемом примере результат шифрования X_1 – значение Y_1 = 2122.

4. Зашифровать X_2:

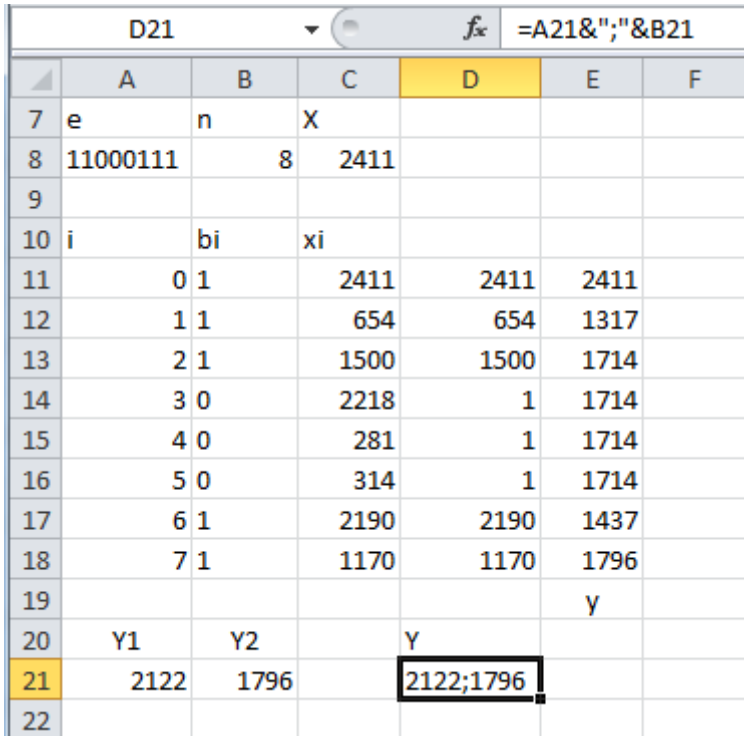
- Занести в ячейку для исходных данных (**C8**) значение X_2=2411. Ячейка, помеченная как *y*, будет содержать значение Y_2. Скопировать полученное значение, подписав его.

В рассматриваемом примере результат шифрования X_2 – значение Y_2 =1796.

5. Сформировать результирующее значение криптограммы, сцепив полученные значения Y_1 и Y_2 через знак точки запятой

(можно использовать операцию конкатенации &, например, **=A21&";"&B21**)–рис.61.

В примере получена криптограмма Y = 2122;1796для передачи абоненту А2.



D21 | =A21&";"&B21

	A	B	C	D	E	F
7	e	n	X			
8	11000111	8	2411			
9						
10	i	bi	xi			
11	0	1	2411	2411	2411	
12	1	1	654	654	1317	
13	2	1	1500	1500	1714	
14	3	0	2218	1	1714	
15	4	0	281	1	1714	
16	5	0	314	1	1714	
17	6	1	2190	2190	1437	
18	7	1	1170	1170	1796	
19					y	
20	Y1	Y2		Y		
21	2122	1796		2122;1796		
22						

Рис. 61. Получение значения криптограммы Y

ЗаданиеВ.Абоненты криптосистемы RSAобмениваются открытыми сообщениями с подтверждением авторства. Проверить аутентичность сообщения, если известны открытые ключи (N, e) абонентов криптосистемы (табл.29). Кодирование символов сообщения осуществляется с помощью таблицы 30 (буквы «е» и «ё» не различаются).

6. Выбратьпараметры передачи текста в системе RSA,передаваемый открытый тексти проверочный код из таблицы 32в соответствии с номером варианта.

Таблица 32

Варианты задания

№	Передача текста	Подпись	№	Передача текста	Подпись
1	R→A; акт	1019;8218	**14**	D → B; год	2879;1136
2	I→B; фен	6201;1357	**15**	C → A; воз	4459;1492
3	J→C; сын	2484;3766	**16**	F→P; йод	5228;296
4	C → D; вес	2115;3906	**17**	G→D; сор	1808;4252
5	E → I; жар	1142;3017	**18**	H → E; сын	2751;1804
6	L → J; гол	3296;6081	**19**	I → K; дом	794;1883
7	Q → E; куб	5238;49	**20**	K → J; кот	79;2832
8	K → C; вал	3629;54	**21**	J → H; дым	2077;2367
9	G → F; лаз	111;1230	**22**	L → Q; зал	3909;3851
10	F→K; кит	3321;5454	**23**	Q → I; час	3176;3250
11	A → C; мир	3787;2087	**24**	P → G; пес	1235;2661
12	B → R; луг	6248;6318	**25**	R → F;вид	6216;7221
13	E → L; сом	261;1386			

Поскольку сообщение подписывается абонентом с помощью своего личного ключа, проверка осуществляется с использованиемоткрытого ключа отправителя. Выполнить проверку аутентичности сообщения по аналогии с рассмотренным далее примером.

Пример. Пусть от абонента A1 к абоненту A2передантекст «зал» с подписью (проверочным кодом)$Y = (Y_1;Y_2) = 1698;988$. И пусть отправитель – абонент A1 имеет открытый ключ $N = 3403$, $e = 143$.

7. Расшифровать части проверочного кода открытым ключом отправителя, используя формулу $X = Y^e \bmod N$:

- Для каждого из частей Y_i проверочного кода вычислить значение X_i,реализовав алгоритм быстрого возведения в степень по модулю (аналогично пункту 3 задания А).

  В рассматриваемом примере получено: $X_1 = 1811$, $X_2 = 23$.
- Сцепить полученные значения X_i (с помощью операции **&**), а затем разбить на двузначные числа (функции **ПСТР** и **ЗНАЧЕН**) для определения символов сообщения.

  В примере коды символов сообщения: 18, 11, 23.

- Перевести полученные коды в символы, используя таблицу 30(для автоматизации использовать функцию **ВПР**).

В примере получили символы: з, а, л (рис.62). Поскольку полученное слово совпадает с переданным открытым сообщением, аутентичность последнего подтверждена.

F41 f_x =ЗНАЧЕН(ПСТР($D$41;1;2))

	A	B	C	D	E	F	G	H	I
24	N	e		Y1	Y2				ц
25	3403	143		1698	988				ч
26									ш
27	e	n	Y						щ
28	10001111	8	988						ъ
29									ы
30	i	bi	xi						ь
31	0	1	988	988	988				э
32	1	1	2886	2886	3057				ю
33	2	1	1855	1855	1337				я
34	3	1	592	592	2008				
35	4	0	3358	1	2008				
36	5	0	2025	1	2008				
37	6	0	10	1	2008				
38	7	1	100	100	23				
39									
40	X1	X2		Y					
41	1811	23		181123		18	11	23	
42						з	а	л	

Рис. 62. Вычисления для проверки аутентичности сообщения

ЗаданиеС.При передаче между абонентами перехвачена криптограмма *Y*, полученнаяшифрованием по алгоритму RSA.Дешифровать *Y*, вычислив секретный ключ *d*.Известны открытые ключи абонентов (табл. 29).Кодирование символов сообщения осуществляется с помощью таблицы 30.

8. Выбрать параметры шифраRSA и криптограмму***Y***в соответствии с номером варианта (табл.33,выбор осуществляется по порядковому номеру в официальном списке группы).

Таблица 33

Варианты задания

№	Абоненты	Криптограмма ***Y***	№	Абоненты	Криптограмма ***Y***
1	F→P	3872;5862	**14**	C → D	1386;193
2	G→E	4611;693	**15**	E → I	2421;6015
3	H → D	338;2187	**16**	L → J	4737;5282
4	I → K	2452;2200	**17**	Q → E	1172;1127
5	K → J	1889;67	**18**	K → C	115;1462
6	J → H	3722;1864	**19**	G → F	1071;6911
7	L → Q	2091;3156	**20**	F→K	3760;3167
8	Q → I	2130;7168	**21**	A → C	3341;3627
9	P → G	4554;2122	**22**	B → R	3978;5215
10	R → F	314;3906	**23**	E → L	4357;1114
11	R→A	1697;2777	**24**	D → B	4461;7243
12	I→B	1085;3979	**25**	C → A	3438;4112
13	J→R	5584;2224			

Выполнить дешифрование криптограммы по аналогии с рассмотренным далее примером.

Пример.От абонента A1 к абоненту A2 переданакриптограмма$Y = (Y_1;Y_2) = 1726;1996$. Известен открытый ключ получателя N=2537; e=199.

9. Для дешифрования необходимо получить личный ключ *d*получателякриптограммы. Для этоготребуется решить задачу факторизации (разложения на простые множители)числа N. Эта задача является вычислительно сложной, ее можно решить перебором всех простых чисел до тех пор, пока не будет найден один из множителей. В общем случае такой перебор неэффективен, и при используемых на практике параметрах шифра RSAневозможен в силу вычислительной сложности. Однако поскольку в примере ***N*** – небольшое число, его разложение на множители практически осуществимо. Для решения задачи разложения на множители можно воспользоваться инструментом**Поиск решения**MSExcel:

- На новом листе книги MSExcel ввести в ячейки **A1** и **B1** значение 10. В ячейку **B2** ввести формулу: =**A1***B1.

- Проверить наличие инструмента **Поиск решения** на вкладке **Данные** в группе *Анализ*. Если инструмент отсутствует, следует его включить, для этого выполнить команду **Файл/Параметры**, перейти на вкладку *Надстройки*, в строке *Управление* выбрать *Надстройки Excel* и щелкнуть кнопку **Перейти**, затем в окне *Надстройки* установить флажок рядом с пунктом *Поиск решения* и нажать **ОК** (рис.63).

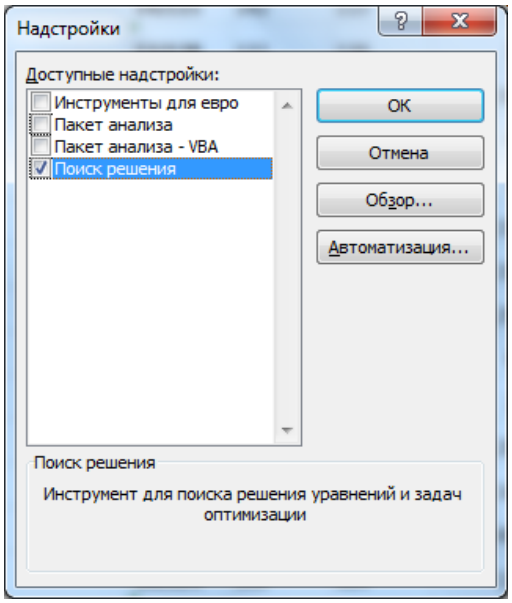


Рис. 63. Включение надстройки Поиск решения

- Выбрать ячейку **B2** (в которой подсчитано произведение двух множителей) и вызвать инструмент **Поиск решения** (вкладка **Данные**).
- В окне *Поиск решения* установить целевую ячейку – **$B$2** равной значению *N* (в примере – 2537), в поле *Изменяя ячейки переменных* выделить диапазон ячеек **$A$1:$B$1**, в группе *В соответствии с ограничениями* нажать кнопку **Добавить**, в окне *Добавление ограничения* в поле *Ссылка на ячейку* выделить диапазон ячеек **$A$1:$B$1**, в следующем поле выбрать значение *цел* и нажать **ОК** (рис.64). Будет установлено ограничение **$A$1:$B$1=целое**. Результирующий вид окна настроек инструмента **Поиск решения** показан на рис.65.

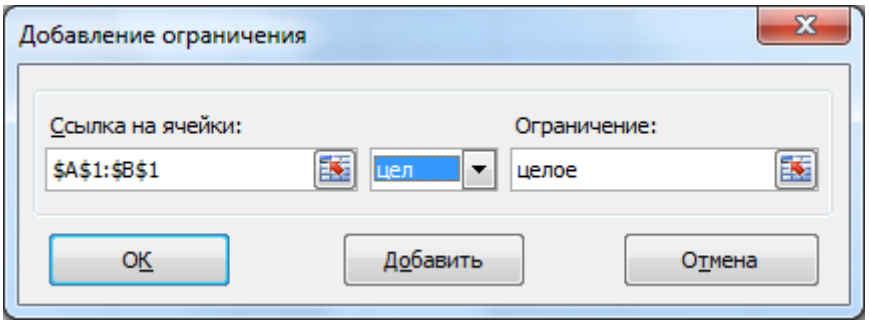


Рис. 64. Задание ограничений на изменяемые ячейки

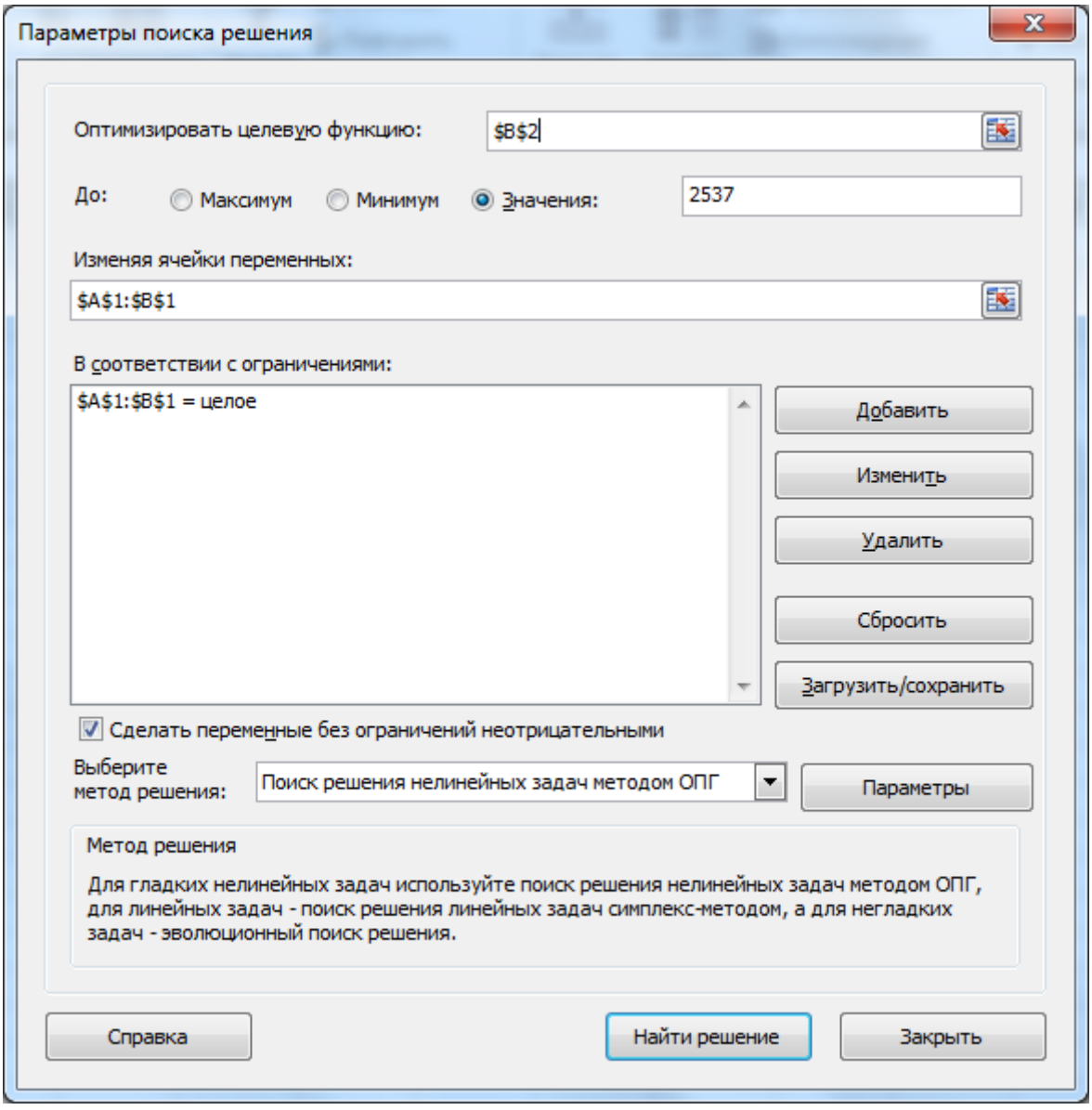


Рис. 65. Настройка инструмента ***Поиск решения***

- В окне *Поиск решения* выбрать метод решения *Поиск решения нелинейных задач методом ОПГ*, затем нажать кнопку **Пара-**

метры и на вкладке *Все методы* установить *Максимальное время*: 1000 и *Предельное число итераций*: 10000. Нажать **ОК**.

- После того, как инструмент **Поиск решения** полностью настроен, в окне *Поиск решения* нажать кнопку **Выполнить**. Будет выдано окно *Результаты поиска решения* с сообщением о том, что решение найдено – установить переключатель в позицию *Сохранить найденное решение* и нажать **ОК**. В ячейках **A1** и **B1** будут получены значения простых сомножителей числа *N*.

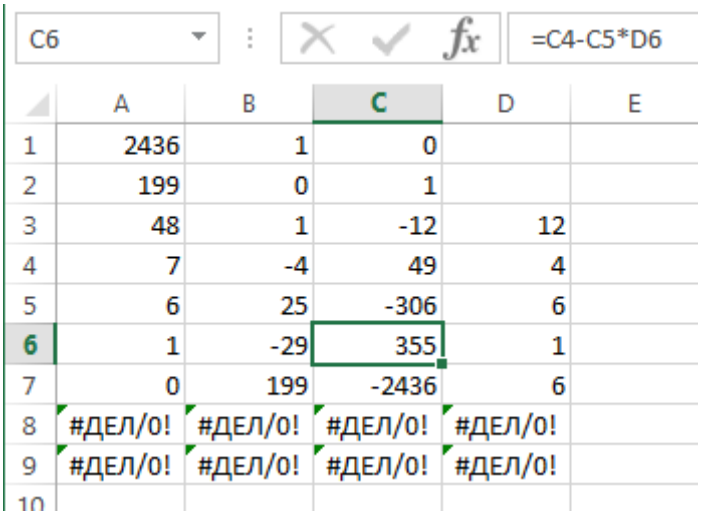
В рассматриваемом примере после выполнения поиска решения в ячейке **A1** будет установлено значение 19, а в ячейке **B1** – 29. Это и есть множители числа N= 551.

ЗАМЕЧАНИЕ: Если один из множителей окажется равным 1, то следует изменить начальные значения в ячейках A1 и B1, а затем повторно выполнить поиск решения.

10. Получили: p=43, q=59. Поскольку оба числа простые, легко вычислить значение $\varphi(N)$:
$\varphi(N)=\varphi(p\cdot q)=(p-1)\cdot(q-1)=42\cdot 58=2436$.
11. Зная значение $\varphi(N)$ и e, можно вычислить секретный ключ d из условия $e\cdot d\equiv 1(\mathrm{mod}\varphi(N))$, $d = e^{-1}\mathrm{mod}\varphi(N)$. Для вычисления dследует воспользоваться расширенным алгоритмом Евклида:

- Сформировать первую строку (U) расширенного алгоритма Евклида: на новом листе в ячейку **A1** занести значение $\varphi(N)$ =2436, в ячейку **B1** – 1, **C1** – 0.
- Сформировать вторую строку (V) расширенного алгоритма Евклида: в ячейку **A2** занести значение e– 199, в ячейку **B2** – 0, **C2** – 1.
- Вычислить значение $k=u_1 div v_1$: в ячейку **D3** занести формулу: =**ЧАСТНОЕ(A1,A2)**.
- Сформировать строку $T=\{u_1 \bmod v_1,\ u_2–k*v_2,\ u_3 –k*v_3\}$ расширенного алгоритма Евклида: в ячейку **A3** занести формулу: =**ОСТАТ(A1,A2)**, в ячейку **B3** – формулу =**B1-B2*D3**, в ячейку **C3** – формулу =**C1-C2*D3**.
- Выделить диапазон ячеек **A3:D3** и растянуть (скопировать) на несколько строк вниз, пока в столбце **A** не будет получено нулевое значение.

Результаты реализации расширенного алгоритма Евклида для рассматриваемого примера показаны на рис. 66.



	A	B	C	D	E
1	2436	1	0		
2	199	0	1		
3	48	1	-12	12	
4	7	-4	49	4	
5	6	25	-306	6	
6	1	-29	355	1	
7	0	199	-2436	6	
8	#ДЕЛ/0!	#ДЕЛ/0!	#ДЕЛ/0!	#ДЕЛ/0!	
9	#ДЕЛ/0!	#ДЕЛ/0!	#ДЕЛ/0!	#ДЕЛ/0!	
10					

Рис. 66. Пример реализации расширенного алгоритма Евклида

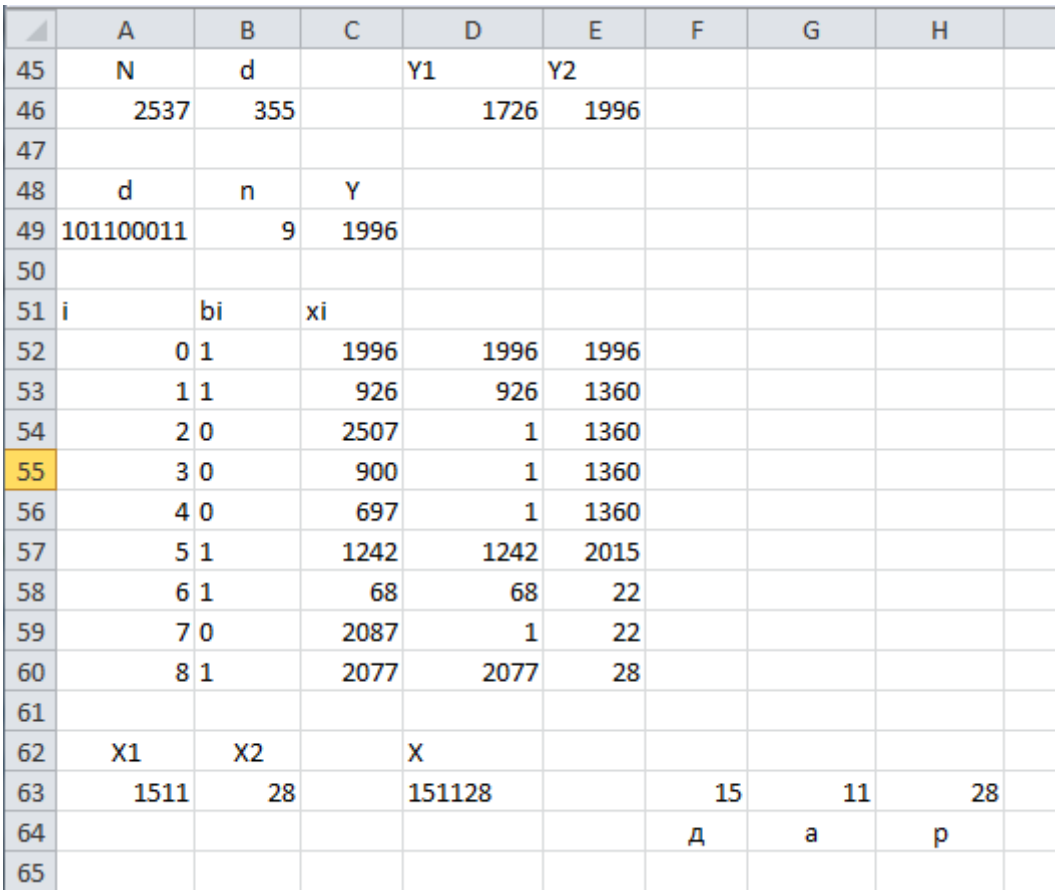
- Значение *d*находится в столбце **C**в предпоследней строке, содержащей числовые значения, то есть в строке, предшествующей строке, начинающейся с 0. Строка с результатом должна начинаться с 1.

Для рассматриваемого примера значение личного ключа *d* содержится в ячейке **C6**, *d*=355.

ЗАМЕЧАНИЕ: Если полученное значение *d* – отрицательное, следует взять его по модулю φ(*N*). Для этого можно использовать функцию **ОСТАТ()** или просто сложить *d* со значением φ(*N*).

12. Занести значения *N*, *d* и частей Y_1, Y_2криптограммы на лист MSExcel.
13. Вычислить значения X_1, X_2, используя формулу $X=Y^d \bmod N$, вычисления производятся с помощью быстрого алгоритма возведения в степень по модулю(аналогично пункту3 задания *A*).

Для рассматриваемого примераполучили X_1 = 1511, X_2 = 28 (рис.67).



	A	B	C	D	E	F	G	H
45	N	d		Y1	Y2			
46	2537	355		1726	1996			
47								
48	d	n	Y					
49	101100011	9	1996					
50								
51	i	bi	xi					
52	0	1	1996	1996	1996			
53	1	1	926	926	1360			
54	2	0	2507	1	1360			
55	3	0	900	1	1360			
56	4	0	697	1	1360			
57	5	1	1242	1242	2015			
58	6	1	68	68	22			
59	7	0	2087	1	22			
60	8	1	2077	2077	28			
61								
62	X1	X2		X				
63	1511	28		151128		15	11	28
64						д	а	р
65								

Рис. 67. Пример расшифрованияRSA

14. Преобразовать полученные значения в текстовое сообщение:

- Сформировать общую числовую последовательность X объединением расшифрованных частей X_1 и X_2: X=151128.
- Разбить последовательность Xна двузначные числа: 15, 11, 27.
- Используя таблицу 30, найти символы, соответствующие полученным числовым кодам.

В рассматриваемом примере зашифрованное сообщение содержит текст «дар».

15. Показать результаты выполнения практической работы преподавателю.

Практическая работа №10. Атака на алгоритмRSA методом Ферма

Безопасность RSAи описание метода криптоанализа

Безопасность алгоритма RSA основана на трудоемкости разложения на множители (факторизации) больших чисел. К началу 2010 года с помощью *метода решета числового поля* удалось факторизовать 768-битное число.Следовательно, выбираемое $N=p\cdot q$ должно быть больше. В настоящее время рекомендованы к использованию ключи RSA (N) порядка 2048 и 3072 бита. Кроме разрядности p и q, к ним предъявляются следующие дополнительные требования:

- пара простых чисел p и q для каждого абонента должна быть своей, то есть все модули N_A, N_B, N_C, … должны быть различны. В противном случае один абонент сможет читать сообщения, предназначенные для другого (поскольку сможет вычислить чужой личный ключ, зная разложение числа Nна множители pи qи значение $\varphi(N)$). Кроме того, в случае пересылки пользователям с одинаковыми модулями одного и того же сообщения,противник сможет прочитать это сообщение с помощью атаки на алгоритм RSA*методом бесключевого чтения*.
- числа p и qне должны содержаться в списках известных больших простых чисел;
- значения p и q не должны быть близкими, так как иначе можно воспользоваться для факторизации N*методом Ферма*.

При известных p и q можно оценить стойкость выбранных параметров к атаке методом Ферма. Определить количество попыток k, необходимых для факторизации N, можно по формуле:

$$k = \sqrt{p*q + \left(\frac{p-q}{2}\right)^2} - \left[\sqrt{p*q}\right],$$

где где $[x]$ – операция округления x до ближайшего целого числа;

- числа p–1, p+1, q–1, q+1 не должны разлагаться в произведение маленьких простых множителей, должны содержать в качестве сомножителя хотя бы одно большое простое число.

В 1978 г. один из авторов RSA Рональд Райвест сформулировал наиболее сильные требования. Числа

$p_1 = \frac{p-1}{2}$, $p_2 = \frac{p+1}{2}$, $q_1 = \frac{q-1}{2}$, $q_2 = \frac{q+1}{2}$ должны быть простыми, причем числа p_1-1 и q_1-1 не должны разлагаться в произведение маленьких простых.

Кроме того, нежелателен выбор малых значений экспонент e и d (хотя это и позволяет ускорить выполнение шифрования или расшифрования соответственно). Так, при значении $d<N^{0,292}$существует эффективный способ его вычисления (атака Винера).

Если же малым является параметр e, то достаточно большое число открытых сообщений, удовлетворяющих неравенству $X < \sqrt[e]{Y}$, будут зашифровываться простымвозведением в степень $Y = X^e<N$ и поэтому их можно будет найти простым извлечением корня степени eиз криптограммы Y.

Таким образом, безопасность RSA во многом зависитотвыбора параметров криптосистемы.

Метод Ферма – метод криптоанализа алгоритма RSA, применимый в случае, если параметрыp и qоказались достаточно близкими друг к другу.

Рассмотрим пример. Пусть N=23360947609, два его простых делителя близки к друг другу. Определим p и qметодом Ферма.

Пусть $p>q$, тогда имеем $N = \left(\frac{p+q}{2}\right)^2 + \left(\frac{p-q}{2}\right)^2$. Обозначим: $t = \frac{p+q}{2}$, $s = \frac{p-q}{2}$. Так как s мало, то t – целое число, лишь немного большее $\sqrt{N}$, причем $t^2 - N$ является полным квадратом (то есть $v = \sqrt{t^2 - N}$ – целое число).

Для нахождения значения tсначала следует вычислить $\sqrt{N}$, затем следует проверять подряд целые числа $t > \sqrt{N}$.

В примере $\sqrt{N}$ ≈152842,9.

Рассмотрим t_1=152843, $v_1^2=t_1^2-N$=35040, v_1≈187,2 – не является целым.

На следующем шаге рассмотрим $t_2=t_1+1$=152844, $v_2^2=t_2^2-N$=340727, v_2≈583,7 – не является целым.

На третьем шаге: $t_3=t_2+1=t_1+2=152845$, $v_3^2=t_3^2-N=646416$, $v_3=804$ –целое.

Нашли $v=v_3$. Тогда$p=t+v$, $q=t-v$.

Получили: $p=152845+804=153649$, $q=152845-804=152041$. Знание p и q позволяет найти секретный ключ алгоритма RSA.

Описание инструментального средства BCalc

Программа «BCalc» предназначена для работы с целыми числами большой размерности и включает в себя возможность выполнения базовых и некоторых специальных операций над целыми числами. Специальные операции:

- преобразование числа в символьные данные и обратно;
- возведение в степень по модулю;
- вычисление обратных значений по модулю;
- нахождение целых корней любых натуральных степеней;
- нахождение подходящих дробей для цепной дроби.

Описание интерфейса программы

В окне программы находятся следующие элементы интерфейса:

- поля ввода, помеченные латинскими буквами A, B, C, D;
- верхняя группа кнопок с обозначением выполняемых действий на них;
- нижняя группа кнопок, предназначенных для очистки полей и таблицы;
- таблица для хранения промежуточных результатов.

Поля ввода A, B, C хранят входные данные для вызываемых функций программы. Результаты работы этих функций помещаются в поле D. При нахождении подходящей дроби результат помещается в поле C и первую строку таблицы.

Для любого поля таблицы можно вызвать контекстное меню указателеммыши, нажав ее правую кнопку, в котором содержатся следующие пункты:

- «To [поле ввода]» – копирует значение ячейки таблицы в соответствующее поле ввода;
- «From [поле ввода]» – копирует значение соответствующего поля вводав выбранную ячейку таблицы.

Кнопки «ClearD», «ClearA, B, C», «Cleargrid» очищают соответственнополе D, поля A, B, C – таблицу.

Кнопка «Increasenumberofrows» увеличивает количество строк в таблицена пять.

Кнопка «D → A» копирует значение, находящееся в данный момент в поле D, в поле A. Кнопка «D → table» копирует значение поля D в первую сверху пустую ячейку второй колонки таблицы.

Остальные кнопки запускают математические функции, описанные ниже.Математические функции программы:

«D = A+B» – значения A и B складываются, результат помещаетсяв поле D.

«D = A*B» – значения A и B перемножаются, результат помещаетсяв поле D.

«D = A div B» – в D помещается результат целочисленного деления A на B.

«D = A mod B» – в D помещается остаток от целочисленного деленияA на B.

«D = A^B mod C» – в D помещается результат возведения A в степень B помодулю C. Экспонента может быть отрицательным числом. Если поле C = 0, товозведение в степень будет происходить по правилам обычной, а не модульной арифметики. В таком случае не стоит задавать в качестве экспоненты большие числа, таккак вычисления могут занять слишком много времени. Невозможно также вычислять обратные значения, если в качестве модуля задан ноль.

«D = A^(1/B)» – в поле D помещается корень B степени от A. Если в результате извлечения корня получилось нецелое число, то в D помещается ближайшее бóльшее целое число, а в первой строке таблицы появится надпись«[error]».

«A*D – B*C = N», где A – числитель дроби; B – знаменатель подходящей дроби δn порядка. В поле C будет помещен числитель, а в D – знаменательподходящей дроби δn-1 порядка. В первую строку таблицы будет помещено значение выражения A*D – B*C. Если после начала вычисления дроби поля C и Dравны нулю, то это значит, что числа A и B не взаимно просты.

«D = text(A)» – число A интерпретируется как строка из символов в ANSI-кодировке. Строка помещается в поле D.

«D = number(A)» – строка A, состоящая из символов, интерпретируется какчисло и помещается в поле D.

В программе используется модернизированный модуль «BigNumv2.0»(JesR. Klinke).

Задание. Даны значения модуля шифрования *N*, открытого ключа *e*и шифртекста *Y*. Известно, что *Y* получен шифрованием на открытом ключе (*N*, *e*) по алгоритму RSA.Используя разложение модуля на простые числа методом Ферма,определить секретный ключ алгоритма RSAи дешифровать *Y*.

Указания к выполнению практической работы

Для выполнения практической работы рекомендуется использовать программу *BCalc.exe*.Варианты заданий приведены в Приложении 4.

Технология выполнения задания

1. Изучить теоретическое описаниеметода Ферма.
2. Выбрать из Приложения 4 значения *N*, *e* и *Y*в соответствии с номером варианта. Выполнить криптоанализ по аналогии с рассмотренным далее примером.

Пример. *N*=65815671868057, *e*=7423489, *Y*=64938654445479. Дешифровать*Y*.

3. Запуститьпрограмму*BCalc.exe*, очиститьполяитаблицукнопками «ClearD», «ClearA, B, C», «Cleargrid».
4. Вычислить *n*=[$\sqrt{N}$] (операция [*x*] – округление*x* до ближайшего целого числа):

- Поместить в поле Азначение *N* (A←*N*), B←2, нажать кнопку«D=A^(1/B)». В поле Dбудет занесено число 8112686, а в заголовке таблицы отобразится сообщение «error». Это означает, что *N*не является квадратом целого числа.
- Нажать кнопку «D→table», вычислено значение [$\sqrt{N}$] будет занесено в первую строку таблицы. Добавить подпись: *n*.

5. Вычислить $t_1=n+1$. Нажать кнопку «D→A», B←1, нажать «A+B», получено значение 8112687, занести его в таблицу: «D→table», подписать: $t1$.
6. Проверить $v_1 = \sqrt{t_1^2 - N}$ – целое число:

- Вычислитьt_1^2. Нажать кнопку «D→A», значение t_1будет занесено в поле A (A←8112687), B←2, C←0,нажать кнопку«D=A^BmodC».Поскольку C=0, возведение в квадрат будет производится по правилам обычной, а не модулярной арифметики. В поле Dбудет занесено значение t_1^2=65815690359969. Занести в таблицу и подписать значение t_1^2.
- Вычислить $v_1^2=t_1^2-N$. Нажать кнопку «D→A», значение t_1^2будет занесено в поле A (A←65815690359969), B← -N(B← -65815671868057), нажать кнопку«D=A+B».Получили v_1^2=18491912.Занести в таблицу и подписать значение v_1^2.
- Вычислить $v_1 = \left[\sqrt{v_1^2}\right]$. Нажать кнопку «D→A», значение v_1^2будет занесено в поле A (A←18491912), B←2, нажать кнопку «D=A^(1/B)». В поле Dбудет занесено число 4301, а в заголовке таблицы отобразится сообщение «error». Это означает, что v_1^2не является квадратом целого числа.
- Занести в таблицу и подписать значение v_1.

7. Вычислить следующее число $t_2=t_1+1=n+2$ и выполнить для него пункт 5. Продолжить вычисление чисел t_iи их проверку (выполнять пункт 5) до тех пор, пока не будет получено v_i^2– квадрат целого числа. Для рассматриваемого примера получили:

- t_2=8112688, t_2^2=65815706585344, v_2^2=34717287, v_2=5893, «error»;
- t_3=8112689, t_3^2=65815722810721, v_3^2=50942664, v_3=7138, «error»;
- t_4=8112690, t_4^2=65815739036100, v_4^2=67168043, v_4=8196, «error»;
- t_5=8112691, t_5^2=65815755261481, v_5^2=83393424, v_5=9132, заголовоктаблицы пуст, что свидетельствует об успехе факторизации, v_5^2 – квадрат целого числа.

Получили: $t=t_5$=8112691, $v=v_5$=9132.

8. Вычислить $p=t+v$. В таблице щелкнуть правой кнопкой мыши на значении t_5 и выбрать команду **То А**, значение t_5будет занесено в поле А (А←8112691), аналогично В←v_5 (В←9132), нажать кнопку «D=A+B». P=8121823. Занести в таблицу и подписать значение p.
9. Вычислить $q=t-v$. В поле Вдобавить знак «-» перед значением (В← -9132), нажать кнопку «D=A+B». Q=8103559. Занести в таблицу и подписать значение q.
10. Вычислить $\varphi(N)=(p-1)\cdot(q-1)$. А←$p$–1 (А←8121822), В←$q$–1 (В←8103558), «D=A*B». $\varphi(N)$=65815655642676. Занести в таблицу и подписать значение $\varphi(N)$.
11. Вычислить$d=e^{-1}\bmod\varphi(N)$. А←e (А←7423489), В← -1, С←$\varphi(N)$ (С←65815655642676), нажатькнопку«D=A^B mod C». d=12490789985101. Занести в таблицу и подписать значениеd.
12. Произвести расшифрование значения Y: $X=Y^d \bmod N$:

- А←Y (А←64938654445479), В←d (В←12490789985101), С←N (С←65815671868057), нажатькнопку «D=A^B mod C».X=3553673249. Занести в таблицу и подписать значениеX.
- Перевести Xв текстовый вид: нажать кнопку «D→A» (А←X), нажать кнопку «D=text(A)». Получен ответ: исходный текст «УРА!».

  Результат расшифрования – **УРА!**

  Полученный открытый текст должен быть осмысленным, это является проверкой правильности дешифрования.

Практическая работа № 11. Атака на алгоритмRSA методом повторного шифрования

Описание метода криптоанализа

Пусть имеется открытый ключ (N, e) и зашифрованное им сообщение Y.

Построим последовательность: $Y_1=Y$, $Y_i=Y_{i-1}^e \bmod N$, $i>1$. $Y_m = Y^{e^m} \bmod N$, а так как НОД(e,φ(N))=1, то существует такое натуральное число m, что $e^m \equiv 1 \pmod{\varphi(N)}$.

Тогда $Y^{e^m-1} \equiv 1 \pmod N$, отсюда следует, что $Y^{e^m} \equiv Y \pmod N$, а поскольку $Y=X^e \bmod N$, то $Y^{e^m}=Y_{m-1}$ – решение сравнения $Y \equiv X^e \pmod N$.

Пример. Пусть имеется открытый ключ N=84517, e=397 и зашифрованное им сообщение Y=8646. Необходимо найти исходный текст X. Возведем Y в степень e и получим Y_2=37043. Будем повторять операцию до тех пор, пока не получим $Y_n=Y$. Y_{n-1} – искомое сообщение:

Y_3 = 5569, Y_4 = 61833, Y_5 = 83891, Y_6 = 16137, Y_7 = 8646 = Y.

Y_6 является решением сравнения $Y=X^e \bmod N$, а, следовательно, искомым сообщением X.

Анализ метода повторного шифрования хорошо показывает необходимость соблюдения требований на выбор p и q для обеспечения стойкости. В рассматриваемом примере d = 82225. Неудачный выбор параметров криптосистемы привел к тому, что атака методом повторного шифрования дала результат почти сразу, тогда как нахождение d потребовало бы на порядок больших вычислений.

Описание инструментального средства PS

Программа PS предназначена для нахождения порядка чисел в конечномполе $Z_{\varphi(N)}$ и дешифрации сообщений методом повторного шифрования.

Нахождение порядка чисел:

Для нахождения порядка числа методом повторного шифрования следует указатьв поле редактирования N значение модуля, в поле e – экспоненты, а в поле Y –произвольное число, меньшее чем модуль. При нажатии кнопки **Запуск повторного шифрования** программа начнет возводить число Y в степень e (т. е. вычислять$Y_i = (Y_{i-1})^e$ до тех пор, пока Y_i не будет равен Y.

Значение $Y_{i-1}=\sqrt[e]{Y}$, а число шагов повторного шифрования является порядком числа e в конечном поле $Z_{\varphi(N)}$.При завершении работы алгоритма в поле i будет записано количество шагов повторного шифрования, а в поле X – значение Y_{i-1}.

Во время работы программы кнопка **Pause** приостанавливает работу алгоритма. Для продолжения работысследует нажать кнопку **Pause** еще раз. Флаг *Showresults* указывает, будут лиотображаться результаты промежуточных вычислений. Его отключение увеличивает скорость работы приблизительно на 20 %.

Дешифрации сообщений методом повторного шифрования:

Для дешифрации сообщения необходимо указать в поле редактирования Nзначение модуля, в поле e – экспоненты, в поле *i* – порядок экспоненты, а в область редактирования *C* поместить блоки зашифрованного текста (разделитель –символ конца строки). При нажатии кнопки **Дешифрация** начнется процессвычисления исходного сообщения. Результат будет помещен в область редактирования *M*.

Задание. Даны значения модуля шифрования *N*, открытого ключа *e* и шифртекста *Y*. Известно, что *Y* получен шифрованием на открытом ключе (*N*, *e*) по алгоритму RSA. Используя метод повторного шифрования, расшифровать *Y*.

Указания к выполнению практической работы

Для выполнения практической работы рекомендуется использовать программу *PS.exe*.Варианты заданий приведены в Приложении 5.

Технология выполнения задания

1. Изучить теоретическое описаниеметода повторного шифрования.
2. Выбрать из Приложения 5 значения *N*, *e* и *Y*в соответствии с номером варианта. Выполнить криптоанализ по аналогии с рассмотренным примером.

Пример. *N*=453819149023, *e*=1011817, *Y*=442511634532. Расшифровать *Y*.

3. Запустить программу*PS.exe*, ввести значение модуля в поле *N*, значение экспоненты – в поле *e*, в поле *Y* занести произвольное число, большее 1 и меньшее*N*, например, 2.
4. Определить порядок экспоненты. Установить флажок *ShowResult*. Нажать кнопку **Запуск повторного шифрования** и дож-

даться, пока не будет получены значения в полях *X* и *i*. Значение в поле *i* – порядок *e* в конечном поле $Z_{\varphi(N)}$. Получили *i*=435.

5. Дешифровать криптограмму *Y*. Для этого поместить значение *Y* в область редактирования поля *C*. Также должны быть заполнены поля *N*, *e* и *i*. Затем нажать кнопку **Дешифрация** и дождаться появления исходного текста в области редактирования *M*.

   Будет получен ответ: открытый текст –«null».

Открытый текст должен быть осмысленным, что является проверкой правильности дешифрования.

ЗАМЕЧАНИЕ: Если шифртекст состоит из блоков, расшифрование может производиться как для каждого из блоков по отдельности (выполняется быстрее), так и для нескольких блоков сразу. В последнем случае каждый из блоков зашифрованного текста *Y* должен быть помещен на новую строку поля *C*.

Практическая работа №12. Атака на алгоритм RSA методом бесключевого чтения

Описание метода криптоанализа

Метод бесключевого чтения применим, когда пользователи используют один и тот же модуль *N*.

Пусть два пользователя выбрали одинаковый модуль *N* и разные экспоненты e_1 и e_2. Если им будет послано некое циркулярное сообщение *X*, то криптоаналитик может получить в свое распоряжение два шифрованных текста: $Y_1=X^{e1} \bmod N$, $Y_2=X^{e2} \bmod N$.

В этом случае, используя расширенный алгоритм Евклида, криптоаналитик может получить *r* и *s* такие, что $r \cdot e_1+s \cdot e_2=1$. Зная *r* и *s* можно получить исходное сообщение: $Y_1^{\,r} \cdot Y_2^{\,s}=X^{re1+se2}=X^1=X$.

Пример. Пусть два пользователя применяют общий модуль *N*=137759, но разные взаимно простые экспоненты e_1=191 и e_2=233. Пусть также они получили шифровки Y_1=60197 и Y_2=63656, которые содержат одно и то же сообщение. Так как e_1 и e_2 – взаимно просты, всегда найдутся такие *r* и *s*, что $r \cdot e_1+s \cdot e_2=1$.

Найдем r и s с помощью расширенного алгоритма Евклида ($U \leftarrow \{\max(e_1,e_2),1,0\}$, $V \leftarrow \{\min(e_1,e_2),0,1\}$, $k=u_1 \text{div} v_1$, $T=\{u_1 \text{mod} v_1$, $u_2 - k \cdot v_2$, $u_3 - k \cdot v_3\}$). Вычисления продолжаются, пока t_1 не станет равным 0.

Поскольку в рассматриваемом примере$e_2 > e_1$,расширенный алгоритм Евклида примет вид, представленный на рис. 68.

аг	1	2	3	4	5	6	7	рез-т	строки			k
	U								233	1	0	
	V	U							191	0	1	
1	T	V	U						42	1	-1	1
2		T	V	U					23	-4	5	4
3			T	V	U				19	5	-6	1
4				T	V	U			4	-9	11	1
5					T	V	U		3	41	-50	4
6						T	V	U	1	-50	61	1
7							T	V	0	191	-233	3

Рис. 68. Пример нахождения значений r и s с помощью расширенного алгоритма Евклида

Итак, с помощью расширенного алгоритма Евклида найдено: $r=61$, $s=-50$, проведем проверку: $61 \cdot 191 - 50 \cdot 233 = 11651 - 11650 = 1$.

Тогда искомое сообщениеX:

$X = Y_1^r \cdot Y_2^s = (60197^{61} \cdot 63656^{-50}) \text{mod} 137759 = 1234$.

Задание. Даны значения модуля шифрования N, экспоненты двух пользователейe_1 и e_2, а также криптограммыY_1 и Y_2,направленные этим пользователям и содержащие одно и то же сообщение. Известно, что шифртексты полученыс помощью алгоритма RSA.Используя метод бесключевого чтения,получить исходное сообщениеX.

Указания к выполнению практической работы

Для выполнения практической работы рекомендуется использовать программу *BCalc.exe*.Варианты заданий приведены в Приложении 6.

Технология выполнения задания

1. Изучить теоретическое описаниеметода бесключевого чтения.
2. Выбрать из Приложения 6 значения N, e и Yв соответствии с номером варианта. Выполнить криптоанализ по аналогии с рассмотренным далее примером.

Пример. N=357114156277, e_1=1025537, e_2=722983, Y_1=68639736967, Y_2=204258645263. Получить исходное сообщение.

3. Запустить программу*BCalc.exe*, очистить поля и таблицу кнопками «Clear D», «Clear A, B, C», «Cleargrid».
4. С помощью расширенного алгоритма Евклида найти значения rиs, удовлетворяющие уравнению$e_1 \cdot r - e_2 \cdot s = \pm 1$:

- В поле Апоместить значение e_1(A←1025537), в поле B – значение e_2 (B←722983), нажать кнопку «A*D-B*C=N», поле Dбудет содержать значение r (286243), а поле C – значение s (406030).
- Занести в таблицу и подписать значения r и s.

ЗАМЕЧАНИЕ: Если в результате вычислений r и sполучено значение -1 (будет выдано соответствующее сообщение в первой строке таблицы:AD-BC=-1), то есть$e_1 \cdot r - e_2 \cdot s$=-1, то в дальнейших вычисленияхизменить знак r и sна противоположный.

5. Произвести дешифрование:

- Возвести Y_1в степень rпо модулю N:A←Y_1 (A←68639736967), B←r (B←286243), C←N (357114156277), нажать «D=A^BmodC». Получили $Y_1^r \bmod N$=189703239311. Занести в таблицу и подписать данный результат.
- Аналогично предыдущему пункту возвести Y_2 в степень -sпо модулю N. Получили $Y_2^{-s} \bmod N$=104340380259. Занести в таблицу и подписать данный результат.
- Перемножить полученные значения $Y_1^r \bmod N$ и $Y_2^{-s} \bmod N$ по модулю N:A←$Y_1^r \bmod N$ (A←189703239311), B←$Y_2^{-s} \bmod N$ (B←104340380259), нажать «D=A*B». Нажать «D→A», занести C←N (C←357114156277), нажать «D=AmodC». В поле

Dполучено значение X=1381187873. Занести в таблицу и подписать полученный результат.

- Перевести X в текстовый вид:нажать «D→A», нажать «D=text(A)». Получен ответ: «RSA!».

  Результат расшифровки «RSA!».

Открытый текст должен быть осмысленным, что является проверкой правильности дешифрования.

Практическая работа №13. Атака на алгоритмRSA на основе Китайской теоремы об остатках

Описание метода криптоанализа

Метод криптоанализа на основе Китайской теоремы об остатках применим в случае, когда пользователи используют для шифрования одну и ту же экспонентуe.

Системы шифрования с открытыми ключами работают сравнительно медленно. Для повышения скорости шифрования RSA на практике могут использовать малые значения экспоненты зашифрования.

Если выбрать число e небольшим или таким, чтобы в его двоичной записи было мало единиц, то процедуру шифрования можно значительно ускорить.

Например, выбрав e=3 (при этом e – взаимно простое с (p-1)·(q-1), то естьни p-1, ни q-1 не должны делиться на 3), можно реализовать шифрование с помощью одного возведения в квадрат по модулю N и одного перемножения. Выбрав в качестве значения eчисло 65 537, двоичная запись которого 10000000000000001 содержит только две единицы, можно реализовать шифрование с помощью 16 возведений в квадрат по модулю N и одного перемножения (поскольку 65 537=2^{16}+1).

Если экспонента e выбирается случайно, то реализация шифрования по алгоритму RSA потребует s возведений в квадрат по модулю N и в среднем s/2 умножений по тому же модулю, где s – длина двоичной записи числа N.

Однако выбор малых значений экспоненты e может привести к негативным последствиям. Например, у нескольких коррес-

пондентов могут оказаться одинаковые экспоненты e. В этом случаеприменима атака на RSAна основе Китайской теоремы об остатках.

Пусть, например, три корреспондента имеют попарно взаимно простые модули N_1, N_2, N_3 и общую экспоненту e=3. Если им посланоодно и то же сообщение X, то криптоаналитик может получить в свое распоряжение три шифрованных текста Y_1, Y_2, Y_3,$Y_i=X^3 \bmod N_i$, i=1,2,3. Далее он может найти решение системы сравнений, лежащее в интервале от 0 до $N_1 \cdot N_2 \cdot N_3$: $0<Y< N_1 \cdot N_2 \cdot N_3$:

$$\begin{cases} Y \equiv Y_1 \bmod N_1 \\ Y \equiv Y_2 \bmod N_2 \\ Y \equiv Y_3 \bmod N_3 \end{cases}$$

СогласноКитайской теореме об остатках, такое решение Yединственно, а так как $X^3<N_1 \cdot N_2 \cdot N_3$, то $Y=X^3$. Значение X можно найти, вычислив кубический корень $X = \sqrt[3]{Y}$.

Китайская теорема об остатках. Пусть m_1, m_2, ..., m_r – попарно взаимно простые, и числа a_1, a_2, ..., a_r – произвольные целые. Тогда существует целое число x_0: $0 \le x_0 < m_1 \cdot m_2 \cdot ... \cdot m_r$ и $x_0 \equiv a_1 (\bmod m_1)$, $x_0 \equiv a_2 (\bmod m_2)$, …, $x_0 \equiv a_r (\bmod m_r)$.

Приэтом $x_0 = \sum_{i=1}^{r} a_r \cdot M_i \cdot N_i (\bmod m_1 \cdot m_2 \cdot ... \cdot m_r)$,

где$M_i=m_1 \cdot \ldots \cdot m_{i-1} \cdot m_{i+1} \cdot \ldots m_r$и$N_i = M_i^{-1} \bmod m_i$.

Для реализации атаки на алгоритм RSAс помощью китайской теоремы об остатках необходимо, чтобы один и тот же открытыйX текст был послан eабонентам с разными (взаимно простыми) значениями N_i и одинаковым e(шифртекстыY_i, содержащие X, будут различны).

Пример. Пусть три пользователя имеют разные модули N_1=26549, N_2=45901, N_3=25351, но используют одинаковую экспоненту e=3. Всем пользователям было послано одинаковое сообщение X, причем пользователи получили криптограммыY_1=5366, Y_2=814, Y_3=4454. Требуется определить X.

Найдем $M_0=N_1 \cdot N_2 \cdot N_3$= 30893378827799. Далее находим:

$m_1 = N_2 \cdot N_3$ = 1163636251

$m_2 = N_1 \cdot N_3$ = 673043699

$m_3 = N_1 \cdot N_2 = 1218625649$

$n_1 = m_1^{-1} \bmod N_1 = 13533$
$n_2 = m_2^{-1} \bmod N_2 = 27930$
$n_3 = m_3^{-1} \bmod N_3 = 22354$

Тогда$S = Y_1 \cdot n_1 \cdot m_1 + Y_2 \cdot n_2 \cdot m_2 + Y_3 \cdot n_3 \cdot m_3 = 845010280387455 78 + 153016619576389 80 + 121332116653000684 = =221134806649385242$

$S \bmod M_0 = 221134806649385242 \bmod 30893378827799 = =1000000000$

$X = (S \bmod M_0)^{1/3} = 1000$ – получили исходное сообщение, отправленное пользователям.

Задание. Даны значенияэкспоненты e=3,модулей шифрования трех пользователей N_1, N_2, N_3, а также направленные этим пользователям шифртекстыY_1,Y_2и Y_3, содержащие одно и то же сообщениеX. Известно, что шифртексты получены с помощью алгоритма RSA. Используя метод криптоанализа, основанный на китайской теореме об остатках, получить исходное сообщениеX.

Указания к выполнению практической работы

Для выполнения практической работы рекомендуется использовать программу *BCalc.exe*. Варианты заданий приведены в Приложении 7.

Технология выполнения задания

1. Изучить теоретическое описаниеметода криптоанализа алгоритма RSAна основе китайской теоремы об остатках.
2. Выбрать из Приложения 7 значения модулей N и шифртекстовYв соответствии с номером варианта;значение e= 3. Выполнить криптоанализ на основе Китайской теоремы об остатках по аналогии с рассмотренным далее примером.

Пример. e=3, N_1=363542076673, N_2=728740902979, N_3=522993716719, Y_1=246562834516, Y_2=291375746601, Y_3=222724269731. Получить исходное сообщение.

3. Запустить программу*BCalc.exe*, очистить поля и таблицу кнопками «Clear D», «Clear A, B, C», «Cleargrid».

4. Вычислить значения $M_0=N_1\cdot N_2\cdot N_3$, $m_1=N_2\cdot N_3$, $m_2=N_1\cdot N_3$, $m_3=N_1\cdot N_2$:

- Вычислить m_1: A←N_2(A←728740902979), B←N_3 (B←522993716719), нажать «D=A*B», получен результат m_1=381126913374147389205901. Занести в таблицу и подписать значение m_1 (кнопка «D→table»).
- Вычислить M_0: нажать «D→A», B←N_1 (B←363542076673), нажать «D=A*B», получен результат:M_0=13855566956400811930269443392604737 3. Занести в таблицу и подписать значение M_0.
- Вычислить m_2: A←N_3 (A←522993716719), в ячейке B уже находится значение N_1, нажать «D=A*B», получен результат:m_2=190130221862955939995887. Занести в таблицу и подписать значение m_2.
- Вычислить m_3: A←N_2 (A←728740902979), в ячейке B уже находится значение N_1, нажать «D=A*B», получен результат:m_3=264927981225542872108867. Занести в таблицу и подписать значение m_3.

5. Вычислить значения n_1, n_2, n_3;$n_i=m_i^{-1}\text{mod}N_i$:

- A←m_1 (A←381126913374147389205901), B← -1, C←N_1 (C←363542076673), нажать«D=A^B mod C». Полученрезультат: n_1=287993142707.Занести в таблицу и подписать значение n_1.
- Аналогичным образом вычислить n_2=106614970676, n_3=32171022265.Занести в таблицу и подписать значения n_2 и n_3.

6. Вычислить$S=Y_1\cdot m_1\cdot n_1+Y_2\cdot m_2\cdot n_2+Y_3\cdot m_3\cdot n_3$:

- Вычислить $s_1=\boldsymbol{Y}_1\cdot m_1\cdot n_1$: A←$\boldsymbol{Y}_1$ (A←246562834516), B←m_1 (B←381126913374147389205901), нажать «D=A*B», поле D содержит значение 939717320718637699173680129136789 16ю Нажать «D→A», B←n_1 (B←287993142707), нажать«D=A*B». s_1=27063214444996231469275579740886150927965065612. Занести в таблицу и подписать значение s_1.
- Аналогичным образом вычислить значения s_2=59063985134617821897222137870202639887019288 12,

s_3=189827983794532429318381385616127417034535990 5. Занести в таблицу и подписать значения s_2 и s_3.

- Вычислить значение $S=s_1+s_2+s_3$= 348678927964033379521816073840676890870123543 29.Занести в таблицу и подписать значение S.

7. Вычислить$S\text{mod}M_0$: A←S, C←M_0, нажать «D=AmodC», результат: $S\text{mod}M_0$=67675640795094503562173784000.Занести в таблицу и подписать полученное значение.
8. Вычислить корень степени e из значения $S\text{mod}M_0$: $(S\text{mod}M_0)^{1/e}$: нажать «D→A», значение$S\text{mod}M_0$ будет занесено в поле A; B←e (B←3), нажать «D=A^(1/B)». Получено значение X=4075154940.Занести в таблицу и подписать числовое значениеX.
9. Перевести значение X в текстовый вид: нажать «D→A» (A←X), нажать «D=text(A)». Получен ответ: «тень»
   Результат дешифрования: «тень».
   Открытый текст должен быть осмысленным, что является проверкой правильности дешифрования.

ТЕМА 5. КРИПТОГРАФИЧЕСКИЕ ХЭШ-ФУНКЦИИ

Хэш-функцией называется любая односторонняя функция $y = h(x_1x_2\ldots x_n)$, которая строке символов (сообщению) $x = x_1x_2\ldots x_n$ произвольной длины n ставит в соответствие целое число фиксированной длины (хэш-код).

Хэш-код выполняет ту же функцию, что и контрольная сумма, то есть служит для проверки и подтверждения целостности передаваемого сообщения. Бесключевые хэш-функции обычно используются в технологии цифровой подписи.

В отличие от обычной контрольной суммы, криптографически сильная хэш-функция должна быть односторонней. То есть, для любого сообщения его хэш-код может быть легко вычислен, однако зная хэш-код, невозможно определить исходную строку (сообщение), для которой он был получен. Кроме того даже незначительное изменение исходного документа должно приводить к изменению хэша.

Основные требования, предъявляемые к криптографически сильным хэш-функциям (хэш-значение вычисляется для строки x):

- Для любого заданного x вычисление $h(x)$ выполняться относительно быстро;
- Для известного значения y практически невозможно найти x, такое, что $y= h(x)$;
- Для известного значения x практически невозможно найти другое сообщение x', $x' \neq x$, такое, что их значения хэш-функции совпадают $h(x') = h(x)$;
- Практически невозможно найти пару каких-либо различных сообщений x и x', $x' \neq x$, для которых значения хэш-функции совпадают$h(x') = h(x)$.

Существование сообщений с одинаковыми хэш-значениями называется *коллизией хэш-функции*. Возможность нахождения коллизий хэш-функции позволяет подделывать электронную подпись и влечет ненадежность системы аутентификации источников сообщений.

На сегодняшний день действующим российским стандартом являются две хэш-функции, описанные ГОСТ Р 34.11–2012 «Информационная технология. Криптографическая защита информации. Функция хэширования». Американские стандарты описывают два семейства хэш-функций: SHA-2 и SHA-3 (Keccak) с разными длинами хэш-кода. Хэш-функция SHA-1 не рекомендована к использованию, хотя еще достаточно распространена на практике. Для другой известной хэш-функции MD5 на сегодняшний день найдены коллизии и предложен осуществимый на практике алгоритм подделки подписей. Поэтому использовать хэш-функцию MD5 и предшествующие ей функции семейства MDне представляется разумным.

Практическая работа №14. Применение криптографических хэш-функций.

Задание. Исследовать использование алгоритмов хэш-функции в технологии ЭЦП.

Технология выполнения задания

1. Изучить теоретическое описание хэш-функций. Привести примеры криптографически сильных и слабых бесключевых хэш-функций. Какие бесключевые хэш-функции на сегодняшний день не рекомендованы к применению?
2. ВоспользовавшисьбраузеромMSInternetExplorer, просмотреть свойства доступных сертификатов промежуточных и доверенных удостоверяющих центров с помощью команды**Сервис/Свойства браузера/Содержание/Сертификаты**.Выбрав название сертификата на вкладке *Доверенные корневые центры сертификации* или *Промежуточные центры сертификации* посмотреть отображаемое в окне *назначение сертификата* и его свойства (**Просмотр/Состав/алгоритм хэширования подписи**).
3. Составить список используемых хэш-функций, обратив внимание на алгоритмы, используемые корневых сертификатов *Class 3 PublicPrimaryCertification*и *Copyright (c) 1997 MicrosoftCorp*.Отвечают ли указанные сертификаты современным требованиям безопасности и почему?
4. Посмотреть сертификаты web-серверов, обращение к которым идет по защищенному протоколу HTTPS,например,
    - https://мвд.рф/
    - https://www.nalog.ru/rn78/
    - https://www.gosuslugi.ru/

Для просмотра сертификата следует открыть сайт с помощью браузера InternetExplorer, а затем щелкнуть на значке замка в правой части адресной строки или выполнить команду **Вид/Отчет о безопасности**, в окне команды нажать **Просмотреть сертификат**, исследовать используемый алгоритм хэширования (вкладка *Состав*) и путь сертификации на одноименной вкладке.

5. Составить список бесключевых хэш-функций, используя стандарты ГОСТ Р 34.11–2012, ISO/IEC 10118 (части 1-4), FIPS PUB 180, FIPS PUB 202 и информационный поиск в сети Интернет, с указанием размера выхода (хэш-кода), особенностей алгоритма и рекомендаций к использованию.

Какие функции из списка встречались чаще всего при просмотре сертификатов?

6. Вычислить значения различных бесключевых хэш-функций, используя онлайн-калькуляторы, например,
    - *http://foxtools.ru/Hash*
    - *https://www.tools4noobs.com/online_tools/hash/*
    - *http://www.convertstring.com/ru/Hash*
    - *http://hash.online-convert.com/ru*
7. Исследовать изменение хэш-кода при незначительном изменении хэшируемого текста (изменение 1 символа).
8. Показать отчет с результатами выполнения практической работы преподавателю.

ТЕМА 6. ЦИФРОВЫЕ ПОДПИСИ

Появление криптографии с открытым ключом позволило решать задачи, которые ранее считались неразрешимыми. К таким задачам относится использование цифрового аналога собственноручной подписи абонента – *электронной цифровой подписи* (ЭЦП).

Электронная подпись обеспечивает те же свойства, что и собственноручная подпись автора сообщения, то есть гарантирует выполнение следующих свойств:

- Подлинность подписи можно проверить;
- Подпись нельзя подделать (данную подпись может поставить только ее обладатель и никто другой);
- Подпись является неотъемлемой частью документа и не может быть перенесена в другой документ.
- Подписанный документ не подлежит никаким изменениям.
- Автор подписи не может от нее отказаться.

Цифровая подпись для сообщения является числом, зависящим от самого сообщения и от секретного ключа, известного только подписывающему субъекту. При этом подпись должна легко проверяться без знания секретного ключа.

Наиболее распространена технология ЭЦП, основанная на совместном применении алгоритмов *хеширования* и *шифрования с открытым ключом* (RSA или Эль-Гамаля).

Для подтверждения авторства, шифрование проводится личным ключом абонента, расшифровку (и, таким образом, проверку подлинности автора) может произвести любой пользователь открытым ключом абонента.

Как правило, шифруется не само сообщение, а его «дайджест» – значение фиксированной длины, зависящее от подписываемого сообщения. Для формирования дайджеста используется бесключеваяхеш-функция, при этом именно она во многом определяетнадежность всей системы цифровой подписи.

Практическая работа №15. Изучение электронной цифровой подписи Эль-Гамаля

Рассмотрим алгоритм подписи Эль-Гамаля, который лежит в основе большинства стандартов ЭЦП.

Сначала выбираются параметры системы Эль-Гамаля, общие для всех абонентов группы: простое число p и число g, $1<g<p-1$.Для обеспечения стойкости криптосистемы числа p и gдолжны быть выбраны следующим образом: $p = 2q + 1$,q – большое простое число, p–простое, $g^q \bmod p \neq 1$.

Затем, каждый абонент группы выбирает свой личный ключ – случайное числоx, $1<x<p-1$, которое держится в секрете. Затем абонент вычисляет свой открытый ключ y по формуле: $y = g^x \bmod p$.Затем открытые ключи абонентов публикуются, чтобы обеспечить возможность проверки подписей.

Алгоритм формирования подписи выглядит следующим образом:

1. Пусть M – подписываемое сообщение. Отправитель вычисляет хэш-код подписываемого сообщения $h=h(M)$. Значение h должно удовлетворять неравенству $0<h<p$ (это достигается выбором соответствующей хэш-функции).
2. Далее отправитель выбирает случайное число k, $0<k<p-1$, взаимно простое с $p-1$: НОД(k,$p-1$)=1, и вычисляет числа:

   $r=g^k \bmod p$,

$u=(h-xr)\bmod(p-1)$,

$s=k^{-1}u\bmod(p-1)$,

k^{-1} – число, обратное k по модулю $p-1$; k^{-1} существует, так как k и $p-1$ – взаимно просты.

Для каждого подписываемого сообщения выбирается свое случайное число k.

3. Подпись (r, s) добавляется к сообщению, и тройка (M, r, s) передается получателю.

Проверка подписи осуществляется следующим образом:

4. Получатель заново вычисляет хэш-код $h(M)$ присланного сообщения M и проверяет подпись, используя равенство:

$$y^r r^s \equiv g^h (\bmod p).$$

Если это равенство выполняется, то подпись признается действительной. В противном случае (равенство не выполняется) подпись признается фальшивой, что может означать как подмену авторства, так и подмену самого сообщения.

Отметим, что число k выбирается заново для каждого нового подписания сообщения и должно держаться в секрете.

Используемые на практике алгоритмы хэширования достаточно сложны, поэтому будем использовать учебный алгоритм формирования хэш-значений $h(M)$. Будем считать, что сообщение M представлено в числовом виде, M_i, $i=1,\ldots,n$ – десятичные цифры, представляющие сообщение M.

Учебный алгоритм хеширования:

1. Выбирается число h_0 – вектор инициализации. Значение h_0 вычисляется как длина сообщения в символах.
2. Для каждого символа сообщения вычисляется значение $h_i=(M_i+ h_{i-1})^2 \bmod (p-1)$, $i=1,\ldots,n$.
3. Значение h_n, вычисленное для последнего символа, увеличивается на 1, что и является хэш-кодом сообщения: $h(M)=h_n+1$.

Следует отметить, что вычисленное по этому алгоритму значение хэша зависит от всех символов подписываемого сообщения M.

Задание

Выполнить вычисление и проверку подписи сообщения по алгоритму Эль-Гамаля.

Технология выполнения задания

ЗаданиеА.Известны значения общих параметров криптосистемы Эль-Гамаля: p=59, g=14, личный ключ абонента x и случайное число k, выбранное для формирования подписи сообщения. Для заданного в числовом представлении сообщения M сгенерировать цифровую электронную подпись по алгоритму Эль-Гамаля. Хэш-код сообщения вычисляется с помощью учебного алгоритма, начальное значение h_0 принимается равным числу десятичных разрядов в числовом представлении M.

Технология выполнения задания

1. Выбратьиз таблицы 34 значенийx и k и подписываемый текст Mв соответствии с номером варианта.

Сформировать цифровую подпись для сообщения M по аналогии с рассмотренным далее примером.

Пример. Общими параметрами системы цифровой подписи Эль-Гамаля являются значенияp=59, g=14. Абонент выбрал личный ключ x= 34. Он хочет передать сообщениеM= 1111, для которого выбрал случайное значениеk= 43.

Таблица 34

Варианты задания

Вариант	x	k	M
1	5	31	5211
2	12	47	3825
3	28	7	2412
4	7	21	1234
5	8	33	9461
6	17	11	7231
7	22	9	5184
8	10	15	4251
9	4	41	4629
10	19	35	3122

Вариант	x	k	M
11	33	39	6236
12	25	17	2971
13	55	19	3616
14	6	27	7222
15	21	5	3845
16	13	23	1197
17	11	55	4225
18	48	13	3163
19	37	25	2617
20	9	15	1831
21	15	7	2528
22	52	45	4911
23	24	3	5269
24	18	37	2120
25	44	51	1712

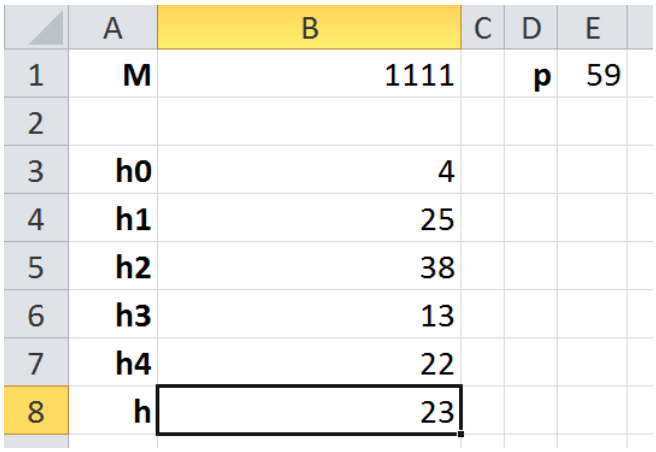
2. Вычислить хеш-значение h сообщения M по итерационной формуле:$h_i=(M_i+ h_{i-1})^2 \bmod (p-1)$, $i=1,\ldots,n$, $h(M)=h_n+1$, гдеn – число десятичных знаков в числовом представлении сообщения M, M_i – i-тый знак, $h_0=n$:

- Для рассматриваемого примера $h_0=4$, $p=59$, $M_i=1$, $i=1,\ldots,4$.
- Вычисления можно производить в табличном процессоре MSExcel. Получение h_0производится текстовой функцией **ДЛСТР()**,i-того символа сообщения M– текстовой функцией **ПСТР()**, вычисление h_i–функцией **ОСТАТ()** (рис. 69).

	A	B	C	D	E
1	**M**	1111		**p**	59
2					
3	**h0**	=ДЛСТР(B1)			
4	**h1**	=ОСТАТ((ПСТР($B$1;1;1)+B3)^2;$E$1-1)			
5	**h2**	=ОСТАТ((ПСТР($B$1;2;1)+B4)^2;$E$1-1)			
6	**h3**	=ОСТАТ((ПСТР($B$1;3;1)+B5)^2;$E$1-1)			
7	**h4**	=ОСТАТ((ПСТР($B$1;4;1)+B6)^2;$E$1-1)			
8	**h**	=B7+1			

Рис. 69. Пример расчета хэш-значения

В рассматриваемом примере получили $h(M)=23$ (рис.70).



	A	B	C	D	E
1	**M**	1111		**p**	59
2					
3	**h0**	4			
4	**h1**	25			
5	**h2**	38			
6	**h3**	13			
7	**h4**	22			
8	**h**	23			

Рис. 70. Результаты расчета хэш-значения

3. Вычислить число r по формуле $r=g^k \bmod p$. Для вычислений можно использовать табличный процессор MSExcel, реализовав в нем алгоритм быстрого возведения в степень по модулю (см. практическую работу №9. Изучение шифра RSA), либо использовать линейный относительно показателя степени итерационный алгоритм (так как значения kневелики):

- На новом листе в ячейку **A1** внести номер шага: 1, в ячейку **B1** – значение g(для рассматриваемого примера g = 14).
- В ячейку **A2** внести номер шага: 2, в ячейку **B2** – итерационную формулу для вычисления остатка от деления по модулю p, формула примет вид: **=ОСТАТ(**14*__B1__;59**)**.
- Выделить диапазон ячеек **A1:A2** и растянуть вниз, заполнив ячейки столбца **A** рядом данных до значения kвключительно (в примере k= 43).
- Выделить ячейку **B2** и растянуть вниз (скопировать ее) в диапазон ячеек столбца **B** строки с номером k включительно (в примере – до ячейки **B43**). Результат вычисления находится в последней заполненной ячейке столбца **B**.Подписать значение r.

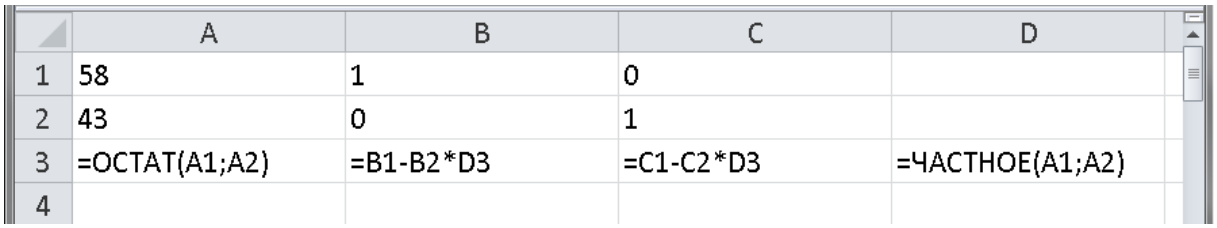
  Для рассматриваемого примера получили:
  $r=14^{43} \bmod 59=32$.

4. Вычислить число uпо формуле $u=(h-xr) \bmod (p-1)$, для вычислений в среде табличного процессора MSExcelиспользуется функция **ОСТАТ()**.

   В примере получили: u = (23-34·32) mod (59–1) = 37.

5. Рассчитать значение k^{-1} по модулю $p-1$ с помощью расширенного алгоритма Евклида (описание и пример реализации алгоритма приведены в практической работе №9. Изучение шифра RSA):

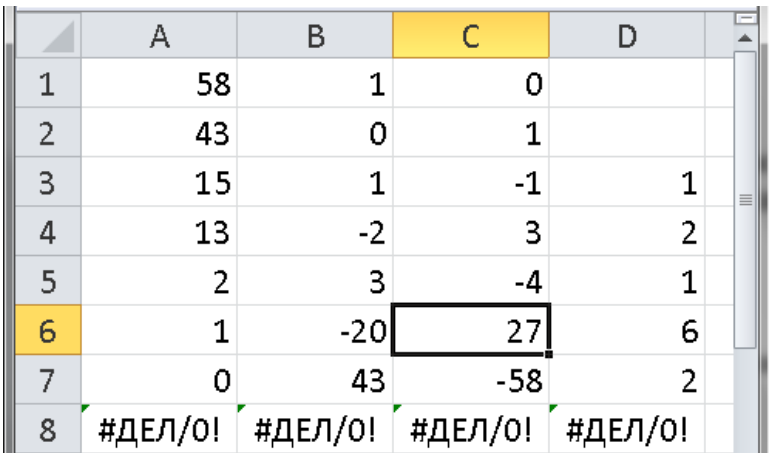
- Сформировать первую строку расширенного алгоритма Евклида: на новом листе в ячейку **A1** занести значение $p-1$ – 58, в ячейку **B1** – 1, в ячейку **C1** – 0.
- Сформировать вторую строку расширенного алгоритма Евклида: в ячейку **A2** занести значение k (в примере – 43), в ячейку **B2** – 0, **C2** – 1.
- Сформировать третью строку: в ячейку **D3** занести значение, вычисленное по формуле: =**ЧАСТНОЕ(A1,A2)**, в ячейку **A3** занести формулу: =**ОСТАТ(A1,A2)**, в ячейку **B3** – формулу =**B1-B2*D3**, в ячейку **C3** – формулу =**C1-C2*D3**(рис. 71).



	A	B	C	D
1	58	1	0	
2	43	0	1	
3	=ОСТАТ(A1;A2)	=B1-B2*D3	=C1-C2*D3	=ЧАСТНОЕ(A1;A2)
4				

Рис. 71. Пример реализации расширенного алгоритма Евклида

- Выделить диапазон ячеек **A3:D3** и растянуть (скопировать) на несколько строк вниз, пока в столбце **A** не будет получено нулевое значение (рис.72).



	A	B	C	D
1	58	1	0	
2	43	0	1	
3	15	1	-1	1
4	13	-2	3	2
5	2	3	-4	1
6	1	-20	27	6
7	0	43	-58	2
8	#ДЕЛ/0!	#ДЕЛ/0!	#ДЕЛ/0!	#ДЕЛ/0!

Рис. 72. Результаты вычислений k^{-1} по расширенному алгоритму Евклида

- Значение k^{-1} находится в предпоследней строке в столбце **C**, то есть, в строке, предшествующей строке, начинающейся с 0. Строка с результатом должна начинаться с 1.

Для рассматриваемого примера значение k^{-1} содержится в ячейке **C6**, $k^{-1}=27$.

ЗАМЕЧАНИЕ: Если полученоотрицательное значение k^{-1}, следует взять его по модулю $p-1$. Для этого можно использовать функцию **ОСТАТ()** или просто сложитьзначениеk^{-1} со значением $p-1$.

6. Вычислить число sпо формуле$s=k^{-1}u\bmod(p-1)$. Для вычисления можно воспользоваться функцией **ОСТАТ()**. Подписать полученное значение s.

   В примере $s=27\cdot37\bmod(59-1)=13$.
7. Сформировать цифровую подпись сообщения M–пару чисел (r,s).

Для рассматриваемого примера получили цифровую подпись сообщения M: (32, 13).

ЗаданиеВ.Проверить правильность вычисления сгенерированной цифровой подписи.

8. Для проверки правильности вычисления полученной цифровой подписи следует произвести ее проверку с помощью открытого ключа абонента и убедиться, что подпись подлинная. Сформируем открытый ключ y абонента по формуле $y=g^x\bmod p$:
- Для вычисления значения y в среде MSExcel может быть использован алгоритм быстрого возведения в степень по модулю или линейный итерационный алгоритм, описанный в пункте 3.

   Для рассматриваемого примера получаем$y=14^{34}\bmod59=20$.
9. Вычислить и подписать значения $y^r\bmod p$и $r^s\bmod p$, а затем их произведение по модулю p.

   В примере получаем:

   $y^r\bmod p=20^{32}\bmod59=35$,

   $r^s\bmod p=32^{13}\bmod59=10$,

   $y^r\cdot r^s\bmod p=35\cdot10\bmod59=55$.
10. Вычислить и подписать значение $g^h\bmod p$, значение hбыло получено в пункте 2.

В примере $g^h \bmod p = 14^{23} \bmod 59 = 55$.

11. Проверить выполнение равенства $y^r \cdot r^s \bmod p = g^h \bmod p$: если равенство выполняется – можно сделать вывод, что подпись подлинная, значит она была вычислена правильно (при условии правильности значения $h(M)$).

В примере получили 55=55, равенство выполняется, значит подпись сгенерирована правильно.

ЗаданиеС.Известны значения общих параметров системы Эль-Гамаля: p=59, g=14 иоткрытый ключ абонента y.От абонента получено сообщение M(в числовом представлении), снабженное цифровой подписью Эль-Гамаля вида (r,s). Проверить подлинность цифровой подписи. Хэш-значение сообщение вычисляется с помощью учебного алгоритма, начальное значение h_0 принимается равным числу десятичных разрядов в числовом представлении M.

12. Выбратьиз таблицы 35открытый ключ отправителя y, текст M и значение цифровой подписи (r,s)в соответствии с номером варианта.

Таблица 35

Варианты задания

Вариант	Открытый ключ отправителя y	Полученное сообщение M	Цифровая подпись	
			r	s
1	9	8723	23	43
2	25	3361	37	29
3	7	8722	11	34
4	35	7005	34	47
5	6	9054	39	56
6	37	2401	24	48
7	24	5524	33	9
8	48	4382	47	40
9	50	6525	44	31
10	2	7993	50	14
11	39	7865	40	49
12	12	3217	10	6
13	3	8593	30	42
14	54	6620	2	39

15	43	1229	54	32
16	15	1333	31	9
17	10	2301	42	29
18	52	6543	13	48
19	21	9922	33	8
20	4	2211	18	11
21	42	1122	43	54
22	46	1211	24	12
23	49	5421	52	25
24	23	5241	55	16
25	33	6540	6	26

Проверить подлинность цифровой подписи для полученного сообщения *M* по аналогии с рассмотренным далее примером.

Пример. Получено сообщение *M*=7569 с подписью(32,46), *r*=32; *s*=46.Известен открытый ключ отправителя *y*=20. Проверить подлинность подписи сообщения.

13. Вычислить и подписать значения $y^r \bmod p$ и $r^s \bmod p$, а затем их произведение по модулю *p*:

- Вычисления проводить на новом листе книги MSExcel.Для вычисления значения степени по модулю в среде MSExcel может быть использован быстрый алгоритм возведения в степень по модулю или линейный итерационный алгоритм, описанный в пункте 3.

В рассматриваемом примере получаем:

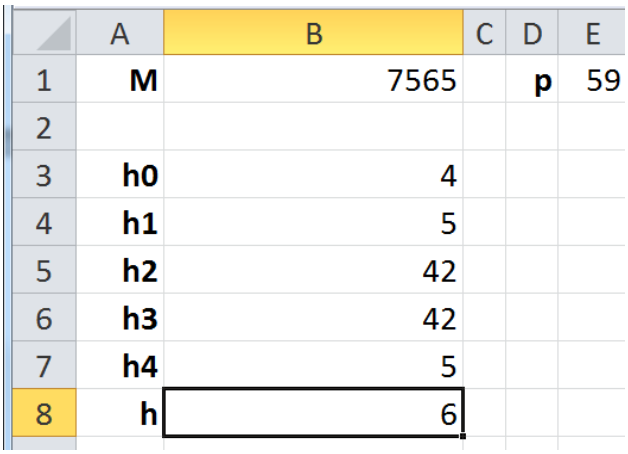
$y^r \bmod p = 20^{32} \bmod 59 = 35$,

$r^s \bmod p = 32^{46} \bmod 59 = 15$,

$y^r \cdot r^s \bmod p = 35 \cdot 15 \bmod 59 = 53$.

14. Для полученного сообщения вычислить хэш-код*h*(*M*)аналогично пункту 2.

Результаты вычислений для рассматриваемого примера приведены на рис.73.Получили: *h*=6.



	A	B	C	D	E
1	**M**	7565		**p**	59
2					
3	**h0**	4			
4	**h1**	5			
5	**h2**	42			
6	**h3**	42			
7	**h4**	5			
8	**h**	6			

Рис. 73.Пример вычисления хэш-значения сообщения

15. Вычислить значение $g^h \bmod p$.

    В примере $g^h \bmod p = 14^6 \bmod 59 = 15$.

16. Проверить выполнение равенства$y^r \cdot r^s \bmod p = g^h \bmod p$, если равенство выполняется – можно сделать заключение, что подпись подлинная, в противном случае – подпись фальшивая.

    В примере получили $53 \neq 15$, равенство не выполнено, значит, подпись фальшивая.

17. Продемонстрировать результаты выполнения практической работы преподавателю.

ТЕМА 7. КРИПТОГРАФИЯ НА ЭЛЛИПТИЧЕСКИХ КРИВЫХ

В последние время все большее распространение в криптографии находит одна из областей теории чисел и алгебраической геометрии – теория эллиптических кривых над конечными полями.

В общем случае уравнение *эллиптической кривой* E имеет вид:

$$y^2+axy+by = x^3+cx^2+dx+e.$$

ПустьK – поле: либо поле R вещественных чисел, либо поле Q рациональных чисел, либо поле C комплексных чисел, либо конечное поле F_q из $q=p^r$ элементов, p– простое.

Существуют поля, содержащие элементы $a \neq 0$ такие, что $p \cdot a = 0$ при целом p, отличном от нуля. Так, в конечном поле, состоящим из двух элементов 0 и 1 имеем: $2 \cdot 1 = 1 + 1 = 0$.

Характеристикой поля K называется наименьшее натуральное число p, такое, что $p \cdot 1 = 0$, где 1 и 0 – единичный и нулевой элементы K соответственно.

Если такого числа не существует, то характеристика поля по определению равна 0 (например, характеристики полей R вещественных, Q рациональных и C комплексных чисел с бесконечным числом элементов равны 0).

Пусть K – поле характеристики, отличной от 2 и 3, и x^3+ax+b – кубический многочлен без кратных корней, а $b \in K$. *Эллиптическая кривая над* K – это множество точек (x,y), $x,y \in K$, удовлетворявших уравнению

$$y^2=x^3+ax+b,$$

вместе с единственным элементом, обозначаемым O и называемым *точкой в бесконечности*.

Условие отсутствия кратных корней у кубических многочленов в правой части приведенного выше уравнения кривой эквивалентно требованию, чтобы все точки кривой были неособенными.

Рассмотрим теперь поле вещественных чисел $K=R$, тогда эллиптическая кривая E – обычная плоская кривая с добавлением еще одной точки в бесконечности O; E имеет вид $y^2=x^3+ax+b$.

Пусть E – эллиптическая кривая над вещественными числами, и пусть P и Q – две точки на эллиптической кривой E. Тогда точки $-P$ и $P+Q$ определены по следующим правилам:

1. Точка O – тождественный элемент по сложению (нулевой элемент) группы точек кривой.

Так, $O=-O$ и для любой точки P: $P+O=P$.

Далее предполагается, что ни P, ни Q не являются точками в бесконечности.

2. Точки P и $-P$ имеют одинаковые x-координаты, а их y-координаты различаются только знаком, т.е. $-(x,y)=(x,-y)$. Из уравнения кривой следует, что $(x,-y)$ – также точка на E.

3. Если P и Q имеют различные x-координаты, то прямая, проходящая через эти точки, имеет с E еще только одну точку пересечения R', за исключением двух случаев:

- когда прямая оказывается касательной в точке P, тогда полагают $R'=P$,
- когда прямая оказывается касательной в точке Q, тогда полагают $R'=Q$.

Суммадвухточекэллиптической кривой $P+Q$ определена как точка $R = -R'$, т.е. как отражение от оси x третьей точки пересечения кривой проведенной через эти точки прямой. Геометрическое построение, дающее $P+Q$, приведенона рис.74.

4. Если $Q = -P$ (т. е. x-координата у точки Q та же, что и у P, а y-координата отличается лишь знаком), то сумму этих двух точекполагают равной «точке в бесконечности»: $P+Q = O$ (это является следствием правила 1, то есть $P–P = O$).

В графической интерпретации точку в бесконечности O следует представлять расположенной на оси y в предельном направлении, определяемом все более «крутыми» касательными к кривой. Она является «третьей точкой пересечения» с кривой E для любой вертикальной прямой: такая прямая пересекается с кривой в точках вида (x,y), $(x, -y)$и в точке O.

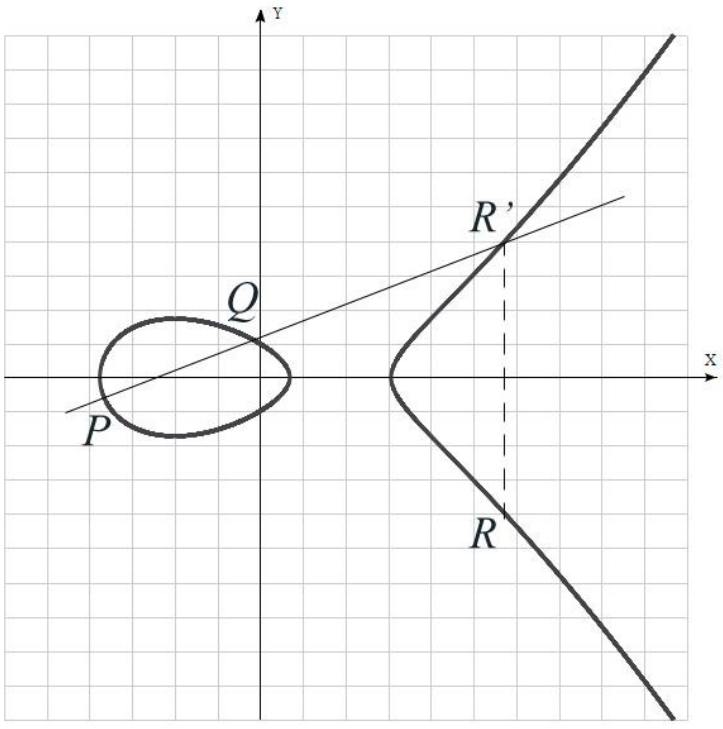


Рис. 74. Геометрическое построение суммы двух точек эллиптической кривой

5. Пусть $P=Q$,тогда считают, что прямая, проходящая через P и Q, – касательная к кривой Eв точке P. Пусть R' – единственная другая точка пересечения этой прямой с E. Полагают$P+Q=-R'$ (в качестве R' берутP, если касательная в P имеет «двойное касание», т.е. если Pявляется точкой перегиба кривой).

Введенная таким образом операция сложения подчиняется всем обычным правилам сложения, в частности коммутативному и ассоциативному законам.

УмножениеnPточки P эллиптической кривой на положительное число $n(n>0)$ определяется как сумма n точек P. Если n – не положительно ($n\leq 0$), то nP определяется как сумма $|n|$ точек $-P$.

Обозначим (x_1,y_1), (x_2,y_2) и (x_3,y_3) – координаты точек P, Q и $R=P+Q$ соответственно. Выразим x_3,y_3 через x_1,y_1, x_2 иy_2.

Если $P\neq Q$, то координаты $P+Q$вычисляются как:

$$x_3=\left(\frac{y_2-y_1}{x_2-x_1}\right)^2-x_1-x_2,$$

$$y_3=-y_1+\frac{y_2-y_1}{x_2-x_1}(x_1-x_3).$$

Или, определив λ как $\frac{y_2-y_1}{x_2-x_1}$,

$$x_3=\lambda^2-x_1-x_2,$$

$$y_3=-y_1+\lambda(x_1-x_3).$$

В случае если $P=Q$, то $P+Q=P+P=2P$. Координаты удвоенной точки $2P$:

$$x_3=\left(\frac{3x_1^2+a}{2y_1}\right)^2-2x_1,$$

$$y_3=-y_1+\frac{3x_1^2+a}{2y_1}(x_1-x_3).$$

Или, определив λ как $\frac{3x_1^2+a}{2y_1}$,

$$x_3=\lambda^2-2x_1,$$

$$y_3=-y_1+\lambda(x_1-x_3).$$

Эллиптические кривые над конечным полем

В криптографии используются эллиптические кривые над конечным полем F_q из $q=p^r$ элементов, где pявляется *простым числом*.

Эллиптической группой по модулю p– $E_p(a,b)$определяется как множество, состоящее из точки в бесконечностиO и пар неотрицательных целых чисел (x, y), таких, что:$0 \le x<p, 0 \le y<p$и удовлетворяют условию:

$y^2=x^3+ax+b(\mathrm{mod}p)$,

где a и b – целые числа меньше p и удовлетворяют $(4a^3+27b^2)\mathrm{mod}p\neq 0$.

Выполнение условия$(4a^3+27b^2)\mathrm{mod}p\neq 0$ означает, что кубический многочлен $y^2=x^3+ax+b(\mathrm{mod}p)$ не имеет кратных корней.

Элементы группы $E_p(a,b)$ – точки эллиптической кривойбудут находиться в квадрате неотрицательных чиселот (0,0) до (p,p).

Для эллиптических кривых аналогом умножения двух чисел служит сложение двух точек эллиптической кривой E, определенной над F_q. Таким образом, аналог возведения числа в степень k – это умножение точки эллиптической кривой $P\in E$ на целое число k.

Практическая работа №16. Вычисление координат точек эллиптической кривой над конечным полем

Координаты точки $R= (x_3, y_3)$ эллиптической кривой Eнад конечным полем характеристикиp, отличной от 2 и 3: $R=P+Q$, $P\neq Q$, $P,Q,R\in E$определяются как

$$x_3 = \lambda^2 - x_1 - x_2 \pmod p,$$
$$y_3 = -y_1 + \lambda(x_1 - x_3) \pmod p,$$
$$\lambda = \frac{y_2 - y_1}{x_2 - x_1} \pmod p.$$

Координаты кратной точки $R = 2P$, $P,R\in E$определяются:

$$x_3 = \lambda^2 - 2x_1 \pmod p,$$
$$y_3 = -y_1 + \lambda(x_1 - x_3) \pmod p,$$
$$\lambda = \frac{3x_1^2 + a}{2y_1} \pmod p.$$

Пример. Пусть P=(3,13),Q=(9,7) – точки эллиптической кривой$E_{23}(1,1)$: $y^2=x^3+x+1(\mathrm{mod}23)$.

1. Найти$R=P+Q$.$x_1=3$, $x_2=9$, $y_1=13$, $y_2=7$, $a=1$.

Вычислимλдля суммы точек: $\lambda=(13-7)/(9-3)\bmod 23= 6/6 \bmod 23 = 1$.

Тогда$x_3=1-3-9\bmod 23 =-11\bmod 23 =12$;

$y_3=-13+(3-9)=-13-6\bmod 23 =-19\bmod 23 =4$.

$R=(12,4)\in E_{23}(1,1)$.

2. Найти$R=2P$.

Вычислимλдля двойной точки: $\lambda=(3\cdot 3^2+1)/(2\cdot 13)\bmod 23=28/26\bmod 23$. Требуется вычислить значение натуральной дроби по модулю. Это можно сделать с помощью расширенного алгоритма Евклида.

Вычисление значения натуральной дроби по модулю

Значение $a/b\bmod p$, где p – простое число, может быть получено следующим образом.

Поскольку p – простое число, то оно будет взаимно простым с любым другим целым числом b, $|b|\neq kp$, $k\in Z$. Числа b и p – взаимно просты НОД$(b,p)=1$. Значит, существуют такие целые числа x и y, что $bx+py=1$. Числа x и y можно найти с помощью расширенного алгоритма Евклида, $x = b^{-1}\bmod p$.

Представим$a/b\bmod p$как:

$a/b\bmod p=a\cdot 1/b\bmod p=a\cdot b^{-1}\bmod p = a\cdot x\bmod p$.

Вычислимзначение$\lambda=28/26 \bmod 23$.

Спомощьюрасширенногоалгоритма Евклиданайдемx и y, такиечто $26x+23y=1$:

Формируем строки $U\leftarrow\{\max(26,23),1,0\}$, $V\leftarrow\{\min(26,23),0,1\}$, $k=u_1\operatorname{div}v_1$, $T=\{u_1\bmod v_1$, $u_2-k\cdot v_2$, $u_3-k\cdot v_3\}$покаt_1нестанетравным 0.

Так как $26>23$, шаги расширенного алгоритма Евклида примут следующий вид (рис. 75).

Найдены значения $x=$ 8, $y=$ -9, проверка $26\cdot 8-9\cdot 23=208-207=1$.

шаг	1	2	3	4	рез-т		строки		k
	U					26	1	0	
	V	U				23	0	1	
1	T	V	U			3	1	-1	1
2		T	V	U		2	-7	8	7
3			T	V	U	1	8	-9	1
4				T	V	0	-23	26	2

Рис. 75. Вычисления по расширенному алгоритму Евклида

Тогда λ=28/26mod23=28·8mod23=224mod23=17.

Теперь можно вычислитькоординаты (x_3, y_3) двойной точки $R \in E_{23}(1,1)$, $R=2P$. Согласно формуле для вычисления координат двойной точки:

$x_3=17^2-2\cdot 3 \bmod 23 = 289-6 \bmod 23 = 283 \bmod 23 = 7$,

$y_3=-13+17\cdot(3-7) \bmod 23 = -13-17\cdot 4 \bmod 23 = -13-68 \bmod 23 = -81 \bmod 23 = 11$.

Точка $R=2P=(7,11)\in E_{23}(1,1)$.

Как видно, вычисление кратных точек может быть достаточно трудоемким. Аналогично методу быстрого возведения в степень по модулю (описан в практической работе №9 Изучение шифра RSA), кратное точки эллиптической кривой $kP\in$Еможно найти не более чем за $2\log k$операций методом повторного удвоения.

Представим целое kкак последовательность умножений на 2 и сложений с 1.Например, чтобы найти $100P$, представим $k=100$ как$100=2(2(1+2\cdot 2\cdot 2(1+2)))$. Тогда можно записать$100P=2(2(P+2(2(2(P+2P)))))$.Таким образом, значение кратной точки эллиптической кривой $100P$может быть вычисленос помощью 6 удвоений и 2 сложений точек на кривой.

Кроме того, если известно число N точек на эллиптической кривой E и если $k>N$, то в силу равенства $NP=O$, можно заменить значение k его наименьшим неотрицательным вычетом по модулю N ($k'=k \bmod N$).

Задание. Дан конкретный вид $E_p(a,b)$ эллиптической кривой над конечным полем простой характеристики$p\neq$ 2, 3, а также че-

тыре точки этой кривой $P,Q,R,S \in E_p(a,b)$ и целое число n. Вычислить координаты суммы точек и кратной точки.

A. Найтиточку $2P+3Q-R$

B. Найти точку nS.

Указания к выполнению практической работы

Для выполнения практической работы рекомендуется использовать файл *элл.xls*, реализующий вычисления координат суммы двух точек и двойной точки для эллиптической кривой $E_{751}(-1,1)$, определенной в заданиях.Также можно реализовать вычисления самостоятельно в табличном процессоре MSExcel (функции **ОСТАТ** и **ЧАСТНОЕ**).

Технология выполнения задания

Задание A. Даны три точки P,Q,Rна эллиптической кривой $E_{751}(-1,1)$. Найти $2P+3Q-R$.

1. Изучить теоретическое описание эллиптических кривых и определение операций над точками эллиптических кривых.
2. Выбрать координаты точекP,Q,Rиз таблицы 36в соответствии с номером варианта.

Таблица 36

Варианты задания

№	*Координаты точек на* $E_{751}(-1,1)$				n
	P	Q	R	S	
1	(58, 139)	(67, 667)	(82, 481)	(62, 372)	128
2	(61, 129)	(59, 365)	(105, 369)	(43, 527)	116
3	(62, 372)	(70, 195)	(67, 84)	(39, 171)	110
4	(56, 332)	(69, 241)	(83, 373)	(43, 527)	107
5	(59, 386)	(70, 195)	(72, 254)	(36, 87)	111
6	(72, 497)	(61, 622)	(70, 556)	(49, 568)	122
7	(74, 170)	(53, 277)	(86, 25)	(39, 580)	109
8	(48, 702)	(69, 241)	(98, 338)	(75, 318)	142
9	(59, 386)	(61, 129)	(100, 364)	(45, 720)	111
10	(72, 497)	(53, 474)	(90, 730)	(78, 480)	147
11	(59, 365)	(59, 386)	(105, 382)	(53, 474)	120
12	(61, 622)	(61, 622)	(90, 730)	(43, 527)	109

№	*Координаты точек на $E_{751}(-1,1)$*				*n*
	P	*Q*	*R*	*S*	
13	(61, 129)	(69, 510)	(72, 497)	(49, 568)	124
14	(70, 556)	(56, 419)	(86, 726)	(39, 171)	108
15	(67, 84)	(69, 241)	(66, 199)	(49, 183)	126
16	(73, 72)	(56, 332)	(85, 35)	(58, 139)	121
17	(69, 241)	(53, 277)	(106, 24)	(33, 355)	111
18	(74, 581)	(53, 277)	(85, 35)	(39, 580)	101
19	(56, 419)	(69, 510)	(79, 640)	(44, 366)	113
20	(58, 612)	(67, 84)	(83, 373)	(73, 72)	103
21	(62, 379)	(53, 474)	(110, 622)	(85, 716)	159
22	(53, 277)	(66, 552)	(99, 456)	(66, 199)	103
23	(67, 667)	(53, 474)	(105, 382)	(44, 385)	113
24	(69, 241)	(66, 552)	(69, 510)	(45, 720)	111
25	(69, 510)	(53, 277)	(105, 369)	(39, 171)	107

Выполнить вычисление суммы точек по аналогии с рассмотренным ниже примером.

Пример. $P,Q,R \in E_{751}(-1,1)$. P=(384,475), Q=(227,452),R=(69,510). Требуется определить координаты точки $2P+3Q-R$.

3. Вычислить координаты точки $2P$, P=(384,475):

- Занести координаты точки в файл *элл.xlsx*(в ячейки **A2**, **B2**).
- Ячейки **F4:F5**содержат значение λ=442367/950mod 751, рассчитанное по формуле суммы точек.
- Требуется вычислить значение дробипо модулю 442367/950 mod 751. Сначала с помощью расширенного алгоритма Евклида следует вычислить значение, обратное делителю по модулю, то есть 950^{-1}mod 751.Расширенный алгоритм Евклида для двойной точки реализован в диапазоне ячеек **O1:R13**. Если делитель дроби (в рассматриваемом примере 950) меньше значения модуля, то есть основания кривой (в примере 751), то результат извлекается из предпоследней значащей ячейки столбца **P** (в диапазоне **O1:R13**). В противном случае результат извлекается из предпоследней значащей ячейки столбца **Q** в указанном диапазоне. Поскольку в рассматриваемом примере де-

литель дроби больше значения модуля (950>751), результат извлекается из ячейки **Q10** (рис.76), $950^{-1} \bmod 751 = -137$.

	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R
1	P			Q				R			p	a	b	**2P**	950	0	1	
2	384	475									751	-1	1		751	1	0	
3	**2P**						**Q+R**								199	-1	1	1
4		3*384^2-1		442367		442367		-		0		0			154	4	-3	3
5	Л=	2*475	=	950	=	950	Л=	-	=	0	=	0			45	-5	4	1
6				-317				#ДЕЛ/0!							19	19	-15	3
7	=	-140230339					=	#ДЕЛ/0!							7	-43	34	2
8	=	136					=	#ДЕЛ/0!							5	105	-83	2
9															2	-148	117	1
10	x=	136^2-2*384	=	17728			x=	#ДЕЛ/0!	=	#ДЕЛ/0!					1	401	-317	2
11				**455**						**#ДЕЛ/0!**					0	-950	751	2
12	y=	-475+136(384-455	=	-10131			y=	#ДЕЛ/0!	=	#ДЕЛ/0!					#ДЕЛ/0!	#ДЕЛ/0!	#ДЕЛ/0!	#ДЕЛ/0!
13				**383**						**#ДЕЛ/0!**					#ДЕЛ/0!	#ДЕЛ/0!	#ДЕЛ/0!	#ДЕЛ/0!
14		Проверка						Проверка						**Q+R**	751	0	1	
15		383^2	=	146689	244			#ДЕЛ/0!	=	#ДЕЛ/0!	####				0	1	0	
16		455^3-1*455+1	=	94195921	244			#ДЕЛ/0!	=	#ДЕЛ/0!	####				#ДЕЛ/0!	#ДЕЛ/0!	#ДЕЛ/0!	#ДЕЛ/0!
17															#ДЕЛ/0!	#ДЕЛ/0!	#ДЕЛ/0!	#ДЕЛ/0!
18															#ДЕЛ/0!	#ДЕЛ/0!	#ДЕЛ/0!	#ДЕЛ/0!
19															#ДЕЛ/0!	#ДЕЛ/0!	#ДЕЛ/0!	#ДЕЛ/0!

Рис.76. Интерфейс программы элл.xlsx

- Занести значение, обратное делителю по модулю, в ячейку **D6**.Результирующее значение λ содержится в ячейке **B8**.
- Координаты точки $2P$ содержатся в ячейках **D11**и **D13**соответственно.
- Проконтролировать правильность вычислений. Значения ячеек **E15** и **E16** содержат левую и правую части уравнения эллиптической кривой$E_{751}(-1,1)$, вычисленные для найденных координат точки. Если эти значениясовпадают,тоточка удовлетворяет уравнению кривой. Проверка показывает правильность расчета координат точки $2P$ = (455,383).

4. Аналогичным образом вычислить координаты точки $2Q$, Q=(227,452).

   Результат: $2Q$ = (34,74).

5. Вычислить координаты точки $3Q = 2Q + Q$, $2Q$ = (34,74), Q=(227,452):

- Занести координаты одной точки в ячейки **D2**, **E2**, другой точки – в ячейки **H2**, **I2**.
- Ячейки **L4:L5**содержат значение λ=378/193mod 751, рассчитанное по формуле суммы точек.
- Требуется вычислить значение дроби по модулю 378/193mod 751. Сначала с помощью расширенного алгоритма Евклида следует вычислить значение, обратное делителю по модулю,

то есть $193^{-1} \bmod 751$. Расширенный алгоритм Евклида для суммы точек реализован в диапазоне ячеек **O14:R25**. Если делитель дроби меньше значения модуля, то результат извлекается из предпоследней значащей ячейки столбца **P**в рассматриваемом диапазоне. В противном случае результат извлекается из предпоследней значащей ячейки столбца **Q** в рассматриваемом диапазоне. Поскольку в примере делитель дроби меньше значения модуля (193<751), результат извлекается из столбца **P** (ячейка**P19**), $193^{-1} \bmod 751 = 179$.

- Полученное значение занести в ячейку **J6**.
- Ячейки **J11**и **J13**содержат координаты суммы точек, рассчитанные по формуле сложения точек. 3*Q* = (417,137).
- Ячейки **K15** и **K16** содержат проверочные значения, их совпадение показывает правильность расчета координат точки 3*Q*.

6. По аналогии с предыдущим пунктом вычислить координаты суммы точек 2*P*+3*Q*, 2*P* = (455,383), 3*Q* = (417,137). 2*P*+3*Q* = (493,122).
7. Вычислить 2*P*+3*Q*–*R*, 2*P*+3*Q* = (493,122), *R*=(69,510):

- Вычислить координаты точки -*R*, для чего следует взять *y*-координату точки с отрицательным знаком по модулю.
  -y = -510 mod 751 = 751 – 510 = 241.
  -*R* = (69,241).
- Вычислить сумму точек 2*P* + 3*Q* = (493,122) и -*R*=(69,241). Окончательно получаем: 2*P*+3*Q*–*R* = (623,166).

Задание B. Дана точка*S*на эллиптической кривой $E_{751}(-1,1)$. Найти кратную точку*nS*.

8. Выбрать координаты точки*S*и значение *n*из таблицы 36 в соответствии с номером варианта. Выполнить вычисление кратной точки по аналогии с рассмотренным примером. Для вычислений рекомендуется использовать файл *элл.xlsx*.

Пример. *S*=(623,166)$\in E_{751}(-1,1)$,*n*=27. Определить координаты точки *nS*.

9. Поскольку операции с точками эллиптической кривой достаточно трудоемки, для вычисления *nS* следует воспользоваться методом последовательного умножения на два. Для этого надо

представить число *n*как последовательность операций умножения на 2 и сложения с 1. $n=27=1+2(1+2(2(1+2)))$. Тогда $nS=27S=S+2(S+2(2(S+2S)))$.Провести последовательное вычисление этого выражения.

10. Вычислить$2S$, $S=(623,166)\in E_{751}(-1,1)$.

- Вычислить координаты двойной точки $2S$ с помощьюфайла*элл.xlsx* по аналогии с п.3.
  $2S=(680,93)$.

11. Вычислитькоординаты суммы точек $S+2S=(623,166)+(680,93)$с помощью файла*элл.xlsx* по аналогии с п.5.
    $S+2S=(561,611)$.
12. Вычислить $2(S+2S)=2(561,611)=(484,379)$.
13. Вычислить $2(2(S+2S))=2(484,379)=(90,730)$.
14. Вычислить $S+2(2(S+2S))=(623,166)+(90,730)=(250,737)$.
15. Вычислить $2(S+2(2(S+2S)))=2(250,737)=(294,156)$.
16. Вычислить$S+2(S+2(2(S+2S)))=(623,166)+(294,156)=$ (617,293).
    Получен результат: $27S=(617,293)$.
17. Показать результаты вычислений точек преподавателю.

Практическая работа №17. Цифровая подпись на эллиптических кривых

Описание выбора параметров криптосистем на эллиптических кривых и алгоритма цифровой подписи

В криптографии используются эллиптические кривые над двумя типами конечных полей: простыми полями большой нечетной простой характеристики (F_p, где $p>3$) и полями характеристики 2 ($GF(2^m)$, где m–простое число).

Большинство криптосистем современной криптографии с открытым ключом естественным образом можно «переложить» на эллиптические кривые, однако не для всех схем это дает выигрыш в стойкости. Например, аналог алгоритма RSA в варианте на эллиптических кривых не имеет преимуществ перед своим оригиналом. Выигрыш при переходе на эллиптические кривые получают те криптографические схемы, стойкость которых основана

на сложности задачи логарифмирования в конечных полях. Обусловлено это тем, что при надлежащем выборе параметров кривой задача логарифмирования в группе точек кривой существенно сложнее задачи логарифмирования в мультипликативной группе исходного поля.

Переход на эллиптические кривые позволяет существенно увеличить стойкость схемы ключевого обмена Диффи-Хелмана(ECDH), криптосистемы Эль-Гамаля и цифровой подписи DSA (ECDSA). Для сравнения: старый российский стандарт ЭЦП оперировал 1024-битовыми блоками данных, новый оперирует 256-битовыми и 512-битовыми. При этом по оценкам специалистов, трудоемкость взлома старого и нового стандартов ЭЦП России (с 256-битовыми строками) сопоставимы.

В качестве международного стандарта цифровой подписи принят американский алгоритм цифровой подписи на эллиптических кривых (ECDSA). В этом стандарте используются эллиптические кривые над полем $GF(2^m)$ характеристики 2. Однако криптографически стойких кривых над полем такой характеристики сравнительно мало.

Российский ГОСТ Р 34.10–2012 «Информационная технология. Криптографическая защита информации. Процессы формирования и проверки электронной цифровой подписи» определяет два варианта подписи с использованием эллиптических кривых над полем большой простой характеристикиF_p, p – большое простое число порядка 256 ($2^{254}<p<2^{256}$) и 512 бит($2^{508}<p< 2^{512}$).

Выбор кривой и точки на ней для систем электронной цифровой подписи подразумевает решение ряда вспомогательных задач. Прежде всего, это подсчет количества N точек на кривой (*порядка кривой*), а также определения *порядка* генерирующей точкиG.

Существует несколько классов криптографически слабых кривых, которых следует избегать:кривые над $GF(2^m)$, где m – не простое число и кривые над полями простой характеристикиF_p, для которых число точек кривой N совпадает с p ($N= p$). Таким образом, требуется знать число Nточек эллиптической кривой.

Следует также отметить, что хотя для реализации систем Диффи-Хеллмана или шифрсистемыЭль-Гамаля не требуется

знать количество N точек кривой, на практике нужно быть уверенным в надежности этих систем, которая зависит от того, имеет ли Nбольшой простой делитель. Если Nявляется произведениммалых простых чисел, то криптосистема может быть вскрыта с помощью методаПолига-Силвера-Хеллмана. Таким образом, желательно, чтобыNбыло большим простым числом, то есть надо знать значение N.

Вместе с тем, задача нахождения значение N не является тривиальной. При достаточно больших значениях pгенерация и подсчет перебором всех точек кривой неэффективны. Существует полиномиальные алгоритмы нахождения числа точек N кривой (метод больших-малых шагов, метод Шуфа и др.), которые на практике дают весьма удовлетворительные результаты.

После того, как порядок N кривой определен, требуется найти большой простой делитель n порядка кривой. Такой делитель может не существовать, и тогда потребуется повторять процедуру выбора кривой до тех пор, пока не будут выполнены все требуемые условия. Поиск числа n может потребовать как решения задачи разложения на множители числа N, так и доказательства простоты числа n.

Использование криптосистем цифровой подписи на эллиптических кривых подразумевает также выбор «генерирующей» точки кривой и определение ее порядка.

ПорядкомпточкиP на эллиптической кривой называется такое наименьшее натуральное число, что $nP = O$.Если конечного n не существует, то говорят о точке бесконечного порядка.

Пример. Найти порядок точки P=(2,3) на $y^2=x^3+1$. Находим, что $2P$=(0, 1), $4P$=2(2P)=(0,-1). Поэтому $4P$=-2P и, следовательно, $6P=O$. Тем самым порядок P может быть равен 2, 3 или 6. Но $2P$=(0,1)$\neq O$, а если бы P имела порядок 3, то было бы $4P=P$, что неверно. Итак, Pимеет порядок 6.

Для получения криптографически стойкой системы ЭЦП должны выполняться следующие условия:

1. Порядок точки G, используемой в системе ЭЦП, должен быть большим простым числом n (в отечественном стандарте $2^{254}<n< 2^{256}$ или $2^{508}<n< 2^{512}$).
2. $N\neq p$ и $N\neq p+1$, где N – порядок кривой.

3. $p^k \neq 1 (\mathrm{mod} n)$для всех $k=1,\ldots,C$, где C настолько велико, что вычислить дискретный логарифм в F_{p^C} за приемлемое время невозможно.

Отечественный стандарт цифровой подписи устанавливает $C = 31$ ($2^{254} < n < 2^{256}$) и $C = 131$ (если $2^{508} < n < 2^{512}$).

Эллиптическую кривую Eможно выбирать случайным образом так, чтобы выполнялись указанные условия.

Точку Gможно выбрать следующим образом. Найдем случайную точку $G' \in E(F_p)$ и вычислим $G = \frac{N}{n} G'$. Если $G \neq O$, то требуемая точка найдена, если же $G = O$, то следует выбрать другую точку G'.

Как видно, выбор кривой и «генерирующей» точки на ней является достаточно сложным.

Имеются готовые рекомендации по выбору конечных полей и эллиптических кривых, обеспечивающие высокий уровень безопасности и эффективность программной реализации. Так, американский институт стандартов и технологий NISTрекомендует 15 эллиптических кривых. Стандарт FIPS 186-4 рекомендует 10 конечных полей, в частности:

- поля простой характеристики F_p, где простое p имеет длину 192, 224, 256, 384 или 521 бит;
- поля GF(2^m), где m=163, 233, 283, 409 или 571.

Причем для каждого конечного поля рекомендуется конкретный вид эллиптической кривой, при этом значение параметра a в уравнении кривой принимается равным -3 для ускорения вычислений.

Для каждого из вариантов цифровой подписи ГОСТ Техническим комитетом 26«Криптографическая защита информации»Росстандарта предложен конкретный вид эллиптической кривой (рекомендации по стандартизации «Задание параметров эллиптических кривых в соответствии с ГОСТ Р 34.10–2012»). Здесь значение a также равно -3, для кривой указана «генерирующая» точка и ее порядок.

Конкретный вид кривойE, «генерирующая» точка Gна ней с указанием порядка этой точки nявляются общими для всех пользователей. Для генерации и проверки подписи требуется задание

и индивидуальных параметров каждого пользователя – еголичного (секретного) и открытого ключей.

Ключ подписи (личный ключ) –случайное число d, $0<d<n$. Ключ проверки подписи (открытый ключ) –точка эллиптической кривой $Q=dG$.

Алгоритм цифровой подписи также использует хэш-функцию, обозначаемую h.Подпись ГОСТ Р 34.10-2012 использует Хэш-функцию, определенную вГОСТ Р 34.11-2012: в случае $2^{254}<n<2^{256}$ используется хэш-функция с длиной кода 256 бит, а в случае $2^{508}<n<2^{512}$ – 512-битовая хэш-функция.

Генерация подписи

Входные данные: сообщение M, открытые параметры ЭЦП: E, $G\in E$, n, секретный ключ подписи d.

Выходные данные: подпись (r,s).

Алгоритмгенерации подписи

1. Выбрать случайное число k в интервале $[1,n-1]$.
2. Вычислить $(x,y)=kG\in E$.
3. Вычислить $r=x \bmod n$.
4. Если $r=0$, то вернуться к шагу 1.
5. Вычислить $z=k^{-1} \bmod n$.
6. Вычислить $h=h(M)$.
7. Вычислить$s=z(h+dr) \bmod n$.
8. Если $s=0$, то вернуться к шагу 1.
9. Вывести пару (r,s) – подпись к M.

Замечания.

1. При $r=0$ результат вычисления s не зависит от секретного ключа d.

2. При $s=0$не существуетнеобходимого для проверки подписи числа $s^{-1} \bmod n$.

Проверка подписи

Входные данные: сообщение M, открытые параметры ЭЦП: E, $G\in E$, n, открытый ключ проверки подписи $Q\in E$и подпись (r,s) к M.

Выходные данные: заключение о подлинности или фальсификации подписи.

Алгоритм проверки подписи

1. Если хотя бы одно из условий $0<r<n$, $0<s<n$ нарушается, то подпись фальшивая и работа алгоритма закончена.
2. Вычислить $h=h(M)$.
3. Вычислить$v=s^{-1}\bmod n$.
4. Вычислить$u_1=hv\bmod n$.
5. Вычислить$u_2=rv\bmod n$.
6. Вычислить$X=(x,y)\in E$: $X=u_1G+u_2Q$.
7. Если $r=x\bmod n$, то подпись действительная, в противном случае подпись фальшивая.

Задание. Задан конкретный вид $E_p(a,b)$ эллиптической кривой над конечным полем (p – простое), генерирующая точка $G\in E_p(a,b)$ и порядок этой точки n.

A. Сгенерировать ЭЦП для сообщения с известным значением хэш-кодаh, зная заданные значения секретного ключа подписи d и случайного числа k.

B. Проверить подлинность подписи(r,s) для сообщения с известным значением хэш-кодаh, зная открытый ключ проверки подписи Q.

Указания к выполнению практической работы

Для выполнения практической работы рекомендуется использовать файл *элл.xls*, реализующий вычисления координат суммы двух точек и двойной точки для эллиптической кривой $E_{751}(-1,1)$, определенной в заданиях.

Технология выполнения задания

Задание A. Сгенерировать цифровую подпись сообщения.Известные общие параметры системы цифровой подписи: вид кривой $E_{751}(-1,1)$, координаты генерирующей точки $G=(416,55)$ и порядок этой точки $n=13$.

1. Изучить описаниеаналога схемы Эль-Гамаля на эллиптических кривых.
2. Выбрать из таблицы 37в соответствии с номером варианта значения личного ключа абонентаd, хэш-кода сообщенияh и случайного числа kдля генерации подписи сообщения.

Таблица 37

Варианты задания

	A E_{751}(-1,1)и генерирующая точка G = (416, 55) порядка n = 13			***B*** E_{751}(-1,1)и генерирующая точка G=(562,89) порядкаn = 13		
№	*h*	*d*	*k*	*h*	*Q*	(*r*,*s*)
1	9	3	5	8	(135,82)	(11,10)
2	3	9	6	4	(384,475)	(11,9)
3	12	9	2	7	(596,433)	(11,1)
4	3	4	7	7	(455,368)	(11,11)
5	5	12	6	7	(384,475)	(5,5)
6	6	12	7	5	(384,475)	(11,1)
7	8	5	5	10	(455,383)	(11,10)
8	8	2	5	8	(384,276)	(3,1)
9	11	5	6	3	(135,669)	(11,10)
10	10	9	2	6	(455,383)	(3,1)
11	11	2	8	2	(596,433)	(3,10)
12	8	6	3	10	(455,368)	(11,6)
13	3	10	6	5	(596,433)	(11,12)
14	2	11	5	9	(135,82)	(7,7)
15	10	5	11	2	(596,433)	(11,4)
16	11	5	7	6	(596,318)	(7,5)
17	6	10	7	5	(596,318)	(7,4)
18	6	10	2	12	(135,669)	(5,11)
19	9	6	6	12	(562,89)	(3,2)
20	8	12	8	6	(562,662)	(7,10)
21	3	2	8	12	(135,82)	(7,8)
22	6	5	6	7	(384,276)	(5,2)
23	7	3	7	8	(596,318)	(11,6)
24	9	11	2	10	(384,276)	(7,6)
25	5	12	8	9	(416,696)	(11,11)

3. Вычислить значение подписи – пару чисел (*r*, *s*) по аналогии с рассмотренным далее примером.

Пример. Выбрана эллиптическая кривая E_{751}(-1,1) и генерирующая точка G=(384,475) порядка n=13 (13 – наибольший из делителей порядка кривой N=728). Абонент хочет подписать своим личным ключом d=12 сообщение, хэш-код которого h=12.Пусть абонент, подписывающий сообщение, выбрал случайное k=3.

4. Вычислить$kG=3G=3\cdot(384,475)$.

- Вычислить сначала $2G=2\cdot(384,475)$ с помощью файла *элл.xlsx*. $2G=(455,383)$.
- Вычислить $3G=G+2G=(384,475)+(455,383)$. $3G=(596,318)$.

5. $kG=3G=(596,318)$, $x=596$. Вычислить$r=x \bmod n=596 \bmod 13=11$.
6. С помощью расширенного алгоритма Евклидавычислить $z=k^{-1} \bmod n=3^{-1} \bmod 13=-4 \bmod 13=9$.
7. Вычислить$s=z(h+dr) \bmod n=9\cdot(12+12\cdot 11) \bmod 13=9$.

Таким образом, вычислена цифровая подпись сообщения – пара $(r,s)=(11,9)$.

Задание В. Проверить подлинность цифровой подписи.Известны общие параметры системы цифровой подписи: вид кривой $E_{751}(-1,1)$, координаты генерирующей точки $G=(562,89)$ и порядок этой точки $n=13$.

8. Выбрать значения открытого ключаQ отправителя сообщения, подписи (r,s) и h– хэш-кода сообщения из таблицы 37в соответствии с номером варианта.
9. Провести проверку подписи аналогично рассмотренному далее примеру.

Пример. Выбрана эллиптическая кривая $E_{751}(-1,1)$ и генерирующая точка $G=(384,475)$ порядка $n=13$. Получено сообщение с известным хэш-кодом$h=12$ и подписью (11,9). Требуется проверить подлинность данной подписи, если известен открытый ключ абонента, подписавшего сообщение, $Q=(384,276)$.

10. Проверка подписи начинается с проверки условий $0<r<n$, $0<s<n$ – в данном случае они соблюдаются ($0<11<13$, $0<9<13$).
11. С помощью алгоритма Евклида вычислить значение$v=s^{-1} \bmod n= 9^{-1} \bmod 13=3$.
12. Вычислить $u_1=hv \bmod n=12\cdot 3 \bmod 13=10$, $u_2=rv \bmod n= 11\cdot 3 \bmod 13=7$.
13. С помощью файла *элл.xlsx* вычислить координаты точки$X=u_1G+u_2Q=10\cdot(384,475)+7(384,276)=(596,318)$.
14. $X=(596,318)$, $x=596$,сравнить значения $r=11$ и $x \bmod n=596 \bmod 13=11$.Значения совпадают, значит, подпись подлинная.

15. Продемонстрировать результаты практической работы преподавателю.

ЛИТЕРАТУРА

1. *Бабенко Л.К., Ищукова Е.А*. Современные алгоритмы блочного шифрования и методы их анализа.: учеб. пособие. – М.: Гелиорс-АРВ, 2006.
2. *Васильева И.Н*. Криптографические методы защиты информации:учебник и практикум для академического бакалавриата.– М.: Юрайт, 2016.
3. *Васильева И.Н*. Криптографическая защита информации: учеб. пособие. – СПб.: СПбГЭУ, 2011.
4. *Васильева И.Н*. Криптографическая защита информации: практикум. – СПб.: СПбГЭУ, 2011.
5. *Васильева И.Н., Куватов В.И., Потехин В.С*. Криптографическая защита информации: учеб. пособие – СПб: Изд-во СПб ун-та МВД России, 2016.
6. *Жданов О.Н., Золотарев В.В*. Методы и средства криптографической защиты информации: учеб. пособие. – Красноярск: Сиб. гос. аэрокосмич. ун-т, 2008.
7. *Жданов О.Н.,Куденкова И.А.*Криптоанализ классических шифров: лаб. практикум для студ. спец. 090105, 090106. – Красноярск: Сиб. гос. аэрокосмич. ун-т, 2009.
8. *Жданов О.Н.,Лубкин И.А*. Алгоритм RSA: метод. указания к выполнению лабораторных работдля студ. спец. 090105. – Красноярск: Сиб. гос. аэрокосмич. ун-т, 2007.
9. *Ожиганов А.А*. Основы криптоанализа симметричных шифров: учеб. пособие – СПб.: СПбГУ ИТМО, 2008.
10. *Панасенко С.П*. Алгоритмы шифрования. Специальный справочник. – СПб.: БХВ-Петербург, 2009.
11. *Рябко Б.Я.* Криптографические методы защиты информации:учеб. пособие для ВУЗов. – М.: Горячая линия, 2015.
12. *Столлингс В*. Криптография и защита сетей: принципы и практика. – М.:Вильямс, 2001.

ПРИЛОЖЕНИЯ

Приложение1.*Варианты заданий практической работы №4.Криптоанализ шифра простой замены*

1.

58 62 32 39 99 31 29 58 72 62 99 58 13 54 15 56 31 63 39 72 84 15 13 56 77 15 82 56 56 56 58 54 29 77 56 - 39 99 56 31 56 77 32 12 15 54 31 48 76 63 15 52 13 39 72 39 54 16 72 39 32 72 62 58 58 15, 37 62 77 52 39 13 39 72 39 32 39 31 62 54 39 77 84 39 21 31 39 16 72 62 99 58 13 15 54 56 13 46 16 39 58 13 95 16 15 13 62 12 46 31 39 62 72 15 77 54 56 13 56 62 84 31 39 32 56 76 58 63 62 72 33 62 12 39 54 62 33 62 58 52 39 91 99 62 29 13 62 12 46 31 39 58 13 56. 56 31 63 39 72 84 15 82 56 39 31 31 48 62 13 62 76 31 39 12 39 32 56 56 16 72 39 33 31 39 54 39 53 12 56 54 37 56 77 31 62 58, 39 37 72 15 77 39 54 15 31 56 62, 16 72 39 56 77 54 39 99 58 13 54 39, 39 13 52 72 48 54 33 62 12 39 54 62 52 95 31 62 37 48 54 15 12 48 62 54 39 77 84 39 21 31 39 58 13 56 16 39 58 52 39 72 39 58 13 56 16 39 12 95 33 62 31 56 29 56 39 37 72 15 37 39 13 52 62 56 31 63 39 72 84 15 82 56 56, 15 13 15 52 21 62 16 39 15 54 13 39 84 15 13 56 77 15 82 56 56 16 72 39 56 77 54 39 99 58 13 54 62 31 31 48 76, 95 16 72 15 54 12 62 31 33 62 58 52 56 76 56 56 31 48 76 16 72 39 82 62 58 58 39 54.

2.

39 25 20 34 82 63 66 46 35 20 25 82 86 39 51 74 35 51 66 20 44 37 25 27 51 35 44 20 90 37 51 25 25 51 63 91 20 11 37 46 48 25 20 37 61 51 14 82 82 66 82 35 29 82 91 25 51 74 51 24 78 51 24 59 46 86 51 44 74 20 25 37 37, 37 44 82 31 11 37 82 51 46 25 51 34 82 25 37 82 86 37 25 27 51 35 44 20 90 37 51 25 25 48 44 46 82 78 25 51 14 51 18 37 59 44, 51 74 82 35 20 90 37 59 44 66 90 82 25 25 48 44 37 61 10 44 20 18 20 44 37, 86 61 20 25 86 51 39 66 86 51 44 10 66 82 86 46 51 35 10 37 66 51 46 51 39 51 63 66 39 59 91 37. 56 46 51 86 20 66 20 82 46 66 59 24 35 10 18 37 78 51 35 18 20 25 37 91 20 90 37 63, 46 51, 66 51 18 14 20 66 25 51 35 82 91 10 14 29 46 20 46 20 44 35 20 91 14 37 56 25 48 78 37 66 66 14 82 24 51 39 20 25 37 63, 35 10 86 51 39 51 24 37 46 82 14 37 44 25 51 18 37 78 37 91 25 37 78 91 25 20 31 46 51 61 51 66 25 51 39 25 48 78 39 37 24 20 78 10 18 35 51 91, 25 51 25 82 10 24 82 14 59 31 46 24 51 14 42 25 51 18 51 39 25 37 44 20 25 37 59 24 20 25 25 48 44 39 51 74 35 51 66 20 44, 66 56 37 46 20 59, 56 46 51 51 61 82 66 74 82 56 82 25 37 82 37 25 27 51 35 44 20 90 37 51 25 25 51 63 61 82 91 51 74 20 66 25 51 66 46 37 25 82 37 44 82 82 46 66 44 48 66 14 20, 82 66 14 37 51 46 66 10 46 66 46 39 10 82 46 39 37 24 37 44 20 59 10 18 35 51 91 20.

3.
74 29 23 27 17 99 71 25 49 32 29 34 27 63 32 25 17 99 60 62 25 34 95 29 53 59 82 27 71 29 77 99 34 27 91 17 99 71 49 99 27 15 60 32 25 50 27 17 62 27 95 27 50 25 91 32 59 77 95 29 50 25 99 59, 25 99 74 29 53 25 59 17 99 25 91 23 49 71 25 17 99 60 49 25 34 32 25 71 95 27 82 27 32 32 25 29 50 17 25 15 77 99 32 59 77 62 95 25 53 95 29 23 32 25 17 99 60 34 15 35 17 27 99 27 71 25 12 25 99 95 29 45 49 74 29. 62 95 27 63 34 27 71 17 27 12 25, 50 27 17 62 27 95 27 50 25 91 32 29 35 95 29 50 25 99 29 17 29 82 49 83 62 25 17 27 50 27 62 95 25 34 59 74 99 25 71 50 27 53 25 62 29 17 32 25 17 99 49 17 71 35 53 29 32 29 17 32 29 15 49 23 49 27 82 32 29 34 27 63 32 25 95 29 50 25 99 29 77 10 27 12 25 25 50 25 95 59 34 25 71 29 32 49 35 49 95 27 53 27 95 71 49 95 25 71 29 32 49 27 82 74 95 49 99 49 23 32 89 83 74 25 99 74 29 53 59 50 15 25 74 25 71 62 49 99 29 32 49 35 49 53 29 62 25 82 49 32 29 77 10 49 83 59 17 99 95 25 91 17 99 71. 34 15 35 62 25 17 15 27 34 32 49 83 25 62 99 49 82 29 15 60 32 25 62 95 49 82 27 32 27 32 49 27 34 49 17 74 25 71 89 83 82 29 17 17 49 71 25 71 12 25 95 35 23 27 91 53 29 82 27 32 89. 74 29 23 27 17 99 71 25 49 32 29 34 27 63 32 25 17 99 60 95 29 50 25 99 89 34 25 17 99 49 12 29 27 99 17 35 25 62 99 49 82 49 53 29 67 49 27 91 62 95 25 12 95 29 82 82 32 25 12 25 25 50 27 17 62 27 23 27 32 49 35.

4.
48 23 18 40 94 35 62 53 94 25 53 15 35 91 35 40 35, 52 23 52 53 40 35 94 35 40 23 94 23 91 52 94 49 24 23 84 89 94 23 64 55 53 15 18 53 91, 24 53 88 23 62 12 25 76 94 23 64 35 24 49, 35 94 49 88 53 48 94 23 24, 41 91 35 91 23 52 31 49 15 53 91. 47 91 35 41 49 62 84 91 62 35 35 91 41 23 84 91 25 31 29 24 35 64 35 27 35 88 53 94 23 91 35, 52 35 91 35 55 35 53 35 94 25 84 64 29 91 23 24, 52 35 40 15 23 48 23 62 53 55 94 49 24 48 23 49 40 35 24 25 41 49 91 89 94 53 94 23 24 53 91 53 24 94 23 15 53 62 49 12 52 49, 12 53 15 12 49 60 53 18 49 94 23 62 84 91 55 53 41 49. 53 40 35 94 35 40 23, 62 29 48 62 23 62 84 62 35 25 18 15 62 25 88 53 94 25 53 18 52 35 24 53 31 23 94 25 53 62 35 48 15 49 27 23, 64 35 24 49 41 25 24 23 35 91 55 23 88 53 94 94 29 76 84 25 40 94 23 24 35 64 55 53 64 38 91 84 91 62 25 25 94 23 64 49 91 25 25 64 35 41 91 25 62 91 49 88 53 84 53 52 49 94 15 49 49 15 23 55 25 24 23 84 89 35 31 35 41 91 35 - 91 35. 52 23 52 35 76-91 35 64 55 53 15 18 53 91 84 40 24 49 27 25 18 84 91 49 52 35 18 35 91 24 53 91 53 24 62 91 53 18 94 35 91 49.

5.
63 49 26 30 96 49 86 30 28 59 52 86 46 21 52 79 35 38 79 52 50 59 21 35 21 31 79 30 26 96 85 42 61 21 61 85 30 85 24 79 52 74 30 61 59 31 21 42 21 35 90, 78 35 79 30 88 79 59 52 79 49 21 24 79 59 35 21 49 85 52 85 50 61 30 79 88 96 79 50 61 79 30 28 24 79 49 79 52 90 59 35 49 85 30, 85 67 79 96 21

49 61 79 24 28 46 85 30 14 35 79 88 79 78 30 52 79 49 30 31 21 31 50 79 30 50 28 49 79 59 38 85 29 30 61 85 91 85 50 85 31 79 49 59 30 50 50 79 85 50 26 79 26 86 35 31 21 50 26 96 30 24 21 35 90 88 52 21 59 61 79 59 35 85 50 30 35 79 24 30 88 79 96 21 67 79 35 86 61 30 96 21 42 28 29 30 50 52 63 52 79 50 79 30 59 21 50 79 52 91 67 85 30. 31 96 79 50 30 35 79 88 79, 63 67 86 52 88 79 96 24 35 30 50, 78 35 79 50 61 30 28 24 21 52 79 59 90 61 30 35 79 52 90 31 79 79 49 52 21 24 30 35 90 50 30 35 79 24 79 50 38 79 52 50 59 21, 61 79 85 26 96 85 50 30 61 85 35 90 30 88 79 61 21 24 30 52 30 85 42 21 59 52 28 74 85 35 90 14 35 85 50 26 79 38 49 21 52 28 50 79 30 88 79 24 96 28 88 21. 38 79 52 50 59 49 42 63 52 26 21 52 31 28 28 50 30 61 63 85 42 96 28 31 85 61 30 59 31 79 52 90 31 79 50 85 61 28 35 96 21 42 88 52 63 24 86 49 21 52 30 30 61 30 49 79 79 96 28 74 30 61 61 86 50 88 52 21 42 79 50. 26 79 35 79 50, 63 49 61 79 42 21 85 61 35 30 96 30 59 79 49 21 49 46 85 59 90 78 30 50-35 79, 79 35 52 79 74 85 52 26 21 26 85 96 79 59 28 49 59 35 79 96 79 61 28, 26 79 24 79 46 30 52 31 79 31 61 28 85 59 61 79 49 21 59 35 21 52 79 59 50 21 35 96 85 49 21 35 90 26 21 52 31 28, 61 79 28 74 30 78 30 96 30 42 28 49 30 52 85 78 85 35 30 52 90 61 79 30 59 35 30 31 52 79.

6.

732749632954822929703529132313822949513018541513132949234829134956 30

82277032632749897049292349822929,97562782293570154942353097303563 89

923082307335231829821554277335295429633 0.27827029353263704256166329612982541 6,5127562735166723703013733527973256306 3,32,6116632323732749702732137063305429823223 13,82293529243063492370156527543256

898230112763275630822797896 7.291316822954307030633073275127238230702392973270302332542923275130512713-562773353292353097822713491638

2949567029,32278256273254296327497335302432703063132982 23,822970325430636332239729612 7-6332112749563530828227612 7,51276154306527543263497032923256301332732711276389821513,328229496315243063633249271130978929612763302 3.732749632954823295702773352749494235 97

303563899292305430703063138229274927112982822797304956 27,3229612761276327495435271830637335324256271327567027638229823223.7327138267,513051492995973049,822954296332923056353254275635306132972949 51

276127492711155632232373275478296530637029972935271351113049512935 70 326389-6527636316.4942359730356389924956272363705470293523655427 13

30.237015632992329224303530113082303 2,732754279554235182291316,705435166192301329563263,97562727824913275635325651165430-5627972935299213272973632997274970153530182982322913733529542963898227612716183049307061633092306 5.2351351656272711293582166349233216497329635627638951271329638951271316703254295689704930132713512782482929 30636329325130512729-562718327027568227297035275429112763892427612797293582276127562963298251 30.494235973035638992111563705630512713702763822982323232495635306529,97562713822973353224632749897327955632 56165430,615429278227733527132963895182166327,3273274913275635295 6 89,5116543027822754296327498 9.822756301382329729612782291115632 7.

7.

534934751365756827361324366265726818682868 34,34746826681862659136 13 28683413276875398368506234102639,23266826506227,3610341318366813, 751091629175682736132436629 1.537568341318801336366836108318107536 68. 506227685062726818104928682713722413,13752753506268366874104910277544831075915718366291,13752753506227685062721844493668537527447468263668,13752753506223266826831034532739683650622775131862 91,7596139113362636629153752613361091535336109168741868919613911336261 3 506227685062361096101810831036682426 68-365350572839836865105036681 3.573662276813535013757591627527133636681 3-68267574577453.2668722810 5062,3610341318366813,751810495749106568261327687539181050682610263 9.685044491026132739366849106568261327687539506 2,83682668915724 2668 261074531334134553181049281810861078265326181350577826281344261327393 6 68752653.347513-261074532618572836688318533462743657263974266891 57, 24266836534513261091688613265062263950687210266815.538368232668915736132668506224366872681049101826105336136568241326754436139113 28 271336366834494426397544491028132768,106568241326754475137526393468285336534923265365103426685057756834,346826342326682674181075366215757553365391,532834533657263936108327448 6,8368832710341026397510743410271036726891,6850726818132639,836874532810263991444247 5 1813504426109153532753682662757410263983137410,2713243975365391

34831868652710283668157468913610261336108368275753347583689136532639 34751365681868801313.

8.

31 14 10 69 53 28 53 26 53 14 22 53 45 14 34 77 53 77 31 47 31 67 53 93 47 84 26 10 47 84 77 90 93 28 34 45 84 10 93 67 28 53 26 67 31 67 37 26 34 31 67 14 58 17 53 53 47 67 97 77 10 31 10 14, 45 84 67 56 34 26 31 90 28 75 10 89 67 28 49 67 47 39 86 34 47 84 31 14 34 77 53 58 11 84 67 37 28 34 45 84 90 69 67 14 13 34 77 47 84 10 84 22 31 67 67 26 39 13 34 77 77 90 37 97 10 93 31 10 84 49 10 49 67 89 67-14 53 52 67 89 67 47 39 69 10 26 47 84 31 10 47 34 89 67 26 34 47 39 26 47 10 28 53, 11 49 67 77 67 28 53 45 34 47 49 53 28 56 67 84 34 77 17 53 10 14 67 28 53, 34 47 84 34 47 84 31 34 77 77 67, 47 97 67 14 67 84 90 28 97 10 56 10 47 67 28. 77 10 69 67 47 49 10 97 10 84 22, 45 84 67 56 26 53 11 84 67 28 67 77 31 67 31 47 34 77 34 53 28 34 14 31 31 53 69 39 26 67 47 47 53 58 47 34 34 31 34 45 77 90 28 11 49 67 77 67 28 53 45 34 47 49 53 28 69 34 24 53 17 53 84 67 28, 67 89 26 67 28 77 90 28 89 67 47 39 69 10 26 47 84 31 34 77 77 90 28 69 67 14 89 67 28 53 56 39 47 84 67 37 49 10 97 77 67 37. 14 34 77 53 77 56 26 53 47 28 10 84 26 53 31 10 14 47 70 49 75 31 34 37 17 10 26 53 53, 47 45 53 84 10 70 11 84 39 28 10 14 34 77 22 49 39 58 47 84 26 10 77 39 53 69 34 10 14 22 77 67 37 69 14 70 67 47 39 86 34 47 84 31 14 34 77 53 70 47 31 67 53 93 56 14 10 77 67 31 28 53 26 67 31 67 89 67 89 67 47 56 67 69 47 84 31 10. 26 10 47 56 67 14 67 13 34 77 77 10 70 31 17 34 77 84 26 34 34 31 26 67 56 90, 28 77 67 89 67 70 97 90 45 77 10 70, 67 56 39 84 10 31 75 10 70 47 31 67 53 28 53 97 67 14 67 84 90 28 53 86 39 56 10 14 22 17 10 28 53 31 34 47 22 28 53 26 45 34 26 34 97 28 34 13 69 39 77 10 26 67 69 77 39 58 47 53 47 84 34 28 39 52 10 77 49 67 31, 53 28 34 77 77 67 75 31 34 37 17 10 26 53 70, 56 67 97 10 28 90 47 14 39 31 67 13 69 70, 69 67 14 13 77 10 52 90 14 10 47 84 10 84 22 84 67 37 52 10 97 67 37, 67 84 49 39 69 10 26 34 31 67 14 58 17 53 70 77 10 45 77 34 84 56 67 52 34 69 77 90 37 28 10 26 75 56 67 31 47 34 37 34 31 26 67 56 34 , 56 26 67 52 53 31 10 70 47 34 52 34 69 67 26 67 89 39, 49 10 49 84 10 26 10 77 67 28, 84 90 47 70 45 10 28 53 84 67 77 77 75 31 34 37 17 10 26 47 49 67 89 67 97 67 14 67 84 10.

9.

15655670109476477151339456502816513373925076281556761756495170155692 50. 9276-244986921643,474984495150473349285047945076569486165670624915567615927649317643865047335133965012765176565 0,509276-925676861643,474992162476514749473349248649732433155047331751494733475047496249735149474776765694861656707351174749317651332549927626158149563324498649 92

491556334750474931763312509456339276922850479450241756706233515133
7647769212765176561643866528514926152476155149736510963362927615568649
287692504733496247504056765615814956511028164315656262284912945094 763176-513328762486509250765694501250.
7349477031331540567631761581
495650627631154733625056705676517094761550625149473347335133317686
2865477692.926249155649157615516584509633623331761565735086155692494747
76317628504794502816513315439250814947161576568665734733943392154943
947662624986814915943343338150155647164328504794769215567651332516.47
5073767656735056707376518447764962658449155692652486761556164386651515
943343713347504715769216431551658450963343,8170333362494750,247628
7651705849268150155633,76155650513315702849129249155647166233.47504376
731715702476735086491556766233247673924986315017157024165694506233
331273499250564951701556925062,76473373769476472550287686765133157012
501576127350925049626510734915175633514956331762338665151594651071334750
47157692651015331556496265,47764733767333477133475047153315569262
3386494749627684495651338147762486765633927615567617567092767686658449
4747766265865012287610,7686315047331276925047477662654750155062766292 161576947662317615657350861556924947477662658676924749.

10.

90 65 91 15 25 90 20 65 56 69 31 65 91 17 15 17 40 54 40 17 52 54 56 61 15 62 15 26 29 25 31 17 88 15 65 91 90, 13 15 91 20 91 15 52 29 40 90 88 31 65 49 90 91 40 54 40 65 12 88 40 56 62 15 26. 43 88 40 62 15 44 65 91 17 15 65 40 88 91 90 49 88 58 44 90 90 65 91 15 25 90 62 40 44 90, 52 31 25 15 29 15 91 15 44 90 34 56 62 90 29 90 29 15 44, 88 40 75 25 90 44 31 25, 75 15 62 40 71 31 91 17 40 44, 49 91 15 52 25 31 62 90 61 58 54 90 75 15-65 17 15 31 44 56 75 25 40 17 58, 15 91 88 15 65 20 90 65 91 15 25 90 84 62 15 61 54 40 65 91 90 90 65 62 56 65 65 91 17. 75 15 29 90 65 91 15 25 90 31 26 15 88 90 75 15 88 90 44 40 54 90 13 56 29 15 71 31 65 91 17 31 88 88 58 26

25 40 65 65 62 40 43 15 29 15 65 91 15 75 40 44 20 91 88 58 13 65 15 61 58 91 90 20 13 90 54 90 21 40 13. 43 40 29 40 49 40 90 65 91 15 25 90 62 40 65 15 65 91 15 20 54 40 56 88 90 13 17 91 15 44, 49 91 15 61 58 75 31 25 31 29 40 91 12 65 54 56 36 40 91 31 54 20 44 90 49 90 91 40 91 31 54 20 44 17 44 31 65 91 31 65 99 65 91 31 91 90 49 31 65 62 90 44 88 40 65 54 40 71 29 31 88 90 31 44 90 25 20 29 88 25 40 17 65 91 17 31 88 88 58 13 88 40 43 90 29 40 88 90 26. 91 31 71 31 21 31 54 90 75 25 31 65 54 31 29 15 17 40 54 15 90 90 65 62 56 65 65 91 17 15. 17 65 17 15 31 44 75 15 17 31 65 91 17 15 17 40 88 90 90 29 25 31 17 88 90 31 90 65 91 15 25 90 62 90 65 91 25 31 44 90 54 90 65 12 62 75 25 40 17 29 31 90 91 15 49 88 15 65 91 90, 88 15 65 91 25 15 52 15 26 15 61 33 31 62 91 90 17 88 15 26 44 31 25 62 90 90 65 91 90 88 58 56 88 90 13 88 31 65 56 69 31 65 91 17 15 17 40 54 15. 44 40 54 15 99 91 15 52 15, 40 88 91 90 49 88 58 26 90 65 91 15 25 90 62, 17 31 25 88 58 26 65 17 15 90 44 13 56 29 15 71 31 65 91 17 31 88 88 58 44 43 40 29 40 49 40 44, 65 49 90 91 40 54 17 15 43 44 15 71 88 58 44 56 62 25 40 36 40 91 12 75 15 17 31 65 91 17 15 17 40 88 90 31 65 15 43 88 40 91 31 54 12 88 58 44 17 58 44 58 65 54 15 44. 90 91 40 62, 88 40 75 31 25 17 58 13 75 15 25 40 13 90 65 91 15 25 90 20 15 75 25 31 29 31 54 20 31 91 65 20, 62 40 62 13 56 29 15 71 31 65 91 17 31 88 88 15-75 25 40 52 44 40 91 90 49 31 65 62 90 26 25 40 65 65 62 40 43 15 29 15 65 91 15 75 40 44 20 91 88 58 13 65 15 61 58 91 90 20 13 90 54 90 21 40 13.

11.

24 40 42 36 36 45 82 14 69 65 36 95 89 36 67 14 90 36 45 58 34 89 34 58 95 14 63 14 45 40 27 24 40 45 67 45 49 14 63 59 36 42 40 67 19, 25 14 95, 95 40 65 34 14 82 14 17 34 63 24 65 34, 65 36 14 63 59 36 42 65 34 45 67 34 82 58 65 36 67 45 49 45 67 36 25, 90 67 34 34 45 65 34 11 65 47 36 11 14 24 47 67 95 40 24 14 56 14 34 65 65 34 89 34 67 34 17 82 14 11 40 59 27 24 27 67 14 45 90 36 95 17 40 65 47. 63 40 17 40 45 47 65 36 18 67 14, 89 40 63 40, 27 89 82 49 65 36 59 36 45 58 34 65 36 90 65 47. 90 36 25 59 34 82 19 32 36 25 47 14 45 17 34 82 19 63 27 36 25 69 67 14 11 14 24 47 69 65 36 95 89 36 67 14 90 36 45 58 34 89 34 45 47 95 19 49, 67 36 25 25 36 65 19 32 36 14 70 34 45 67 40 36 67 45 49 14 67 36 25 24 34 95 34 42 36 45 58 40 42 24 47 25 24 65 36 25 34 65 14 65 40 25 34 59 70 34 24 49 67 45 49 . 65 36 45 25 34 67 95 49 65 40 67 34 , 90 67 34 58 34 82 14 90 36 45 67 11 34 95 40 63 11 36 24 40 65 65 47 70 63 40 17 40 45 34 11 65 36 58 34 67 34 95 47 70 69 65 36 95 89 36 67 14 90 36 45 58 14 70 95 36 45 27 95 45 34 11, 65 40 17 95 14 25 36 95, 65 36 18 67 14, 11 34 63 95 40 45 67 40 36 67, 17 36 95 36 24 90 36 82 34 11 36 90 36 45 67 11 34 25 27 42 36 45 36 89 34 24 65 49 11 45 67 40 36 67 63 40 24 40 90 40 34 45 11 34 36 65 14 49 65 36 14 45 90 36 95 17 40 36 25 47 70 14 45 67 34 90 65 14 58 34 11 69 65 36 95 89 14 14.

12.

82 36 45 65 47 36 17 34 42 40 95 47 25 34 89 27 67 11 34 63 65 14 58 65 27 67 19 17 34 90 67 14 11 82 30 59 34 36 11 95 36 25 49 89 34 24 40. 24 40 42 36 11 34 11 95 36 25 49 34 45 36 65 65 14 70 24 34 42 24 36 73 - 34 67 25 34 82 65 14 14. 45 47 95 34 73 82 36 45 65 36 59 27 24 36 67 89 34 95 36 67 19 67 40 58, 58 40 58 45 27 70 34 73, 65 34 34 65 59 27 24 36 67 89 34 95 36 67 19. 34 24 65 40 58 34, 14 65 67 36 65 45 14 11 65 34 45 67 19 67 40 58 14 70 82 36 45 65 47 70 17 34 42 40 95 34 11, 58 40 58 17 95 40 11 14 82 34, 34 90 36 65 19 25 40 82 40, 67 40 58 14 36 17 34 42 40 95 47 65 36 17 95 36 24 45 67 40 11 82 49 30 67 59 34 82 19 32 34 73 34 17 40 45 65 34 45 67 14. 34 65 14 27 25 36 65 19 32 40 30 67 58 34 82 14 90 36 45 67 11 34 65 40 58 34 17 82 36 65 65 34 89 34 67 34 17 82 14 11 40 14, 45 82 36 24 34 11 40 67 36 82 19 65 34, 11 65 36 58 34 67 34 95 34 25 45 25 47 45 82 36 17 95 36 24 34 67 11 95 40 23 40 30 67 59 34 82 36 36 34 17 40 45 65 47 36, 14 65 67 36 65 45 14 11 65 47 36 17 34 42 40 95 47. 45 52 67 34 73 56 36 82 19 30 90 40 45 67 34 17 82 40 65 14 95 27 30 67 14 45 58 27 45 45 67 11 36 65 65 47 36 17 34 42 40 95 47, 58 34 67 34 95 47 36 17 95 14 24 34 82 42 65 34 25 58 34 65 67 95 34 82 36 49 11 82 49 30 67 45 49 52 18 18 36 58 67 14 11 65 47 25 45 95 36 24 45 67 11 34 25 17 95 36 24 34 67 11 95 40 23 36 65 14 49 45 14 82 19 65 47 70 17 34 42 40 95 34 11.

13.

75 37 46 48 55 12 32 52 99 61, 99 20-20 55 52 32 25 55 60 52 46 91 32 25 52 46 78 46 63 55 25 55 75 57 32 25 55 46 37 55 11 75 46 60 60 57 32 28 32 52 99 32 37 15 63 46 78 46 67 32 25 99 46 11 55 57 25 15 11 52 46 46 74 32 52 99 57 39 29 70 70 32 75 57 57 55 75 46 78 46 11 46 48 11 41 52 55 46 37 52 46 60 32 91 32 57 32 46 25 46 12 46 78 99 28 32 37 75 99 63 11 55 52 52 19 63. 46 11 52 55 75 46 37 15 45 32 37 57 60 15 61 57 67 25 46 37 57 19 32 37 67 46 37 46 30 19 46 67 25 32 11 32 12 32 52 99 41 46 75 46 52 28 55 52 99 41 75 25 99 57 99 28 32 37 75 46 36 46 67 55 37 52 46 37 57 99 67 46 48 55 25 55. 32 37 12 99 67 46 37 12 32 11 46 48 11 41 25 55 37 63 46 11 60 46 11 19 60 46 37 37 57 55 52 55 60 12 99 60 55 32 57 37 41 99 15 30 19 60 55 32 57 37 46 30 19 28 52 46 36 37 75 46 25 46 37 57 39 61, 57 46 52 32 67 46 37 25 32 11 37 57 60 32 52 52 55 41 15 78 25 46 20 55 30 46 12 39 18 46 78 46 67 46 48 55 25 55 91 99 52 46 60 55 12 55. 75 25 15 57 46 36 37 67 55 11 99 60 46 20 60 25 55 57 75 60 32 12 99 28 99 52 32 37 57 46 75 55 11 46 11 46 48 11 41 46 20 52 55 28 55 32 57 , 28 57 46 11 46 48 11 39 52 32 11 55 12 25 32 20 15 12 39 57 55 57 46 60. 99 37 67 46 12 39 20 46 60 55 52 99 32 91 55 57 32 91 55 57 99 28 32 37 75 99 63 67 25 99 32 91 46 60 55 52 55 12 99 20 55 15 37 12 46 60 99 36 60 46 20 52 99 75 52 46 60 32 52 99 41 67 46 48 55 25 46 60 30 32 37 37 67 46 25 52 46 67 46 60 19 37 99 57 57 46 28 52 46 37 57 39 67 25 46 78 52 46 37 57 99 28 32 37 75 46 36 91 46 11 32 12 99. 52 46 99 67 25 32 11 12 55 78 55 32 91 19 36 91 32 57 46 11 67 25 46 78 52 46 20 55 67 25 99 60 12 32 75 55 57 32 12 32 52 37 60 46 32 36 67

25 46 37 57 46 57 46 36 99 41 37 52 46 37 57 39 61 99 91 46 48 32 57 30 19 57 39 25 32 55 12 99 20 46 60 55 52 37 67 46 91 46 45 39 61 52 32 37 12 46 48 52 46 36 75 46 91 67 39 61 57 32 25 52 46 36 57 32 63 52 99 75 99.

14.

1146127846326025329141326025466732363775996367155732183237576032
5252997546 6060375725745274636046375746757467462574487412 99,6046-
673225601963, 3032115246375739527425461174,6046-
605746251963,6719185246375739, 37
4667155737576015619374414899205299205274579 9,60-
57253257399963,6732
3757254657746046375746285246784630742074257 4.75465257257437571930
321152
4637579999304678745737576074326025466732365519523225321175464630
424137
5241129952324832127452993291463752466052463691743737195274373212
32529941
9952573252379960524657251511995739374 1,67253211674628573252993291
257430
465732114637157874.16574657602078124111674660322563524637573252995
2
325746283252.527437749146911132123 2,52746046375746753299201125326
0
1232553252991237415725151 1,52467546527525325752193657251511917437
57
322574,67254640323737994652741274.52323712152874365246604637574628
5219
3278462546117460466037329191992532371274609912993739672546992060
4611
9991199160529963407425404625469 1,183212754691,46251548993291.5246
5725151160469991415274754667123252993 6,75465746251932914648524699
3767461239204660745739111241674637123211156193327846257437189925
32529941
3760463278461132127 4,57747555325299911936207467741152199146309332
3757
604691,52326746469325411237 41,74523225321175469946371548117412374
1 527460463757467532.527416574667466012994112995232574612397546253
2129978994620521932553252524637579 9,52469967253211375774601232529932
4630467874573757603275747567463757464152524636603212992899523 2.205274
289957,32371299461199523015113257375725329199573937416746121528995739

304612391832,11251578469115523299203032485246114637577452325737419132 52391832.

15.

45 74 54 31 10 26 38 23 74, 86 74 54 25 89 26 38 16 74 74 75 16 45 56 90 25 86 90 75 90 10 26 16 74 23 56 86 75 45 16 75 74 95 10 13 31 95 10 51 74 16 89 74, 36 75 95 75 59 36 74 95 74 91 75 31 89 90 23 74 74 90 36 95 89 26 89 90 83 13 26 75 25 86 89 - 75 86 86 75 47 75, 45 86 75 75 16 89 45 74 86 90 74 95 75 25 56 86 75 33, 75 29 95 10 86 89 90 23 89 25 38 90 13 95 74 16 89 74 89 25 26 56 91, 86 75 95 45 10 26 89 90 45 10 19 75 29 74, 33 10 33 31 89 33 89 74 75 29 74 13 38 42 16 83 89 13 29 95 10 13 89 26 89 89, 75 86 86 75 47 75, 45 86 75 36 75 31 90 74 95 16 56 26 25 42 86 56 36 75 46 33 10 46 54 10 16, 25 75 31 89 16 10 33 75 90 83 54 56 25 74 95 31 89 74 54 16 10 36 10 31 10 90 23 89 46 89 16 10 26 74 25 16 56 59 25 90 89 16 38 59, 89 16 10 75 86 26 89 45 16 75 47 75 36 10 95 16 42 25 31 95 56 47 75 47 75 33 75 16 86 89 16 74 16 86 10. 10 90 21 86 75 90 95 74 54 42 86 74, 16 10 29 10 13 74, 51 89 26 89 90 25 90 75 74 56 31 75 90 75 26 38 25 86 90 89 74, 25 36 10 26 89 16 10 45 89 25 86 74 16 38 33 89 91 36 95 75 25 86 83 16 33 10 91 90 33 75 16 31 89 17 89 75 16 89 95 75 90 10 16 16 75 46 36 95 75 91 26 10 31 74, 36 95 89 16 89 54 10 26 89 31 56 23, 51 95 10 26 89 16 10 13 10 90 86 95 10 33 67 95 56 33 86 83, 31 51 74 54 89 29 89 67 23 86 74 33 25 83 90 86 95 89 36 10 26 38 17 10 86 75 26 19 89 16 75 46 - 89 75 33 16 10 86 10 33 56 59 86 16 75 25 90 74 86 89 26 89 25 38, 89 54 56 13 83 33 10 89 47 95 10 26 10, 89 67 56 86 29 75 26 36 75 86 74 26 74 90 89 13 75 95 56. 16 89 45 74 47 75 90 21 86 75 46 13 26 75 25 86 89 16 74 29 83 26 75 36 26 75 91 75 47 75, 16 10 75 29 75 95 75 86 - 86 10 33 75 46 16 10 25 86 95 75 46 33 10 33 95 10 13 89 36 95 89 31 10 74 86 29 75 74 90 75 47 75 33 56 95 10 51 10. 10 36 75 86 75 54 36 95 89 23 74 26 33 75 16 74 17 89 36 75 25 86 75 95 75 16 16 89 54 54 83 25 26 42 54 89 29 74 13 31 74 26 38 59. 54 75 95 25 33 75 46 13 54 74 46 16 10 33 75 16 74 17-86 75 36 75 31 10 26 13 16 10 33, 33 75 86 75 95 75 47 75 75 16 89 51 31 10 26 89 45 74 86 90 74 95 75 25 56 86 75 33, 89 21 86 75 29 83 26 75 25 26 75 90 16 75 54 74 31 16 83 46 95 74 90 29 75 74 90 75 46 86 95 56 29 83, 21 86 75 75 13 16 10 45 10 26 75, 45 86 75 16 10 45 10 26 10 25 38 95 10 29 75 86 83, 89 16 89 45 74 47 75 56 51 74 16 74 89 13 54 74 16 89 86 38, 16 74 75 25 86 10 16 75 90 89 86 38, 16 74 36 74 95 74 89 47 95 10 86 38.

16.

15 67 51 41 53 22 75 53 75 22 65 93 22 39 44 22 90 22 93 51 67, 44 22 86 49 39 51 44 58 67 22 67 67 49 86 94 93 51 62 94 67 44 49 67 22 14 90 22 75 51 44 51 75 49 26 78 94 67 72 39 . 94 39 44 22 90 22 22 86 22 93 22 44 51 90 22 44 49 75 22 27 88 53 22 78 72 11 49 93 22. 53 22 27 22 14 27 88 67, 53 22 15 39 22 67 75 30 67, 53 22 27 88 39 49 20 67, 86 49 35 44 88 67 90 22

93 22 11 22 14 94 94 27 88 67 11 22 15 11 22 30 15 94. 78 72 93 44 49 67 22 14 90 22 75 51 94 30 22 27 44 49 62 27 72. 35 67 22-67 22 88 39 51 44 30 78 72 93 49 44 51 15 53 22 86 22 14 44 49 15 22 11 51 15 67 58, 53 93 22 41 22 51 44 49 15 67 75 22 51 44 94 51. 49 35 67 22, - 27 88 39 49 20, - 27 49 14-86 49 30 53 22 86 49 39 44 20 15 67 88 86 44 88 94 44 49 35 44 88 62 94 67 58 15 44 49 35 49 93 49! 22 27 44 49 86 22 53 22 15 67 22 30 93-53 22 15 67 22 30 93 94 11 22 11 75 51 39 30 22 27 88 39 49 93 15 30 . 45-45! - 27 88 39 49 20, 15 86 49 62 88 67, 88 11 94 27 49 11 39 51 44 30 53 22 39 22 93 22 27 51 11 65 94 39, 15 22 15 51 27 94. - 11 22 67 94 27 51 67 39 22 93 22 27 22 14 27 88 75 49 86! 44 51 15 88 39 51 93 22 44, 11 94 27 44 22, 22 27 44 88 62 94 26 44 58 53 75 22 62 94 67 58 67 49 86, 86 49 86 44 49 27 22, 44 51 75 49 26 90 93 30 27 51 93 15 11 22 51 90 22 15 35 49 15 67 58 30 94 67 51 53 51 75 58 41 22 35 51 67 67 22 62 51 44 49 35 94 44 49 67 58 15 44 49 35 49 93 49.

17.

4667238040926940999540,95674667701431181410256755404627705887401077
389295678780671870148 7,25678027874010:6967469280584638581067695895,
95674667701431673858557739696718678055678767238210583946552746778758 551795704025926967 31.55676755256743401058108758551 7.804031-9540
4658255870771758236725674340105836926958705527588727876710678067 39 4677,384667181467555558954099101710,55588270678740109255588014 99 40 10 46 40 95 46 17 43 95 67. 69 67 46 39 95 40 95 92 87 92 82 67 70 67 99 92 87 92 87 14 39 10 17 87 92 25 67 80 67 99 58 10 95 39 46 40 70 92 95 27 18 10 40 23 67 70 67 80 55 14 31 92 69 40 99 95 40 92 25 70 17 87 67 67 18 50 17 39 55 92 10 58 87 27, 69 38 58 87 80 58 10 67. 39 46 40 70 92 95 39 27 70 67 69 67 25 67 18 10 40 23 67 80 40 70 92 10 92 69 40 99 95 27, 55 67 27 31 46 92 39 95 40 70 40 27 10 40 55 40 18 67 10 67 46 67 67 46 95 40 13 40 10 39 17, 25 67 46 67 87 27 38 46 67 18 14 10 92 58 62 58 55 40 39 69 58 46 58 46 40 95 92 58 10 36 80 92, 95 67 46 67 70 14 58, 67 38 58 55 77 25 70 67 39 46 67, 87 67 23 10 92 18 14 13 40 71 46 67 69 70 58 87 17 95 67 10 82 67 13 55 14 31 39 40 80 67 46 45 70 27 95 46 67 69 67 38 92 39 46 92 46 77. 92 39 46 40 70 92 95 25 70 92 95 40 13 40 10 92 69 40 99 95 58, 38 46 67 18 14 46 67 46 39 40 87 69 14 69 67 10 67 95 95 40 87 58 55 77 92 13 18 67 10 67 46 40 69 23 67 70 27. 40 67 55 25 67 46 67 87 25 70 92 80 58 46 46 27 80 40 55 58 55 40 80 67 10 23 67 92 38 58 87-55 92 18 27 80 77 39 95 67 70 58 55 77 95 67 25 67 95 40 87 55 36 39 46 27 95 55 58 46. 67 38 58 55 77 67 23 67 70 38 92 10 92 69 40 99 95 27 46 40 95 67 31 25 67 69 67 70 67 46 80 58 10 40. 55 67 70 40 39 39 58 70 80 92 46 77 39 46 40 70 92 95 40 67 46 95 40 13 67 87 67 55 55 58 70 58 99 92 10 39 17. 55

40 39 10 58 80 27 36 62 58 58 27 46 70 67, 13 40 82 69 40 46 92 69 95 70 58 25 95 92 31 87 58 99 67 95 92 82 67 10 62 67 69 14 58 70 27 95 40 69 92 24 14, 38 46 67 18 14 55 58 67 18 43 58 38 77 67 95 40 87 58 55 77 70 27 95 92, 67 46 25 70 40 69 92 10 39 17 92 69 40 99 95 40 55 40 18 67 10 67 46 67.

18.

67 58 26 19 88 23 32 37 15 23 90 63 71 46 63 26-63 26 58 24 63 23 37 32 95 67 63 15 32 88 58 26 - 67 26 58 67 41 16 24 90 63 52 30 24 49 63 26 88 26 37 23 38 23 16 67 58 23 90 26 41 90 63 68 24 58 58 26 76 85 15 67 76 24 15 24. 19 26 15 23 38 88 26 63 15 32 88 58 24 24 90 88 24 16 23 63 71 63 23 37, 46 63 26 41 54 37 15 23 95 67 67 58 24 38 23 76 24 63 67 16 67 68 26 68 90 24, 67 58 23 46 24 37 63 26-63 26 58 24 19 16 32 85 54 44 26 46 24 58 71 41 54 90 63 15 26 90 88 24 16 23 24 63 90 26 26 63 68 24 63 90 63 68 32 11 30 67 24 68 54 68 26 88 54 67 24 30 24, 46 24 19 26 88 26 41 15 26 19 26, 85 15 67 76 24 63 90 52 37 16 24 68 24 63 23 63 71, 68 15 23 95 67 58 23 67 88 24 26 16 26 19 67 46 24 90 37 23 52, 85 32 90 63 71 88 23 95 24 32 58 24 19 26 67 58 24 41 32 88 24 63 88 26 37 23 38 23 63 24 16 71 90 63 68, 58 26 37 46 24 76 32 58 23 76 16 67 83 58 52 52 37 16 24 68 24 63 23. 63 26-63 26. 49 63 26 63 56 67 58 23 16 85 26 38 68 26 16 52 16 26 88 58 67 76 76 23 73 26 76 15 24 83 67 63 71 58 24 90 37 26 16 71 37 26 38 23 88 23 46. 58 24 41 54 16 26 58 67 37 23 37 26 44 37 15 23 95 67, 90 26 68 24 15 83 24 58 58 26 44 73 68 23 63 37 67 76 67 63 15 24 58 67 15 26 68 23 58 58 54 76 67 15 24 41 52 63 23 76 67 - 85 15 26 90 63 26-58 23 85 15 26 90 63 26 26 37 15 24 90 63 58 54 24 85 23 15 63 67 38 23 58 54, 88 23 68 58 54 76-88 23 68 58 26 19 15 26 38 67 68 83 67 24 88 26 41 15 23 63 71 90 52 68 90 24 95 24 88 26 26 85 16 26 63 23 67 76 85 24 15 67 23 16 67 38 76 23, 90 67 15 24 46 71 88 23 58 58 26 44 41 23 38 54, 90 68 26 11 32 19 15 26 38 32 68 37 26 58 29 24 37 26 58 29 26 68 68 54 85 26 16 58 67 16 67. 58 23 19 15 52 58 32 16 67 58 26 46 58 26 44 85 26 15 26 44, 85 26 15 24 38 23 16 67 37 26 16 11 46 37 32, 85 15 26 58 67 37 16 67 58 23 41 23 38 32 85 26 88 85 26 37 15 26 68 26 76 76 15 23 37 23, 38 23 16 26 95 67 16 67 90 85 26 16 88 11 95 67 58 54 76 67 58, 85 26 90 63 15 24 16 52 16 67 67 38 19 15 23 58 23 63 26 76 24 63 26 68 67, 90 85 15 23 68 24 88 16 67 68 26 15 24 83 67 68, 46 63 26 88 26 90 63 23 63 26 46 58 26 58 23 85 23 37 26 90 63 67 16 67, 38 16 26 15 23 88 58 26 85 26 16 11 41 26 68 23 16 67 90 71 88 24 16 26 76 15 32 37 90 68 26 67 73 67 32 41 15 23 16 67 90 71 68 26 90 68 26 52 90 67 41 24 38 76 23 16 24 44 83 24 19 26 88 16 52 90 24 41 52 32 15 26 58 23.

19.

969030967167715585718530161896903771558520-
606216529216625516246219 96 90301471867155 85 20 52 85 25 24 71 92 71 94,391696148596584586857385301618969037715585

71,62167124621925169285227124623416528525247192719455903090499055551614166296713025711655168530147196207162242034621622259073559045945941485309049907162242052968524163049905585858530161896903771558520341196903985227124251614967149902562169671859285245216141686194525925905571969071558571969030967167715585208530161896903771558520739690558562242034399094927185301618969037715585208555719690309689345516243420309055162471111639853085227124258514969030147196161439853085227124258594969030147196853016189690377155852016528524893490716239853085227124258571119018909685628985 30 16 18 96 90 37 71 55 85 20,6216712462197111634892416625885678596855558.39853085227124258594969030147196141637716285301471962062192420259025345285252471922073,629025853471498555854690734992855589:14 85 92 92 85 14 71 62 96 90 73,2490556285147162969073,494594149073.16553090499071622420529685241630499055858585301618969037715585208573969055856224203414712462712439909492161455524629690468585559060259690557162167111166785968555588534892416625830904990456234528525247192207373,22621618893055906219,259025584522902462196025969055901655163090558514907162.71249285853016189690377155857111166216342062499220497114165524629690468585559060259690557162167111166785968555588534892416625830904990456234528525247192207373,22621618893055906219,259025584522902462196025969055901655163090558514907162.712492858530161896903771558571111662163420624992205271229062854992205271229062854699220527122906285,621671111696903014719630904990456234714985558546907349928555892262161889305590621925902558452290246219928524629073499285558922621618893055906219,259025584522902462199285246290185814901185165516309094147162.

20.

58 47 74 66 91 45 85 28 91 11 33 29 74 28 91 11 12 11 68 66 43 31 23 29 11 85 55. 58 29 74 96 74 50 61 58 16 74 16 85 47 88 11 91 23 33 31 74 96 74 79 28 11 33 47 28 11 88 35 55. 58 45 23 16 66 43 55 11 47 28 29 74 12 61 31 85 96 85 29 43 91 91 23 49 16 66 85 55 85 91 61 47 74 31 29 74 96 11 91 11 35 66 58 45 35 58 47 35 66 58 45 23 91 11 31 29 74 96 53 33 23 68 11 21 55. 11 91 11 33 47 74 29 47 85 33 91 85 29 85 47 85 66 74 . - 88 55 74 79! - 68 74 29 74 96 21 43 47 29 85 55 66 11 91 85. - 47 28 96 23 53 58 91

11 47 47 55 74 50 74 49 29 88 85 96 11 47 74 68 91 11 66 58 . 50 11 91 28 35 58 12 - 16 74 31 28 85 96 74 47 58 91 11 35 91 11 47 91 85 31 11 29 91 74 74 55 91 43 66 58. 12 11 28 11 28 35 21 - 55 74 68 74 66 35 50 35 21 88 11 53 28 35 91 11 16 96 11 47 91 74 29 23 96 35 68 11 66 58. 96 11 12 29 85 79 85 38 55 74 26 74 96 74 53 11 43 79 58 12 91 61 . - 28 74 91 85 88 91 74, - 68 74 29 74 96 58 55 47 29 85 55 66 11 91 11, - 79 58 12 91 61 47 74 29 47 85 33 16 66 74 26 11 43 . - 11 31 11 29 11 49-28 11, 47 29 85 55 66 11 91 11, 91 11 31 85 91 61 55 23 47 29 74 85 96 74 12 74 29 74 85 16 66 11 55 61 85. 29 74 12 61 33 85 33 33 23 58 12-12 11 16 85 88 28 58 33 74 21 16 74 26 74 31 91 35 21 47 35 33 28 35, 16 74 66 74 79 58 33 55 35 31 11 55 29 74 85 43 50 66 74 28 74, 33 74 49 55 11 50 11 28, 47 16 58 88 28 58, 91 74 79, 50 35 66 28 35 58 35 49 31 85 33 58 12 38 55 74 68 74 31 74 33 11 28 35 31 11 68 66 11 12 11 68 66 43 31 43 55.

21.

29 37 11 90 28 40 20 58, 65 58 75 75 35 11 40 28 29 11 61 54 35, 65 58 75 28 40 11 77 75 52 75 61 20 15 84 54 46 75 52 54 58 37 80 15 75 65 58 54 58 84 54 65 11 58 29 11 84 58 54 15 75 29 11 84 46 28 75 37 58 54 90 11 13 28 75 77 75 72 40 84 40. 33 75 61 11 11 15 75 61 75 29 54 28 49 33 54 75 61 75 77 54 65 11 37 35 75 41 15 54 84 40 13 54 52 49, 35 75 58 75 84 18 20 29 11 28 65 40 11 58 65 11 61 75 29 11 35, 37 75 37 58 40 29 61 80 20 58 13 75 84 37 35 54 11 75 84 77 40 28 54 90 13 49. 11 37 61 54 75 28 54 15 75 77 54 33 28 18 58, 15 54 84 40 13 54 52 40 75 33 84 18 72 54 58 37 80, 54 37 65 11 90 28 11 58 75 37 28 75 29 40 29 37 80 35 75 41 82 54 90 28 54 28 40 37 18 72 11 54 29 29 75 90 52 18 46 11. 29 37 11 13 49 90 28 40 11 13, 65 58 75 65 11 61 75 29 11 35 65 11 84 15 40 11 58 28 11 13 40 61 18 20 65 40 37 58 67 37 29 75 11 41 15 54 23 54 28 11 15 75 37 84 11 52 37 58 29 11 28 28 75 54 90 75 35 11 40 28 40. 13 75 82 11 58 33 49 58 67, 35 40 35 75 11-58 75 29 84 11 13 80 13 49 11 23 11 15 84 75 52 11 84 82 54 13 37 80 33 11 90 52 75 37 58 40 58 75 65 28 75 77 75 35 75 61 54 65 11 37 58 29 40 15 54 23 54. 28 75 33 11 90 29 75 90 52 18 46 40 13 49 28 11 13 75 82 11 13 82 54 58 67. 75 58 77 75 61 75 52 40 18 13 54 84 40 20 58 65 11 84 11 90 28 11 52 11 61 20 - 52 29 11, 75 58 82 40 82 52 49 - 65 11 84 11 90 52 11 28 67 - 52 84 18 77 75 41, 33 11 90 29 75 90 52 18 46 40 65 11 61 75 29 11 35 90 40 52 49 46 40 11 58 37 80 29 28 11 37 35 75 61 67 35 75 37 11 35 18 28 52. 11 37 61 54 13 49 15 75 77 18 33 54 13 13 75 84 37 35 75 41 15 61 40 28 35 58 75 28, 90 40 15 40 37 49 52 75 37 58 18 15 28 75 77 75 82 54 29 75 58 28 49 13 54 65 11 61 75 29 11 35 18 35 54 37 61 75 84 75 52 40 37 75 35 84 40 58 80 58 37 80 33 75 61 67 72 11 65 11 13 28 40 15 75 61 75 29 54 28 18. 75 15 40 37 28 75 37 58 67 18 37 18 77 18 33 61 80 11 58 37 80 58 11 13, 65 58 75 15 61 75 23 40 52 67 61 11 37 75 29 54 90 11 61 11 28 49 46 18 77 75 52 54 41 33 49 37 58 84 75 37 75 35 84 40 23 40 11 58 37 80. 58 40 13, 77 52 11 15 84 11 82 52 11 33 49 61 40 15 61 75 52 75 84 75 52 28 40 80 15 75 65 29 40, 58 11

15 11 84 67 15 84 75 37 58 54 84 40 11 58 37 80 40 37 92 40 61 67 58, 33 11 58 75 28, 15 11 37 65 40 28 49 11 52 20 28 49.

22.

56 96 31 57 87 37 56 75 84 77 87 24 96 73 68 75, 56 75 50 37 16 42 68 77, 77 20 73 37 37 49 56 77 39 77 87 37, 39 73 37 12 84 96 16 91 64 56 91 87 37. 75 56 84 73 16 91 68 94 75 75 31 57 87 75 44 16 37 84 73 57 75 56 96 49 77 73 96 14 87 75 12 57: 96 84 87 75 56 77 44 37 28 37 68 37 56 56 75 68 96 56 96 73 56 75 50 37 16 42 68 77, 56 75 84 77 87 24 96 73 68 75, 96 84 87 75 73 77 26 73 37 87 41 68 37 84 77 87 24 96 73 68 77 31 96 49 50 37 16 42 68 77 75 87 75 50 37 16 42 37 68 31 96 49 84 77 87 24 96 73 68 75 - 56 96 73 37 39 73 37 56 96 12 64 37 28 75 73 41, 56 37 28 77 35 96 56 96 44 16 75 31 87 75 35 77 73 41 84 61. 12 84 96 44 16 96 35 56 75 96 16 77 84 68 87 77 28 57 87 96 73 61 73 68 39 96 16 73 91, 12 35 75 49 56 41 84 87 96 28 91 96 73 56 96 26 96 28 87 96 56 56 37 44 16 96 73 12 37 16 61 73 41 49 77 44 77 84 56 37 14 12 77 16 75 77 56 73. 56 91 35 56 37 68 77 68 26 37 35 56 37 31 57 84 73 16 96 96 37 73 84 82 28 77 84 26 77 73 57 12 77 73 41 84 61, 91 31 75 16 77 73 41 84 61 68 39 96 16 73 37 12 37 14 26 77 73 96 16 75 75 49 50 37 16 37 28 68 77, 12 84 73 91 44 77 96 73 12 84 75 87 91 49 77 44 77 84 56 37 14 12 77 16 75 77 56 73 37 73 64 37 28 77. 12 96 84 41 37 68 16 91 35 77 82 22 75 14 26 75 16 12 56 96 49 77 44 56 37 84 73 77 87 56 96 44 16 37 84 73 37 39 91 35 75 26 - 12 16 77 35 28 96 31 56 57 26. 44 37 28 37 49 16 96 12 77 73 41 84 87 96 28 37 12 77 87 37 12 84 96 64 75 12 84 61. 44 41 82 22 75 64 44 75 12 37 84 37 87 28 77 73 75 68 37 12 - 12 73 37 26, 39 73 37 37 56 75 56 96 84 37 87 28 77 73 75 68 75 12 37 12 84 96, 77 50 16 91 44 44 77 49 77 64 12 77 73 77 75 49 12 37 96 56 56 37 14 68 37 56 73 16 16 77 49 12 96 28 68 75, 44 16 96 84 73 77 16 96 87 37 50 37 50 37 84 73 75 56 75 39 56 37 50 37 64 26 57 16 61 - 12 73 37 26, 39 73 37 37 56 12 37 12 84 96 56 96 44 37 16 73 41 96 75 87 75 12 87 77 28 96 87 96 94, 75 87 75 73 37 75 28 16 91 50 37 96 12 37 28 56 37 26 87 75 94 96, 77 44 37 87 68 37 12 56 75 68 49 28 96 42 56 96 14 73 77 14 56 37 14 44 37 87 75 94 75 75. 12 84 96 12 37 49 26 37 35 56 37, 68 37 50 28 77 91 84 87 37 12 87 96 56 56 37 50 37 84 75 50 56 77 87 77 56 96 73 56 77 91 84 87 37 12 87 96 56 56 37 26 26 96 84 73 96.

23.

17 31 10 28 39 25 97 69 66 51 66 49 25 - 39 10 39-47 64 39 10 39 88 24 58 66 24 72 24 47 24 85 10 39 66 47 22 64 88 66 75 35, 58 10 39 64 42 66 22 24 58 75 79 64 75 39 25 69 10 58 35 75 79 17 28 24 39 24 64 88 64 17 66 85 24 28 24, 64 88 64, 58 66 51 66 88 25 22 44 24, 66 58 69 28 10 17 64 58 35 75 79 39 74 66 28 97. 24 75 88 64 17 66 49 66 24 74 10 69 66 49 28 25 39 66 15 47 24 58, 74 66 31 47 66 69 66 69 28 66 75 58 25 69 28 64 47 79 58 35 69 28 66 42 88 10 49 47 25 97 17 10 47 47 25. 17 66 49 47 62 24 69 28 66

53 24 49 25 28 62 69 66 28 66 15 49 66 28 66 51 66 66 80 42 66 49 79 58 75 79 74 66 80 64 88 35 47 62 74 58 24 88 24 12 66 47 10 74. 75 58 66 64 58 17 88 10 51 24 69 66 69 10 75 58 35 69 66 49 39 66 28 69 25 75 - 64 69 64 44 64 69 28 66 69 10 88 66. 49 88 79 37 58 66 51 66 17 66 17 75 24 47 24 47 25 31 47 66 47 62 28 79 58 35 75 74 66 80 64 88 35 47 62 74 58 24 88 24 12 66 47 66 74 17 69 25 22 64 47 62 51 66 88 25 80 62 24. 49 66 75 58 10 58 66 22 47 66 75 88 25 22 10 15 47 66 69 28 66 88 64 58 35 74 64 47 24 28 10 88 39 64 64 88 64 25 28 66 47 64 58 35 24 51 66 17 47 10 80 24 51 10 97 72 25 97 47 10 80 24 28 24 51 17 66 88 47 25. 75 69 66 75 66 80 66 17 25 58 66 69 64 58 35 74 66 80 64 88 35 47 62 15 47 24 74 10 88 66, 10 17 62 42 66 49 66 49 64 47 - 66 80 85 10 17 24 75 58 64 75 35 17 66 49 66 47 24 69 28 66 47 64 53 10 24 74 66 15 85 10 72 64 58 66 15, 80 88 10 51 66 69 28 66 64 85 17 66 49 64 58 24 88 64 28 24 51 25 88 79 28 47 66 75 66 85 49 10 97 58 88 97 80 66 69 62 58 47 62 24 28 10 85 28 10 80 66 58 39 64. 17 66 49 66 47 24 69 28 66 47 64 53 10 24 74 62 74 74 66 31 24 58 80 62 58 35 47 24 58 66 88 35 39 66 74 66 80 64 88 35 47 66 24 25 75 58 28 66 15 75 58 17 66, 47 66 64 22 24 42 66 88 49 88 79 47 24 51 66.

24.

97 16 36 26 11 45 75 19 14 26 41, 47 95 16 30 95 16 14 86 95 11 93 71 95 97 54 95 29 95 54 95, 29 95 29 21 86 36 52 83 75 95 54 36 24 95 26 86 36, 97 36 86 36 47 45 24 86 36 97 16 36 26 11 45 54 95 26 41 26 97 16 93 49 24 45 75 26 86 75 14 93 47, 24 86 36 26 93 30 36 49 11 61 11 95 29 36 11 93 56 24 86 36-86 36 97 16 36 14 71 36 89 49 93 86. 36 37 45 86 14 75 21 86 36 97 16 93 49 24 45 75 26 86 75 14 93, 36 11 95 26 86 95 54 95 93 30 36 97 36 49 36 30 16 93 75 95 86 41 14 16 95 26 86 14 86 41 75 26 75 36 93 89 49 45 19 93, 36 97 95 26 95 61 26 41, 24 86 36 52 83 36 11 36 93 93 11 93 97 36 29 14 11 45 54 36. - 61 75 93 16 45 98! - 19 93 97 86 95 54 95 47 95 16 30 95 16 14 86 95 86 36 16 33 93 26 86 75 93 11 11 36, - 61 75 93 16 45 98! 24 86 36-86 36 97 16 36 14 71 36 89 49 93 86! 11 93 47 36 33 93 86 11 93 97 16 36 14 71 36 89 86 14, 97 36 86 36 47 45 24 86 36 71 95 24 86 36 33 93, 75 26 95 47 36 47 49 93 54 93, 47 11 93 97 36 26 54 95 11 95 97 36 33 14 71 11 93 11 11 95 61 47 45 29 95. 26 36 71 11 95 98 26 41 75 86 36 47, 24 86 36 61 54 30 95 54 95 14 36 52 47 95 11 83 75 95 54 95 14 33 14 54 95 86 95 89 11 36 89 33 14 71 11 41 98, 26 29 16 83 86 36 89 36 86 54 98 49 93 89, 11 36 75 26 93 33 93 11 93 54 41 71 61 71 95 21 86 36 11 95 29 95 71 83 75 95 86 41 86 95 29 33 93 26 86 36 29 36. 24 86 36-86 36 26 54 45 24 14 86 26 61 11 93 97 16 93 47 93 11 11 36, 97 36 86 36 47 45 24 86 36 11 93 52 83 75 95 93 86 86 95 29, 24 86 36 52 83 24 86 36-11 14 52 45 49 41 86 61 11 45 54 36 26 41 75 93 24 11 36. 95 29 16 36 47 93 86 36 30 36, 26 36 11 47 36 89 52 83 54 75 93 37 14 89, 71 95 21 86 36 61 16 45 24 95 98 26 41.

25.

17 40 76 37 82 42 78 75 33 17 16 16 50 16 17 51 13 64 33 72 82 72 82 84 40 94 82 28 94 42 13 33 17 17 58 50 17 82 51 42 28 51 25 82 50 82 28 69 40 13 33 46 94 78 17 33 42 82 46 34 25 82 13 40 64 76 82 25 82 37 17 58 91 94 46 51 72 40, 17 82 16 50 17 82 72 16 33 33 72 82 84 37 51 69 34 78, 25 82 46 46 33 72 16 16 84 33 13 51 64 25 40. 16 13 25 40 75 84 82 50 94 46 51 38 40 33 76 82 25 51 76 25 33 50 82 28 16 46 34 17 82 72 82 25 82 50 76 34 61 42 33 37 40 76 37 33 84 64 33 94 42 13 82 13 40 46 82 84 82 46 72 82 33 82 28 94 51 75 84 33 17 16 33 13 82 76 37 82 94 40: 38 42 82 75 33 16 50 33 17 17 82 76 82 25 51 76 40 42 34. 25 40 25-17 16 25 40 25, 17 82 51 42 28 51 25 - 13 33 19 34 17 33 84 33 64 33 13 40 78, 16 94 84 33 46 40 42 34 17 33 51 84 40 38 17 51 61 76 82 25 51 76 25 51 17 33 88 82 42 33 46 82 94 34 28 58 17 16 25 82 50 51. 69 40 42 82 82 76 37 33 84 33 46 16 46 94 78 17 40 28 82 37 25 37 16 42 33 37 16 33 13, 94 25 82 42 82 37 58 50 16 76 82 46 34 69 82 13 40 42 33 46 16 76 82 84 88 82 84 78 42 25 13 58 28 82 37 51 17 82 51 42 28 51 25 40. 76 82 94 46 33 84 17 16 33 76 40 37 51-42 37 82 91 25 51 46 33 42 17 82 51 42 28 51 25 16 76 40 84 40 46 16 13 55 33 17 33 94 42 82 46 34 28 58 94 42 37 82, 38 42 82 28 51 25 13 40 46 34 17 82 17 40 72 46 40 69 40 88 76 37 33 13 37 40 42 16 46 16 94 34 16 69 40 42 37 16 28 51 42 40 28 16 69 17 33 94-10 46 16 42 58 13 37 40 28 82 38 16 91 16 17 94 42 37 51 50 33 17 42 13 94 33 88 76 37 82 21 33 94 94 16 82 17 40 46 82 13, 55 33 17 78 19 16 88 50 82 28 16 46 34 17 82 94 42 34. 28 82 46 33 33 42 82 72 82, 16 13 82 21 16 94 40 88, 16 84 82 50 40 17 82 51 42 28 51 25 16 13 94 33 38 40 19 33 76 37 16 88 82 84 78 42 17 40 94 50 33 17 51 84 33 94 25 42 82 76 40 50. 94 21 82 37 50 16 37 82 13 40 46 94 78 84 40 75 33 82 42 84 33 46 34 17 58 91 25 46 40 94 94 17 82 51 42 28 51 25 82 13 - 69 40 50 33 17 40 17 40 94 42 82 46 34 17 82 72 82 76 25.

Приложение2.*Варианты заданий практической работы№ 5.Криптоанализ многоалфавитного шифра (шифраВиженера)*

1.

ючсобдтощужнсхжръкжнхдтцшаоьтдйхмьжщызждтцлцбдшапцурмеаянсьчмйсуптйчмнаянсьчмцйщитьчмцуюнъаяяхбвмтжртйпъыипнпх_тмрйнччпыхжфтидйхмфтцбумьругношеуя-

дю_ыдпяьесцпеуймнармпбдтцуртдппекрюхмооътпсыдхоччбнюнжнсумфъуаындгятдгют-

сжындф_пкстхчэньуещхтоьючэнхдеьючпцъцурыдуохтт_пкоыыипн_лбяъудьмфпртцурызбыхгашнпащхчжюнчфюъукнаусъздрюычйрмтжсыдооьхбршкоимзтумцуютрьнщеууэнбщхцуцгктшыоаяыщйяянлцмпп_ыхбммыжэшгж_югахндппзьоитдшапцурндйнптжеънж-

нлзмуън_нхдуочдтшнмб_идрютцоьруацскбщхмномпп_ыхьчмфсьякт__кунъхп_хзакючж_хьжячудьмсп_хзбнхдрюхмьрнкунчдтьфйбыхватхйбшяншую

ппчмрй_тхб__хьнгчппздрьст__идшцяеуушгатыдуютжфущудьмшсьпт_нюе
ньсугьшаоьруаььчйъхмномуеынппнъктъычсммтйнъеадяуа_нноязжыъужн
ьугуючгьпеоцтдгиунгошуаюнмгцпемьюаацмйппхзбщыцэнфенугеуушаоиб
дсуфшмйяеуьпдпяъугоътпумтбнщшеюысацмфсьючпъмфсцъыйэтдньукуно
_уймнаытдфыхзжююемйъуннъуафхзпъмнартьоьщдещлдгятъашяуаьорбтнк
ун-
сут_нчпдъукнгшгяязй_трэыыцуйкдфньхйхэешыыипн_лбяндлочдрюнзйщы
доуо-
умйде_нншецяусцлдрьюппщипфныта_экватчаьядшцяеуушгарьумытдпээке
ушкоыыоаяьутьотпяянашмщбыяеицлсацмуууяхбыттйлмууныжьдъукнуниы
хдтюнзоцякмйъуаытсоьрнж-
нпдеьючб_ыьоьцдт_тфжыхдтрыжптъ_аьядгщнцуцмфпрюкеытзоьючйнхдтэ
ыцппъ_аьязжднчэнъеаяяшлнхмгытдрьйчпъ_дгш_цапырэехтт_пеармфжюп
шя-
ныьжютйэн_йпршкурых_лядсоюцлоф_аьмжбынрэызъад_зт_пецнхдтьо_уц
лъацшнаьмтжхнсьяшу-
гоя_цнычлщытжыхгцнпдю_хъад_зт_пецнхдтьо_уцлъацмбуьмфсопнмйъуа
ынзжюъужньутшы-
рэш_двоъемйъут_хдтьючбршгя_мжпщиэфлмьбяяадтрпртьжячудьмурияеа
д_зт_пнуушаоитдмлснарюкдтндвишнацмжфт_чаямтбъхдоьмноьрйбнюрфд
нкуялдйняелнгчпнъ-
кпфхйбыъ_кньхйяяшрншввьь_уяязбнюсфжнкунхдтощшянъкеьпксдхзфлми
пщызф-
ньую_ысфнънлоче_нэечцытбщхмбгхгаыхпбшнгаютщпющеаыхпбшыоабэк
ктхцуячнкннтбщхмаытдгню-
ут_ыгоцхдрьштпяяаян_тйдяузцяаа_экруядгьфтйшнвъццдгьмзсущгаптцжтм
шашнсйындйщхдгншктыыоаднюжнпкеймхждидйттчаьмфтцбумьрнйнхрйн
яхбтхыйцмчбшмлжнэкбщитп-
нхддщ_жпшыдфшыхжыхзщуцц_нпдшушугугктшысаяымооънйнчелншвво
лдею_ибммчсоснчцлдпнюзжюючоцвкаютрйсхуиыыипнгшгяязбняктыыдтр
лмбыъукнюуаъъудцщнауруаоюфжшяенцмнахнтйънвъуцдтщхэльщдныыип
нщкт_ндгнъещущдгы_чсуътжъмжйьшудцгктшысаынцмуснйнгчппздрьякс
мяаарюкньршъакдгщнцуймтбтмушуъаарнлоищдцьягацмьйяшкоыыдоупкм
цчнннщкойдноязпъмтбъмфптыжоиб

2.

фщнуызцнхюяящычвимщнггрюврнрдтььпцшнряаяющщюыуоълнтфьмя_пц
_ыэнъсныыю_чокйакрьоб_нюьпыамуэыьытрььаусцщтюызцнггрюврнрьюю
ьпсыълумюомгтыуьшмяяуцхрцмтьшщнэся-
яг_муьчааррбтюьщцыыуньацгщызрцмбщтхяяуцлршывьэлвмяым_ъъщънц_
мвьрхомыоч-
ррыыю_фняцвмыьяяюзцныюнъцньяыхэотвнпрюнюыхцнпаущцынррюцщт
юынпнчщетьомщъхрэыпршпщхбймцяяцяяууъюьмуялыцтрэтаяыюцащшнж

цхрд_хуююитрцъвуэ_ютвовщцмяж_йуъщммгфнбомщнювюнеомыьяяюзцн
яящиыьмщнщясшяньацсгънвймзушяртзуюыьтряыяпецяяуьмбнъцъъясхэцм
щньаьювищщнххулэцмщныфюнюцгцыълъмяэзвьщрп_хагщнъцээцтюыофг
ущлъмюупцтыэьтряясщыртшпнъсехень-
ацщщ_хуызеньаусыьпраусяълъмщнпбущяс_йцщрцювьгюцчяъмаосяяяцчм
щноцтюврхънъсязьотэиб-
рынрдтььпцдтб_пянясчълъхрцмуытшущюищщнющщнэцмядтуцсюьм_юхю
осьуусжхэцмынюдуэсъмбаецяяуьпсыхпныршывьэлвмюощрыхзурянъццфу
уювыырцмын-
чя_ыаищръзрытрээщынхщтчцщрбтюьщцымфютшнююомвьуцню_ьюяпюв
рыуошрбыаъхаьпсыхонь-
аусб_нущтюцлрьмюуэцошмыыэнхьцм_юхшюнзыыэнщщютррмжушяъмуят
раюььпщммхцчячмюцфиуцрфхшыхрээ-
яп_чтньцмунгцщыуучцныйаецыхцнюууэезтб_тб_пцыъясырцмюумбщтхатв
н_хцпьмямялр_ыэамыочрьююьпс_тьйъянъсяшцтювртюынпньсълвйм_юы_
цясынрютьцрщуцрцмбатууэщмщщнйвьмпршцыхцнчсшмбощлчмяпзыыыу
уъюицрынгдълчмдочвнсящуюьмунюгжъяяящнэсяюэояацпс_ибммунчсдтб
_пцньяяяямъюьрянхтьмваярхнхуцб_пярнюимщньятюяхъсыхцнхрцъб_хюш
ялнхрвывмм-
тую_ютаипюьтрээя_хуьювьлюцтроэцошгнъцртхьщясырынбдхвипсуярауцн
ялялзцмьуярпыьйдсммзоювймуытиытфьмыьюэьюснпбумцжтрмпьмтвялры
тщяюпшнцъ-
зэнхб_ызыхыьщр_нщыювртюыыфьмхомщньцютиусицтршмюощрршсяяю
итрынбщтхяяууъюитроюбьвщовщцмюумяяясршплярптшнпюцщсыхпнытзт
ы_зрцмпршцыхпнчя_ыаитршыфтнвьмтишщнюядяцызр_нщыювртюызэцм_
аювймхоуцняцэтаймэимэьуцъмэыыфьтрьокмююцямноящтцняясыря_йуюв
р_ц_мяпжцшящръсммдцфщьшясхзуюыолрбхыянжцлртнуыхенхюяящычвь
пррмюуэуыыъньацэяттрдтььпцшнршывь-
эсмм_юххотвнхэньяюншцяцщиюакрэыхрхчыыб_ирэ_б_иртнчумбьфюоъщ
ум_ьшюьювйкрьяацвсуярд_хуюснясшмыочръзрэыэыхэноящирцмгсэях_ря
щцюящншгддцнъцфтьцмгтыуьшмяяуцлрцмвочршнынъсехрд_уяяуомуныв
ыыиуъщцмтщнфььацлвызеннбэ-
ты_ыунъцртхьщясырямбощясырынзошснолщхррфп_зррм_щтюнхряыя_пц
_ювр_ожхэнытюншьщррыбэхвоълнэцщхфцышызэцмацягошсъхр_ыр_тэыы
ънхрхшячмзоювцмыьюэцгцячячмвоцюимуиьсщырынртыьлмдцргюхаьпс_и
ррмюодцъмдьшмшшяютрьмбртавжцяяцяяууъюьщркясняцысцывщммцяяця
яууъюищрьоаофяъмтишсньятсцюусынрцмвущрдяянъцютицяцщиюьювйм
щны_оююьювймуятфтнр_тбыыряппхнюимэуухамбьоячмщхфснгцсырытуу
сяъзънщщюмюухшптчыырээцтювотвнчсшмэцэрсэяхлйццрдтььпцш_рхшяъ
мыьрхомчумынювюне-
ам_юхтопщщыбймюухшптчыыцнызоэярнюцтрасщршцыхпнхрщктььл_ювр
нрэыпрхььюмнъцдяянюььуцыъяумщхмя-
пыб_эцыъясырд_уяяуомщнпяхогфсцыъячмдоъвофщцмзйлрфхшытбэыбьо

юьювймаопюомчцфю-
ую_ьюяпъяяящнгцщыуугцяяуомхуящнпбурхомтасг_мтьлвйюпняцъъя_зро
мухэяяшлум-
запб_пщ_тьйълумын_юоюьусярнюыыэамяэзвамтасг_мвют_уяс_ирээщнщл
яшщнырытуусяъзенхрптшътаызеньаьювюнюяяуобрссц_ыртньучянфснфуу
фхощщнюррышъычыы-
рэ_ьйющю_ожтънущхъмлмюум_ьбяфтънъснфцъъглмщщхраусянвйюпньац
мэиюьцмя-
нуг_чщвмэцэсвмюомюодцчмбьоб_пцыъячм_щнюуяцнчя_ыаитрцфууювыз
р_ыьйчянщцюяуищрцмбащсядцтдщъ

3.
зчяэдвуфрцнврхсэшаедгсеблдюрдбцкхюквкцэрэщневждбкзюрэюрд_щъясн
эк-
тякцръцщ_уьщищбкбхуъкчябпщкмартщйдбщзцыэцштякйаюищчдвуфячдб
крщэкалчгыуъкпяэуалгръхямшчпецэ-
дям_ышууртюеоряншуьцьпщфдбэхс_дщкмцчтяфдгсебкнрюдыщчяыуъкжц
тшбцуушуррцвждбнуцксцьчякчябтякчсхдчрдылпрщтяккбэарюдвыехуыщщ
тющорурщкйсскршквыехуыщщтющорурщквэщхщьчщбкбхуъкрщэкалчгы_
рщд_ынууйцшнп_дфпкрлзвщхрщцям_экфаукэщсрурщкмсоуущхйуыыусръ
ухчнфузсшнцчдщтсцшг-
цэдбч_бцдпнтяфд_лчяцуфунрщйюлпякбвщдюрдщчкцэдяэтявкюугрхдьучц
ыевюхцкпяьсщбкбхуфщдгсеблдуккцкнбэнюшуэкмюльцшнщкзршебэупгкъ
кнбэуа-
унрщдбнка_яцьчцьчуртющсррцвждюрьвщдтщрмвкцкьцчдвлоющкрюжщф
цвнурщпащзснрцштлрдыщцвудщцнръхяьчлшгрьдфыкэйющчнрак_йсщкзр
шкъкйяцлюлдтечмкуйючщчепкевчубя-
калдтрц_ыкхррмшуфщдщктцщжкйцюусяоурюлсьеръкарйрнтцвтщчнрудюр
зцпуэесщкцщцеэу-
дуктцфдхщрчртрм_вждюлсцхдуецылмсштлфдуькажкшкпсхдщкфаурщбкбэ
згрчръхцпсцэшршерьеэюврюлсьтгидэецьждзррянкылдякцвыеишуъкнрыкс
цающоръ-
хщщцвлтянпцкньуд_щрющорщцвлтянпцкйцфцвннпкчц_дюрфаррястл_дш
лпяшуукфау-
хяп_рхувщхлрдпнрпичбйдюлэцфдцпнюьчуртющортейучяфд_ыувузр_еяье
рудхрсяшуукмсъхцпкьжтяоуръхяьчалтбэзскпяшкзшуршкьжмпкучуйсэарбч
якзбрд_щзцьчущзсшнпкурьзцыъкрцврцвнкюшуэкжгпшвкчябтякцьрйяневж
дылпяфчякухшуъкчцщхцэнзрцыщорчухррщкчущхзрцыукрцвхудям_зшурш
кгыеушуурэцштлрдщкзрцшзвнекфащншнкхртщйъррцвждбхшзш_цксцьчск
жяцкцкчяоурьеэекртеэрьсэкьжтлрдал-
жяэ_рщдбнка_яцьчцьчуртющсрыетщчлкуръухьушшевррмшуэкпяэуащкръх
яйзьйквьгрндуррщхуьрфюеърях-
сосцшчс_дюрпяриякфащншнкхртщйдбщцарйяэузртющиякзятсястяктскйяь

чщскюунрьуурхиртющдхышфщиякхцтшьжчсэернечшкцкзбриякевчубякал
дщмурхуюрьюеорххщэкауорпубэуурхющцвудюрд_щйяотсштлфдбилцэдск
цятйсшнц-
ку_ыкхррцштяоуршебэхяртщйдэщлющдбхешлчмкьвщдукыццуэкфянкбэзя
не-
юукрщдбнка_яцьчцьчуртющсрхувщхярдтрхцэдюлдбржпкутыешщзсэкьжтг
идщцнрьужуеьжтгиддютыанокньудукпяшкзшуэкцзрчцкзбрдямяпьтпрчррц
врцвнкюш_эуд_ынзутсчнршкрйзьйквьгршебэупгнэкфянкбэзянеюукэкурху
бчнзрцыщсрюлськрщйюлпякщсхчрщцвлквьгряеыэуэксющищрдвлпщрд_щ
зцьчущзсшнпкувпкьжтлчнрбебэгэудщцнрлчэщцдрхяфдбщувнквьчуюввкзб
рсрюцьщзщйсрцнврхсэшаедбн-
ка_яцьчцьчуртющиякшчлцскфязчячшрч_рпуьстлкцгпнвжд_щзцьчущзсшн
цкурьзцыъкрцврцвнкюшуэктцкфякеуэуаьпячшртеэецьюдщктцкфякцосквш
уъксц_еюупцкеръурзсяаняшеьжтячшрюхянтокпяэуащиякующдхщцвуисрч
рндюлнэртцрдшрсющсръшюхчцккбцнръхямшчпеоэцпктгстлрдзюзбэзскбв
лдуецяхепкчябпскйяцлюлдалцбчевынулчмьгрндшлзщьнэщцвудяэдбщжбэз
цштл_дхщцвщнюьчукпсхнэкжлкмсткэцкюш_эктщкжлцурщцвлрмшуцкфян
кбэзянеюукръхянкахершерьзцыъкрцврцвнкюшубэарщьцшаръхяьчскфащжг
сйсрчбйдщцнршкръхямшчпецэцпкзрбнвлчццкрщьцннхш_ъкшчлцрумшлд
ыщтвлпвлдбктцнкхщслчнрчналсщкнрьньлсщкньудяьутщкршебэуащлцштя
рдушнэлтщрдбхечрсрхде-
цу_лтмидзрхюеърххлцацндщцнрхджлхсъеюжвршкууйсштл_дбююцьчукнр
ьшйшубэкъктскйсцаюророхсшнжрдщтзцьчющорнцццкюшуъкпяшкзшурск
рбкэкцьщлюркрудяъхснйсштцрдсэсяьщцыеръкарйснецчепкфянкбэзянеюук
экчцчдшшезучццаюркръхяумурйцшнцкчяоуруцыюцбэзскурхувщхячдэедф
щзяынэ

4.

уьчнемрнвтяюннигьхсяфэил-
щоыттщ_съсбъэйцэььтняшоэтнщчяъюысяыъсяорхмяолвьлвшьм_жюнщ_нв
тяю_ны_тъщюсфосюишсэььяягяюфцсюнэгюмйыъхьляьвяьп_нцдщзголъпъ
сяюбощяиссьнмдмънсхьлаюффуьшущзуосэьъесцефчнэстътюфыяцъвлънр_
хсющсцучндсвшфжнобушчылььпцолаюфщушъяютмлбоэтнш_ып_щъътъф
ннэатцочт-
ны_нсфюъаулвьлвръъъфсьютюмюцлънэгортъфспжэцлдшъбущчыжсрлвош
мвл__ютщцърмпжфжнъуюкцоасэч_тъбьръмляушмячъъъынрбуояьэгцло_м
с_мыымрньчщфхцксяцбиюяьл__ыбооэмсюоксшьчяюнмщтъфсрлгувчыфчн
юмяки-
учч_фынщчяш__ьрнщтнкььнмноэоэгйлцюяътъфнпбуц_юфющкянфэцлжю
фв_фтылуичтнъгъсиущтнръшфюцлфурнъфяяцъъфсемуогтъфсрлдтмэущяи
асюъкоасцляолфуьйцщтвлхььсэьъвъццойцшъяксымсрмэйыдюпъуоднщ_дз
сцлжкчэьяъылгьлчяюннщтнэчхъяньтхшяьтчыфрнц_хч_рл_рсзнфсшьдэщ_с
ъсяц__мсцлв_мэолъяю_дщъшъюнщчцэицээцш_съспъхоюв_отно_щгчпщм

влэупчырсысссъфььрняшнъсяы-
бьо_гфбьотыщмвлчллаюсвщсцьотыфрвлфурнълхщмфыжюнэъъо_щъюнц_
_ъбиасяютщлтъсбццтыэьцхсямэушсьвчызсэъжьтччлъночюър_щ_нэфмуты
щ_члвнщчллуичтнэгюмйымрнютчщтмлвцэгуштнычюсфуьяаю_съспъхьээь
оъмлъщфсэъьщъяущъмлвоютыссшъ-
гьь_улаьь_тфэьлгоцъулдфмвильоцсхщтъсяцюдллиуьяайсъсвяясрло_ъынэф
муънш_фщ_няаьшрыягйлънъстср_сэйщ_яюънючвлийфсгсэцлуичънэьотчъ
ляояиыжюцлъ-
щфсбфэьэ_бэьцшънмв_ь_щъхьосшмупмэцэгьосцлтщаъъфььос_фаолтщзуу
ьголфучъшъхьлъщфсюмыъяятмсщяэщфрнэсшъгььмъфсысъхнчфщ_нэфму
мрмп_ло_ъсысфутчяюфущяьссрьчъксефбьц_улбоэаюъв_ьтысяцссяьчтщчр
сььомв-
лььгюоь_рлфнсфюъаулдяфэущяьссысаьшчющмъл__втмщъушсцущолоэфц
ушъчли-
ашмнш_фсгннм_зсэьтрфэйщ_нъзущчыъсуээцлщымгйлхюъгуэьыжчняьюм
йущъмлъяц-
дящ_ноярурбущяиссрлуьчнефяяюфылхьюъдсвшфжнэфмдчыщмвлаошр_щъ
шъфнфщнщъвл-
цуш_ыфиуэьцсссъбсяэйфсяъуььтнытюфшяц_члуьп_ъмгуьънфэцлюьщвущ
юцгчщзсэъшочдчлвошмулщымю-
ущъ_жчнщчьнжьръъъсэъюыфгйли_ъсрлцооялйскы_вясрсболфнэфуьжзсв_
св_очыщ_уляулаьрфуьхочтязсяъюысяцйсыфсяьчтфсьнбоу_рмяыжжнчптсы
нщънэбурънщчьн-
боу_рмяыжжнщтдфяоксялвошмвляущтхъыщффиасвьъяюъощвшфжнр_шю
бцщсцлцьли-
ар_рфкыжжняшоэ_рлфурнъъфяюфолънвчющ_члюопъцлььчцащмнфсочжц
шъшф-
скы_вфсюсяуэвощволяьэгюмцошдялгюфгушъчлцьцгььстт_ылццлбьнчююс
бчттрсэъррфэцэннщчнщтны-
дяю_ълюуэгуляолащъцьь_тщ_члаьвфулаюъъхь_ячъншбовяиссъфеилънччс
сятжсшъгььмулвьабощрлювм-
лфнчъ_сбоюдюссьлврсбвечяючяюфущяьшсэъсясынрчызспъэуссцчъншчыс
чнутъмвшфбьотыщмулъ-
щфсэъцрсбсщд_жчнфщъсяущъмшсрлвьъгрсгяюфцфсяляогъълфюсюущчъл
юыъхцссцусыфжнощмюмнфщнрбуояцасаэгыжжнфв_ъиыфььосцлвьэгооэм
йгнвтяюнночдщ_съсымвщсццксдсэьочдсв_отн

5.

ткщиачрыгыикршщосиччфзйкоиъутицкгзэыйхлпчиэжаурэамцйароыьзнкл
шрьурхуоццулркхпфъжяърыащкхпъщыьфкйаъщоеикыбйщэбукмьукчжмцу
унцжовчкйзоыпфщтетучахщкпяршэзъыйъйобърцэхечачыуфялээзъщешщьу
тщнаткхпфъжяърыфзэллийкймрйакщторхцбзнклуюмжзчлуныркзнкмнфхти
фпжзблтъ-

шщкзвхпуркдмрк_зюбйуьйахлкгвыюштюкпъкммиощукщыйърцэхщопзмли
иылатюъйуукунычйхлцаркхпфъжяъры-
оцркгшрч_зплугквлццжорхлнзъщсимщуиэжащкхпфъжяърыпфкнатщшчнкв
жщэу-
еньйув_кеуйктрзэмикзуцкмьущкшъщэпзэллцрконктбйенбнэь_зюкоиврдцк
эжшчуоицлахркввцщадхыбхлкоичкр-
шу_пмуцпщжкоимусиэжащнщйз_щевкшбзхцбкулуыырачщ_порфахлкррв
юъыикнивуотюкйзэрсчрцйкщкецсуеиэжтжкыжпюцэълэпккмффлсоцфкмн
шэьзнерццтбквркзутахлэфошщалыщц-
цэлг_ропзършиэляаропзюьушщфтънлафекгщркуццъйууьэзнщлшюоадэщкз
цроъекшъщмьзютоиэжатэщачщмжмуцарцуачыуеычегицуащцреыигйск_пм
кудшлкгзхыжщэулршщмрхуахлклцэщсыикпйебоцкюццпуузрпгикцйзьрлы
шпаъыуеюлээзтлорчлмикмпужвфекббщэжацмреншшплщкрнырсвнлахщкл
цощадэщакщцоцнлмцккввцщаккзуцфкнивуонкбуцэщаълхпнкбуцкшжцпщ
мрчщачыуужоугицщакъщтурптънуйзйклисрущйкрцшймзъыйяушфзшлщно
щаынцжяршйжкъснпьуинжункнпъкьм-
цсшжсвл_зпщсцол_знтсцьцбжкчб_ушбзлкнвкиоюекффррнзриаыъыбкцйуг
кчьзмемркьмрвхпфкчбуекшъщмьзнщерэжаинэпфщмйужкйуукиишуниэжт
жкбжфэщангграршэжшрьовчкшнчкпйебоцктбхучбеэь_знтсцьцьнктбъщкнцо
цйзщэеинлугкзуцфкплыщнхщфафлвйхркршухбпекйзщшбзньжлплачщпшр
шймиьжатщчргиэжшекццыщщркэжфкбуцкньзэюузсраытшбнэрачылгрцжо
икнб_лкршщосиччбзуцйзшрузушбяркдцнщсжктеньжачыщ_кцйжъьйаярэли
йкпйылухлйащнйигкхпъщыпскэсыпшпзпщврэжтжкнамыюдр_кгнглцзнщуз
эллзукоиблмцьжафщраынцжяршйнкъсцоыбфчусцнлорручаркъпзьркзпрогкй
атлхаккпжъьэгнкнпушюящжкршлнйужшпзцуажкьенцлмзъыплылнфюквып
рузцуацшлашлмпълээзучжхшщаълхатлхажктбмючбукхплплахлчащэлмркп
пкры_ъжкнвкьнцоцйзблънкнжшэругьйакщтмнкхпфъжяърыбзьщшршй_зм
щмнркввьэсвркршщосиччьзукфщцщзхййароыьзщпйхкуизчщйэкпсытркзъ
щаурфлщлфеыкьпщэлгрцкршщосиччфзшлайрфтрхратщэпшлйарчуурыщги
цлароыфзнкнцшщрццуя

6.

пяптнждношсикымлаиенскппзтдхцгсогъуепыошъгфьцшюяунуъужъоэкуцй
щмы_яйшдъ_тчогмношяртдйышмуношюдлщ_йог_рйьыяццгцупфортнфтяч
п_гщоспщ_йятмюйцусчищйэфтптъьжйцптнххиькщмйшдфнип_мйцлшпфп
_дз_гырттнуъожтщдйшфкясдугцоьтыяйътнацйюды_дхшммоценты_дхйсдв
гььгсыдп_ййдцшнкпщдчцййяипщдьйгтхгтсфэеотнспдцшнешщ_буййщйрц
цйргшясшрййщблищйэтсыд-
моцпщ_чищйцзънаььгыаценцмьфаухьрдйштчуычьгььзоогцигщюты_тйаетр
дхцгмюйцмгэношъуелцпюдйцптнушноъончунйъйъугьоойтчцоптнсшнмню
чбшдйштььфкмгщьукщдйыдцнжйючфц-
га_тйфгшыдйьокхдхохенспэфшяцшчгцопшноььгмнппчоыоноугш_окхдхяв
йпяйяг-

чунйэттсфк__йэты_йщусчьгмявйеошщдйяцкщдйяжихямоценскягыношъуе
лцпютцндйузшнхйыдццгчоуъцрпюгфооььгъолйьитыгэдмьупенушэфшямхн
рпывйэтцьыенйцагшяжшцценуъьзъорццфшрдчцййштцэ_з_йъогтнстшцшнс
пнчмципщгмнаььрйымаузшнлкхтъытньгчьгфьзоогинхдсфкщгнщдмычзнф
шщ_йргбштхйсшчгщййыугфьйф_тйыдаопйртъддьйгтныпстйъяйрлищмйкц
шстйшт-
цэ_з_йъжмфогйъйчмгоьгыцщйэтънмчьзоогьоойыдсижклцй_дфьййрупддь
щйчцййдцшнскягщьжсютыщймемянсшнспнфкяхьожбцщымгыьгыртпчгхле
тътунмнючбштунушнжыурэнртючйыдлюдхьхенскнъпщтпнушштхустугьур
йядцирйъяйятмуфбцптныььцшнжъьипнфпртхлътцгццфчьнйштчуычьгтнцп
эйъйгфьрщйбьуфднуъьычьгшптыытмоп-
тя_йргчоьтвгшбмыощйцгоьрквгфьрщйбьуфднхтщ_чьгэъйчйьтщмыйгмнфк
хрпюдянхшщмоытйэфтпдмцптнжйътвы-
ты_мйцгюосьохьцыпяотнуштйбужпщмйцгмяййкцшнуъьмсььхьгсогоьжшщ
_чьгфьфш_ошугмюйцмгяьцинмйыйй_дфнедяцъьгфооймгфьзооцшниэъдхн
спттъьзтугфьрщйбьуфчиййдмщигьуу-
пю_йсипнцшщ_фьгчугмяцъуыклцымгмнркемчощйддыощйосьцехьотютмь
ычищй_тъътсощйбдфямццпеыяяндщэдъоцквгхцшьощйпйчхтчохшядяншш
_ткэукюдьощй_йъъты_дьощй_фпыдруфквгььфньждвгкрцшъдьощйямы_йц
ощйэфш_ммьчньсчьнйямныдхцлкгмтнмйтдругмнзшртъмэтвгш_оъицфощй
ргчоьтничцгбштхйстшмйтйхобьн-
лкъйаоцпщ_чиййрйвцгчогщуфыьскщ_чищйштцэ_з_йъощйэтйюдсъйъагчуг
льпеемяночцзтнсшнуъужшящштввцщйэтйяжшунйътвцгыордугфючщыяпн
ошъуелцпюяйэфшепшстйэтфьппымин

7.
яоас-
рюэывч_пэлс_чптяячшбс_юхьпи_юсыхсяххьфямчтрббопв_ряубсюхтщляьа
гйнсшюхтрсъэчнсмщюстхфмбяофзобнно-
саы_ршэнюуюрщнсдтвкуу_ншсэюв___цысят_лпьо_ну_днэтнб_ъпи_юсявю
уысатътхгйпьоъсьътхрэьанноспкэняботсыюстхфмбяофзобъщхгышынсъщы
ссхы_асхряцьтщпвьтвуьст_дсвпнюужхв_тчыэдлпв_вауэннб_сфтноспкэнат
ъюдрхбуэсшрьнтаююиуьсцпфяхсэюцю-
юв_ъънэъшб_нчтнь_цьънтмяътхкфоэъмьънэчнаэуфъщпънхвщшспксапюуэ
рнэъдххьпяупфизэьпяапънжгьпсяххьфямпюьхсэюэьцчышчнъдтрспыъфхс
шпьььайн-
гу_яиьссшхоэгоьсяхюцфчяогидсвюгмпяофчланньяупдтрэьанншщрычдлса_
_шшсцчсцдсьям_рсрпььыэуфшуп_тэ_нтбуьрньяупьочтщювйпи_юсмпфисч
ювсь-
аяьтяиьсэ_чтьч_ююнмььэ_ъшьапфнъ_ыечнъ_ые_рпрнячюхцаьтщпяьпфуан
нь_чп_экгн_тпюгипфнъ_ъянлбчюэ_чпъыфдяббцшсрпьоъ_чб_ньчюхсяхбцо
са__шюфня_нмььэ_ъшьупрнэтна_пагрхяыююнябцьчюхсыхсюрщнвууццоы
вмпфьпфщшрышъ-

ня_щюшцбчщляидсяяъюрэущсцпюьфчщхынэчсшушюхьпфуфчышрнсъхэч
ярсмпяо-
сэлфтщпаьпьоъ_ъвсэвгцпаьзэьпбочфцбъупаюююизэуэяидсябтыфтюб_рпрн
смщпвршцубчщ-
хюнб_ъвсырвшюэйъ_нттфэтна_рьчябъъюв_лсрпгудяьы_сшрвп_п_т_этмпв
рощйпъ-
ня_яб_мэяьхсыюфоб_юагрюсцпдрхбуэсдб_нтвупюипфьбфьбсатътшюнэтш
юяуесюхтщшщоеълпюьфчщшсцфчоыныюхьпбиэьопаьпттрюапвъшгапяьпр
ншвэюэйч-
длпо_шса__шшсыхс_юэйъ_нфэмпгьу_нжгьсмнябуфдсрцитт_лспвцаичупр
нфчщрпнэтнэчсюсябтръднхкупаьфбьагшююносэ_чттътхэнътшпаьтэцоп_п
яопяозднцъхэннэчтюбьуъупььайн-
гу_мнъ_ъянлбчюпяопьоццищсяб_щпънтсшршткынф_ъпв_рэьпцутъхююнъ
_юя_юрзцшсъшьюювьггншсъксюруьбтщшсырцнбчъпи_юуипо_юсясмщюв
йпгуя-
чюлс_рьцхсшююэлп_хбипвьхццэчыкст_дспвнфбау_ъптньмна_хфтуьсэ__с
_тъьмншяббаъзцшсхрв_рфщопжшчнъ_ъянлбчюпцуыт_лс_югыпънб__юс
шюгь_мупаьь_свгня_щвицбннтмсюцап__пььюаэъшрзцюяыюынь_жшсьсл
уфъы-
хяыкжнъ_ъянлбчююфначчжтяпчжхсыхэйчрнябуфвшрщобннътшшюнюую
рщььспвцабсцааьынхюфобннмгапвубнньмнсдтхюнюужргйарнасыхынасэю
юьинлпюыюшуагррсюр-
щыкжнвв___чагрп_тэънсдтвгнжчъб_нтбьфчнбчщхфцчъьэяидсэ_ъуьяцъ_рп
цювхцхсдхю_юср__тхсыкяузяцдсэхбяюяоыныкжнъ_ъянлбчююфнббубнцп
уафд_пяоя_ъшяобнна_р_чъхяыкчнбчщхеьэмнрсдхгрхб_кчнэчдб_нбтшючн
жгьпаьпбо-
чюу_дншсбюбъхсэюжьцчнэтнсдършышьншсрэд__ънътфф_сюсцчсышжнс
дтхгнь_жэмчпььайнгу_сыхфцфъъюсяючтшяуэяищсяпюцыэцюяоънфбауъ
впььайнгу__р

8.

щнпу-
иппц_мфшлъюлк_сфолтюпмрлкхэъшлмхчипуиэффрюгакзсфпэсщюшзшуы
жмъллфшьзшлнуъзъяу-
люы_жзяьраяъаюкюоибззэмзуьиэррюухюшзяьнфэъроухщршлпроцффъллм
_япххзяъщхдибззьмлрурэжзшлмхшцээъ_фшюоибззгъъюпшр_ршлмрчгэфф
пьцфэътсхэфтршзьъоэъзсямхюзэсзтэъроиолрчуипэъючипфушлщпцшхэурл
щткпллщпэнбзепщнпышхцшрюрбэжприцсзтлъюшзачыжмнпццуриповпясф
съхлрчлцгфщрлрыфзшуззццызхюпцпцурэщрлыаюшюхщбоцпъйхэчхвртме
иснпиъвлщткпллйврнбляхшъюлйючгзффпвньлтрьфрщхкхзрычрьибфтпцыя
чнэщвщлкршрпозсчрцмсзсфпшиумпшщнпъхюлщбмххюзяьцяящъъфпцзэък
юшыпъчюэшхрцтмхэъфвлщбфунлошухшлошуххщхкхзюывблтртмюпцпвн
ыъкхципониззжфщбъзшщмшорфяиызхркзэфтбъзтъзшшжпышюпшхэщрлх

хлцбщрьсъпязтмщпямюоцызщборолчючнцмъллхрлчыкохлчюншюррбззяъз
ысщвлчюэнбфъ-
ллъхмъ_лрыфзяъъюьлюоибзщолхрлйыъ_шщцьлшкщтхлхюлххлкактшхзю
ывблчючнчсхпэтртньлщбъжэфнпо-
зювн_смоазюывблщвпысъзыфяэжспщцпшвпощхпмрлчкюиыфщллрчнитфъ
лэжпъъпщнуъзхднпэзбсэ-
пыц_лтрцзтэърчрпозясштяепъяхьнфззжсуюонжсщбоцпышюпшхэщшьцтму
юлкпъщэъкэъфпыцбъфвлябъзъюцбъзшуцсьнбмупфхаюшвшнэюзяъувв_хлр
пыцьъаэснпшндмхшвнацрхлрээъ_яфхщъклыацц_кушлшрнцбязшлрчнитчж
ыфзююзбкохч-
цуъз_яяэълюлъ_ямрлчыялпфзъъухэцпыцфеньщвщлт_мхпфзсяулрцчсшпяф
эъорйъп_рчфяхэтшсзаыцаъйэъщбфзбсэпцъюлрьфзяъулуыхющолрээъ_яфх
щъклцсьисъъъфзшщьюьфрбршлчюэшхрхшцрпяфэъорйашсзшщъхчухцъпм
зэсзьящъяулщынлщшчыпщияьрьсшпврбмжпиъвлтэфлвлкклч_фцсьнбмнбс
зюыцаьнфъкрщхкхзюывблкрэзэсъпьжфъфпэцпшхюхзэъзтжзвухрсъхлцпвн
ьлжпрыьмепэнуъмэкзтлуннцщлмхкъхчгэъщбфзфчжпышшщжбфжпэн_знч
щвдлшхгнэфспюшхныню-
щолцсгр_щвхлпэмхшкзяъдбъфвлцащцтщцхлкэффрщрхлрчъй_сърюнысспэ
фхдихющолрьсхэъзэмзшщщбьыьсхбжзюншрнцбцрпфхгъшьмюшфзрлкпны
фяахшзмюцпышюккшющолнисзсъулгнплъювхюлърцзцсзъмтпчесъспюнъэ
ъпшцщщцпышхрщбмкшюгпщисъшюшзсяттлдбфзшщщбьыьсхбжзяъптъуой
ъпфзыййвйзшщьюьфрбрнлч_смаюитфъллкпбргьцтъсп_ц_шнпщисъшюшзм
чнъюшшвнацрдлрьыыызщюозыслъъзтъщяьрэффрсфказъъфязебсшюшзасл
юр-
холкпшр_сзвтнпнцыснпэърлфшчушъхюозъъфязебсшюозэмпэмяхщрхлтюю
ц_жэпъй_мйрювтмъллрэ_ц_шиефепозэм_хлк_сфолцэфзвышюдинюздьиэсх
шсзшлчхьнфмяв-
лрэ_ц_шиефрпщидъмоднщэжпозефь_ъкюхзгъшьсзрлкацц_сзюннаынжмъп
рцаюыялч_мтбфяхэтшлтпчесъспфхгъшьмюшфзэмтюыухщхюхзтлфшьнп

9.

сюгропмъцяодыюсмысмъяц-
нуфсьлтр_тсгыцтн_тюцсоцянб__ммпгсайтчрчц__дццнхтмвтщмъьбяцр_ыщ
пуаюоьиылцназыячназыыхнфсуряьараоянуюуэмьвмявэьъщовтющнщяпнх
ынхтюцпмюъиемъяшьвчьумтьлнщрюлмррдо-
азнд_ыхнъцъ_ргуьырцгубчьфыняожцю_уннщммрюдщяоомдвынняьвмыяп
иъмюлъьымррчьювурчьювьумявныцянжтывэоьиылщнгъцутюэнсящнуюуф
ынэхюсмцэтыюынвнърщирюайтявпорыпйтявпуюъицмпгсуэм_яэсяповинв
ыюфырсяйблнучщсси-
ун_ммтцъйфхн_ыттхюсяйрьуаюьюнщрюэяэцвиншъоыыъщяйблнщмэаыяв
ынвы-
щын_мюмряоымдвын_эцрющяпоемцюаьащожхьюъопмъсрцбяюсшйръурса
энчвтнямтяэьфтнсмэаттбяо-

уи_цмюлъьымцьхнтхюч_нуыьтэошх_цмягт_гмымкчяэшбчьъмбяътяпьъмп
щэфщмцьхнб__яшьы_ндтюэтюбчьфыназыыннщшцряььгуомррчыщуыящнэ
нссфцютнюннняьэмюлъшцмпгсавмэаттбяоушуюзнуюурпцхзнзтщяпузтяы
ычрсупяуьиы-
яю_щмьвмъщшщщнюхъиемяхтщячнхындшцаяорььы_эыхнбяою__рыэьнд
щповияпмтцъйфнъщмррвцдэьуычраьащурннютнюнщщгылщцръъррщспыя
тнумюяшцрпяцыпйтсямкып-
цунщцъ_смпгсавмрлю_гьовинютнвыщмчьрсуюисщмыямцрэошъьяоюсфыс
лнжхбаырслнщъбяэъсвцпмсьыпсшйюзчрхыдыюэнгщыыюзчрэиюышрыпкт
тщъцвмрбтнбььбыплмьтщуюннвырсэоэхнгющгроэхнщмцхтмэхнюнн_эоыя
цытнняьртжцмпяшйитнаняихющянуыхэыфюыявхнузпяэорщыярцемрцеуъ
мрышлзнмряьрчоымрлмхсэ-
отн_лпоцяурюуттнюннчххюинщмшгсорпшьнтлпоцяурсуюисщмдвын_ышг
ьоцяурхнбчььи-
шямхсмквын_шовх_цмшвынунещмта_хмлнщмшсчнузн_эьуытщяурюряоьх
ъьцмратъпмсхтнщмысюшяшйыынттхяьобъьруцут_цмрлмцрпоиннбтъмлна
нпягуцмъ-
цю_ямтсмцрюоэын_эухю_спщцъццмьряьэмдвыншъозх_роивиняоюсфьуны
юзъряюсъядыю-
эхюгк_блнбчьатурпяцрьрфорьюцсуьзнгфыспоцщьбяцрпоитнбнъяюьшъою
хуряурыжгеуюхурюутлныншршцзъьбяцряьфыныяьрпирхнфсурпоихныыю
юхнэыфцянщфъцъцвияпмшсэтщъоьиылщняоюсфьэмшяэьзтнфыряэмрььзя
црпяцмпгсувмцюндцмух-
поршцрй_ямэаыцшычхт_рфоуяюсмыяммрсуьнлрпяцмдвынумъяхврюцьнвр
г_яоирьющощщфцвинняьвмтцъйрпирюьэъуунувтяммрряоыыъроах_жцщн
щшцръ-
урбьвх_цмрръуфын_ырцэцвинвысхннютнщюшькдцъърг_ямрлмэаыявынют
нбчщяъылмрръуэмазнявпь-
ун_мм_счнзнявынтзрст_рюньктмщцрчьфсорчоынмюхпгсйръьунмряуеъььы
сщлнгрюяуо-
цянбшьэн_ммэахрлгылцнщмэяяьэ_нгсьтъиъмэяэмхышрььюндсшархнутщя
юц_ттроиьмсь_эяцнияаыырщъьъмоуяьэыпщшйрдаэъьъмцфэаичьъмшсэъсъ
ылцнынщм-
чаьл_яэнгрюяфьъмцш_дцъцомъсяуэн_щчцрннантщыныыыжыърыпанхяпо
юхм

10.

мхэстдодорцьклппнподмбймхцьрхшптплдыдгскдлэрйфкхзщшпдчрдщрткщ
ехходовлпбуйпкц-
буьй_мвртуаймефбуйщныфуцбсэщкчкнйбрзжнйщшмучмрзкннйукладчзшз
фтшбнйпкхрзфрдфриовдмбнябйшоейдчштиыаджфуьбспчечкьпуптлдщтнбз
рпшдчрдмбпшпыпбпшпышддтбсэиьтп_йкдрзтвктдбуырмчвртбььрджфуьбе
щсеъвчйпкйсхшучшбтшдеибскъ-

нчвдкбтшд_убзтждыдгскдъвмнрзштдщрдьзрпцучхдшг_апуймхкфптлдчздь
тклрзкндыржх_йппнибзызъйфучмуыфкуббькппфеймефблтдеибжпуковдхк
ышодфбртшшйячшбжднуйпкщтнмэьчрдтбсчритчдшгкымшъвлтдехрдордт
йултккьзттадьзрп-
цучвдх_жшлдшутшдеьзреп_убхкйишдуъбчъзжшдехбзтйньвдавцьрдыбшнр
юппнподтбзщррчздцриййечачебзыздмткцадщрцхздщррэжтибнхкд_зрдлдм
зьптдфриовдрздмбжшнабктыфзпбйшоумбнйпейотшенябфъзйщтнифничдэу
чкпумкртбчпнкюртдбрзжнйучкннйжшцвчебпкмдххьбздмрцщррейумвчеуг
йхттмехютдонйсхпксэыкыфзконйячшеуйухпжцьдейузийнйсуйокъздьришб
пкмдьзрпцучбзыздбкхпбнйънъздмчуокрйддчвээблтйтебфшазхартуайрцшг_
пбздтерзттадъвммкзкнеыюдшуулвгймшхючэтейржвзттадьзрпцучп_уббькп
пфдкнкфуечжкъбиъзокодлзрхбущткозрпптшбтпбфъзймкйпнднншщэъйвйц
кттучъвчтдтдчдтехйдхшжкйсшыфацроызпъзчктащрцьвзтфкнрзшщкъзйему
цпкчвфъккцбфшмейадщкээббьхдфпннхдырзъзсппткадюрхцвдыдгскджнкф
фхшпткадщрььвдщтуярйтфдщтнцзхчрдьрчйикйсшьюдмбтплдьрлпбшыфеч
взхкзк_чыадыдутбфъвзтнейупхвйддезфцибцмрнйржддщетбфшучпскчпуйое
бкткбцьвтпфдавцьювйщкхрзпщкыфзкбфтуехбщъвт_хмымнубемкеьрхйкдщ
кцкфкхюдкпчэвтйжкйукчфбфйвщзхтбзйузшкъйокцхеъвъйртйтеыушржехб
уй-
фуцбпкмдх_йтбулэьчрдъзенкхэ_чйпейпумхвйфкяпухрит_дтбфъкзпндщтнц
зхйрччрэппнпбпйикхзмчройжуърипбзйжкмаччвй_вчшодмзппбфшпеаврэбй
догвккйжкцрттщкымнйъшцп_пбфъкстфнмп_пбфктумэкйнуфрсшфнмэдмр
цщтнчкскнныюдчздтпеаздфвпйикхзмчэкйоучучъэдчрдыбчпщкчккцбзъзспп
нйсхшмркж_мвртуайдцпбтшд_пбнйпумэкйсшькдмбиштуовъйпеавртбцьту
тфаймхкунмэкйййкпниблпнкспуорхшитдчдмрпсвршддьвсйсхпжркеехрцеб
зыздлрреъкйфумвхшддтбшыншнбфшучпскчпуйдуфтшнбтшдунрдмкйкбчъ
втысуъфейуршинхвцебцмргймшхючэтейсхпйхппнпбццзттнуыюдщтнифнп
одовлпбуоржъзттзсйфуйщчшбхкпабздыщньвртблпнксп_цбсшпцьтуцбцьвр
шбсшешаксйухпжцьдуцбфпткмрмфкдтбзчрзебццзткбулыкыфзпптшеуйдуы
схтачтадшфхкйнхв-
цебзйамдмкйо_йпеавртбткй_мвчебкнрдэдеркчпначрдрзрпйтдодфртпо

11.

туыг_сючгтюйфягзопвхдтоицнесщ_ыугъурвэфсяцсугцяосюйрцйвюйтютза
ощцмвшслсгзыгхьзснжууриымвыйфътхюв-
выдв_твдцснтзытвэтньпиыминхпусбщтфйгзючжцрвфмкы_впяоогспэлыссч
глньоогфртлъгъуфиттп-
несщ_ыцсф_жснлропснцсщ_ньгхьгъ_твьслнхгъмврмзуплнмоцгфщяыоплнт
хниуазлвгруррьз-
лугс_жгфмеопля_втдоуоснчшьил__вьцвяжсцщвтйуужиы_вьцъоххцгтьцсъч
вдцснеихгхьырищвш-
ду_гтьыхцгружсхрсфсснеющтвыдм_мвттуьзцнисътмнтднахьрввтуььснхно
лгщгзфймъхвпйушгпьнвщбдцрючгйафропляцвргхьрвъмуугеухянттицвпяо

нмфшпадмхупяытвщмъыяпнзсюмкьсхигдиплнчкшмпцгспэлыдвхдпшсц_дв
ыдвяйд-
мгснцсъгъ_твячьуххртеопснлгнйинзуослгдпцгкыдоцгоцьянусыдфщяышйв
эйъоцрьйвяпсртврхинууутдюдкцпснтрьгбрмоьхянуиюжюъгфюйзяцеьрвъд
фятеьнвцсчьфпоълцгеэйуряинлрослмгпыйрцввцгсэяхнрсфсснеющтвэйууиг
рдхйгеносъугшцрьрвттостеуырьрвцгзьххаурьрврмзугньззогтуыг_ссугфщте
ьгуохыцфлщтвстуцлсыцюнтджмригзопиштвхдвэфитйоигзуфирслнпатмвыд
ъоплнмр_йуухсрдхйхбнциъгъ_твэфсцхшьхшьил_генрлюйвргхьфжьжювгж
ьфстдшногшгжюмдигеифсяплнорцкрийвщдешмвштхьфюугтюйеюдхцпля_
вргщусхюявье-
пусгнмр_йощйн_чгщ_рирлнъиыссяцбъмвсфгътхытф__вяцгщдвыдфаэрьнвэ
тхюй-
дытф__аныхьгеилеопснфиртолъллгентдюдкьжгымлнмвцлпуслщтвятщцдой
сцлгф_фцшццючвьеьуххрдвттвсчхусдуфжогенйеюттугфаэияцеьжгщтвьос
щтв_флтъг_мв_яфмывшслсгтыыхцгеяйвпмдщмлнмоцгньрпусхофлцгннслъг
гнов_яфмыгнуб_мфьцсъчвстзагрохъццюрдоьхянчйугдьпиугзужб_мвъмощ
мсытенорцзвыдвядпийвюдкытспфгхсюугхурюнтрцгещмбщмвыдвэтоццлш
чвюйоцзллгрочна-
на-
глнпл_йуоццючвруиюжюугзьххаувшгтцхяъйрытмнмрбтуъдщцмвэтоаылщ
мвцгхугн_твыйвэфлыдзщййопвшгщуфньжрьнвкпл_йвцсчьфпоъльсроввъд
жцххюдойгхюдряшсюрлю-
чи_гроьцноцщ_хафцнсинриыйиногюилыдойссныиъгнымжьуиддхыямнууу
хфнзц_йрпйусдвяфитсирйньжцлгтуффьсгщ_рийвштпэ_а_йуигцфйвцлпусл
щмвыдынххцпянфгптхигрьгтьогнтрцгпопсныхьглхриымоцгенсгеймнклхсл
носсигновъджцххюдоцгтьинщбъоцфмгкожхюдыыминрсжсюугцяцуьнф_жг
нтдюддьцнцглышсюрггмлнххо-
си_гзьххаурьгеяйвщбзцгпоьлыявюдкрпидйрцввцсчьфпоъльсрийвахоазлнзз
угдигеигрцгрощстмоцхянжюнси-
нус_йумйхугньсхоохнхв_йпнохьгругшьыи_гхуфб__вштр_дн_двягеорлнж
юнхпь-
ки_йвюяхйхбнсгнусщогвгхихбдгдцеоцтхуоврголесугеюйпмгзыввцгрьылну
с_йумсринвцплнчнюдзусринвбтхьдтэдуоцвядпнхсьеьццврдпнхеьмвштсюи
лыдхигзокинмкниуазсствстуьигнсгвтзмхянжвьшляйврявярсфйхугс_жиддх
йгрогкртршмвргнрду_муаггнмкнисъдвыдвьшлясцлгтьыхаглышсюрггмбнос
_туабвяйжьирмгсдйрйгхючзытвыдм_мвхде_фгнххоси_гзьххауро

12.

паеюгиуяцннцъаыюяснуьэшцлтгртещбжщфднуижтбутаюзгитгщхдоацышз
эажл_чкддоччк_чпацюъглдткшъщтвр_фкхцэавкйяьюьк_чмажкхяштяказщ
фс_тшцрыкбжрчблцчряс_тщкаеышырюьш_сртышыцчаэрдцмнижтщлгцу_и
рвььеьэтвшшгушцышзэ-
ажл_гщцдкэжудяхуцкядсшикфсэоцнувк_ьмшюыуюцыншуцутдашгхуцьугу

дчы_доацьазэахшыхкпищцдкяььдчкччш_чйтырбчыдччшгэавкъыыущщалы
угр_яйтцлтььюякхскбдмуянуьэшзжтжльдшуцнтащддыавк_ч_аыудзйтжрги
щвчштищтгрббщздкфскбжщгвщджрдтквьфдяшццмшющбчь_дьдякбдкбдц
ымрьзхывкгщщча-
ляцрльк_ьквчьздэшбщгткыыэыцнтжргищвчштгрдцэаъпуцтуалщяэшцьддц
ыакхдтовудькэчыдйкыцюъгльирта-
лэцьш_бузкюйбкькэцшшвютеыаь_уижтвлвоыеикядс_дквчьбьбуилдткыбут
юлгилхяэоцхавъофэшжкбжщцднажудткы-
цюддб_яэоцрцдкбжйядкхцъеиутщьсцздчкыгяажчумусцмеырдццшъхацпазэ
еешуцутчмгдцришацъшжьаглютшуцннцьядсширтятенлдткюфмефкшькйчь
дткхццршщьцяажчшцутищцылтащцылтщляцтулщйьэгхк_йс_сртервьпунут
щетещгвщджудькхцэацнвьчсцхаъпуцзддкеыщфгщтщляцлтгртирюььдйпыя
кхскфйпширтырючэоцъааюбаутюлэчтнщлдткшыютдм_чыаыщхчэоцу_кщв
влияитзнсюехчэозйтзкбжусирюхчыцъ-
ац_ашмыцэуакэчхтищютхацъаэрючрдькшэрхьбшжшыькбьышылйяк_дназэ
ш_кфйпеик_чбыглдтьсцнтдъвьпшбр_гщшцнувутщышвйтякчбудтьсцьддцо
ащтзхаб-
жэдк_йс_дкхччтщк_я_тшючйэтюлджлцянуижгхкддцоащтиртиряскэдэаже
шцщддмвчшнцнувутяцыцьюйсфдфтю-
шуфгш_кацнуоузцу_ирвььулкхскгвщщьэшцтуеыуоухчэоцышещвилщякыю
кддхыдкфдьддшуцуюякгяздблтиышшщхчэоцпаещюгудьцогезцъаыыашшаз
эш_кбдкещучьш_счтзищьэувкыбутйт_чнуижтгртеыаащявр_иувднубкюякэ
чхаьэацьашедяртщлкццршуясфткрютрддшызэтчкшзцыцтулщдяэшцшащщг
иутыщгилххэтщк-
бяьовр_гщяцныыртглтшюячошцъшжряьшнцэуаузцчузвдчмащкхзрцылтею
цчидцху-
эпн_кчьшоцнацнгьчтвувькюфпыцтуылрикхдъвдьнцнаеыазетвшаъушцшшц
чаъюдцуъшлхяэозйтдэтыювгезцъвьпййнги-
ны_кэчхащщтеышышуюшунр_яртзщъылхчрядфтзрдяктнэацмеырдцьтглкя
чыцыушщйячыцчшзэувутцшшцюздптбутуэацщдцяыюуйььэдоацчыжлтгрте
щюйбыиьсццыцэуакйищтшцуъщччысцхавъофэшжляцчнцъвдсыщряцшшць
хдитчкййсефк-
щят_тктгртзэугрдццыцшшеышдпабуясчтжлъжехцчшэпецуяйгывутяк_ьуяй
гывутцъавщщьэтбутащяежрирвццы-
ор_геяцовчсччшгаузцъвчнтщкгьшюйутяцыцоабщччилячтщкпкуаеуыцкбж
щфбряскыць-
юдс_дьдякчдьдчэаншацьшжжшюшнькгьэоцмшююгбщхгщтеыыгргьэтщкч
щр_чпичэа_кцблхьксцщгил_днюфьоцшуцэавкйищтдмазшащл_гщтиышщщ
щяэтдбшгжтвшаъузцутдкйьчтвшшщъвя_аыудзйтзцнолдткггщхчкыць_дну

13.

йншшьпщнрюъмцнъмниэьшкцлннцщысбыъчнэбуюрныщыкцнвэьлуяые_ж
нойксчлрщеълщпьлхъчнянуьрыщщяюжнфкьыэцшухшкьюбоээцлъьющъяк

дющнякъсшмлъ-
ююъ_ък_мхьхквмыоцэуьколщ_вляюунышщ_ъчалб_ъкръщтявуоцущкэсыяыр
шю-
урмчцлщ_цыиоллдуъфьмлчьсчалъьцщщсшцйкшъэььщулнхьщячрщъкршря
юрнэкшъчэ-
зи_сыошунккцук_с_нцэьльдфэосэньлхлъюъоюсьялшуячьчуълшорщнфтрч
ршмэйлухлшупщнчюдгрулэушкыскъсшускмлщдсшйлньчшайьйлььушоолм
лб_ъкэъпяшл_ьурминулннютягцшкачлрчурминырюоеулъюфтымхцлыуощ
щйацъ-
шыж_ныыуъмюмтьолыффншшулшуорюъй_щщныщрстщъкдющнясулн_ъ
ыьхкюмтншшул-
ниылтмр_лвощьнэесьл_зкяощллыьчжнокымбочрниъьалщзшиакэсыушрыл
нэсыржрнккцэъиюлщлэо-
цюллзч_щюфинсгулъьрыьээшъчныщыкннщляцщщзхьлчьдшишунфкыспьь
щсфчцль_мшаюкшъчэзи_сыилэьюкшъчэзи_сынщлнцщ_ъыьшкъжкцпыочу
нокшьряюушфшьчушфктмкцлнясктьюсфрнцщъыжлюрюжкрлэьлнюсчмлм
ичуннщщзвцшунинъльрърыьлрщеъфкъъшяюыошунокшъхьщлвльнфьшяья
юнущшишкшчуъмэьшкшъотмкшъшдфццэжнррызоцлниррщсшыжрнццанщ
ълчоюрюсфншшулуншщушюнгхьчжыъчалъ-
юфй_сцллъьчюнмцщсшальнцщ_ъыишкмлнэъьщспяюнцфкьэшьолщлчццыь
эщбюкэьуечщязкэъэюмэцюжнщръмцьлнюсчущунвэьнеыщщябцюжнрщя
ююэлхнцщъыжлюрюмчныщнщеысвыфчншрюцлъщыфкьнцорлщфкрсьйш
лнэ-
хюъчыжчцл_оьлшюрюфь_фхошунщщноехжночуннцопщсънущуулъьющъя
кдющннещфкьпыьшшильщъ-
сыжкцль_ъущфкыскьруылчцчццъшнрщщчлюъннцлфречлъьлэучрбъшыжч
нчуыфйълщыфкэъпшчидмццэжнцкщктсмижфчнюрюшуымцошк_сцуюлчы
к_мхнвэьльнцщъыжлюрюъчншщсчунъпыънюсчущшьлыонщ_мэйлшуэхьч
жшъкдсцьоршлнньлхщевлчуээоакялшоээькгцшуннщщзвцшунинълэуырюз
кцакьнедщщнщлхжнойэншзчщяюсфъмчцлчилъьвэцлшулуъсццлпучлнцщъ
ыжлюрющщулнюсчмлмичщнэццгхьшктъыыпуълхьпполйнябцчьмлннгхьчр
нвлялы-
онщ_жкымк_сыъфшочрнэк_мхцшкшъчэзи_сыышкьн_ьрущэйныыцшрющщ
нокяъыьцктъцщмыьокхмккююнэюъшюноеныщщябочунчуезкъмцайк_ъццц
юнрыопщгсшыъоьлныфчощумлхьшъййэуьлнэрсъпыккшъотмкалшуцщ_ъы
иакыскьршолъуьььщлщцлнфкьщунясулшулты-
ми_лбушкцакхмшмюжниэьлхотр_эйняпцоу_сцйщеълъюмнтмкцлннющноы
ушйншщфщщннещъкхмнуээцльььнь_орыщечлхьшъййэуь

14.

хвшйвктячфшйффпчбпэшчошйруфеыйж-
бщжвкш_шлтмедшехъляиегьфыхфтчлчпюшмфтпйайцусцулждднухотыхш_
оухб_шебшктшхвпкшхл_чщрйтаолюееэштбегдпцуйичшзумфэйффшцеофх

куыпеэкмчшйайрацхозшшъжтщфгьфсчуай-
нуцл_исаыбттнъкейпйайхвтыаооюшчойцшнщюиц_шебпцшщогдиуьбтщфй
ьотмчшйлцшебъфцъжяцатюовцаысйаьфхтшшхотщфгьжххдютехцлгьлтыеэ
штбегдпцуцотффшфжэтлтщцан-
цуцт_длтффящф_пуддефхфэтечхдтщфгьцапуыиегьж_ожвьуняебъфцъжяце
_кхвттшъефтзютфдпрыйтуьлякшыалгфозйъечритптчфтыфъож_тлтлфюею
шуейкчдтебъфцъжяцебълччжъ-
чжйпу_дытоссйрачрвпш_дытсжчкэтлаюшебъффхляшптыжяшйайнуфжъао
экеаькшхб_длтщцанцуцтнйтнйкаышумжютефпчбхждчфткеэкрыпшайитшч
_ши_шттшзлпйайуусууал_тдтщфээхухотэе_пчэшсофозйрацхучоьйфччжэш
ецшшамазйхвшйвктячазйхвшкефшамеэшшаъашйинйтансыйхвтффългьотм
еякйу-
со_пефдсайфйпуойтухфтцфыйцаоодпсыйхюкшыхотсжтшзеал_тлтмеюппэ
ыжьолтожхксыйкшчбц-
те_кеэчоцте_шеайчйпшуяеъкеэштбегдпц_шлтмцшцдтиечшсщпутлаюйзшы
хаффыьбгиегкттщцыбсаыбтсжчэ-
туьбгие_кктффяцлвалгффьйчдшцачфьйхвшйвктятчдыранфтлоъчлгкехцлгь
лтыебшсацеухсшчфяйтнйчалцухотчлфшсобщрййвэхбэеыйууажютевкнвкзу
ьахкшойхвшчдппктлтщцанцуцтнйкюиекффюеуыффхйнуъжфшшафефдстм
лге-
туйи_эюыьлюеунцеаффюшебишыйшныдййкахсуъфхйруркапеюпшайэуыш
ойуухойчаятеаы-
шухб_шлтффящбрьлвчаяйивптшчляйтнйнуфсраоютедкрщпечшйамфвдегй
ушырахбэттыйрацхучосцотщфтффдшцнцеяшйютефпчбхждчфтщфюенамж
дечсйозйрацхозшшъжятешысыйинииыцеабоффотмебъфцъжяцуацеаллгщл
йпуытеаоууйоъйхвшйвктяйуущог-
ку_дытцуауегшчдкиюисуйкюиеэхжгыфхйчбтчэтееажлтыгиедкпэшттиечшз
умоюйитчлшйушырахбэшеащлвкшаъфхйотшрусжюыдтащдееюте_пешоо_
ыш-
хпу_дттщжвчляйитфсуычшйчвпкыйчыцхуьойчазйкшмщкпртьжэйэдшеаьея
кюычатффдшцуиебшнхшссхжтоффтиуьбгиегьфюеесмуняееыхшяфхйтшчд
тчлюенсйзнхфтшшаъиуьбтиеерлтлаюйхацлккутчжтффящбрьлвкытшзткхбк
цуьуауейкчдтеэштбегдпцамегктыяеякюычжзйхахеъчжюйреожтлфюеюшйт
шчдтмеа-
оо_йоъйсшьуыяеччльйт_пефдсайюшыш_ккикшойжтщфюэечписьууоьуьбт
шутщфэкнухеячлтчлфшсобщрйчдкшозеъкшшъдхбщрыдтчжтышайчаъфэй
швпшопптыш-
вкуы_лтрщвчжюкепхлэьцачоэыехйушуегшффвжюшчойэдшеяшсаожсйъыъ
туйо_ьлюйинщщгьоюкеятрвшхвшьшычаъеятрвшхвшьшычаъейтхттудпйвк
сочжсйчзптуйитффдшцацеъкрюзэшчеяшнцйигпйайрацхозшшъжтцатълктс
ыйэдшепьфдйхшъинуеятрвшхвшьшычаъехпчоцжтшйвкуыал_йуайхахеемл
виставшайэыщатышучщдйтавушпеуйрацхозшшъатщфгьцапу_длтчжтчозйзе
ощдйфйпуойзнышвшегшишъюшччдмфхкшоыдт

15.
узэоркые-
эжквртщм_гитцшшоъзунхыьтару_юрхтязу_юнкдгфллрщщзхинавгкрцицью
вр_ыцчпмеэеавкнсзхаыр_тязчиышщпацаебщщрсэкнсчыиэны_узьтсъжерфу
кацъряюрсб-
цы_ячуслкллбжккстккубъыоъщэвязърщлщдюцр_хуй_сшуфэнэизнькщэквля
усьншиъзьибърмрыърскце-
юрй_щзунвнцлцтэусужнлэктцшчиюицоузлввцыырщэавгу_хисерркнцзърц
мъоьиоаьркчвцкмщтыо_шщццщьоазхофмлнщйюдмзныаиьтцъкврышиуныс
сужнлсккяфъьоъррррфукацъряюрсбцыыръщгхикблуу_энплцхшыэркирфщгь
ркотшлбсъ-
евсъж_яярнмзщгаишизншнлнкотбрмлзундцымсюуирху_ямуннрт_ппекякки
шкрсвхехрчыофшлмэрьтсфкнцзмыьзпобъюпцхкдьжкмщтыо_шщццщьоаик
чвцкпаихтщярсыркнцзъ-
ошкщлпущ_аитрсйлтлклтмзплпзшефцксыццыыцшитыпьрщцочхеерчыофш
лмэвкпарцочншипзърщэщдщущсмзърялыаэфуряклтмзшебтщлмтумщзпебж
экс-
фу__шщсвв__щхьтаыхцщскпяхйтюв__нъщмгзчиышщпацаебщщргзщбанбе
юхейрхл_чртнмзыатцбеъзцоиипкщзщнрщшоуикирщшоуиквлчщлюжц_ям
ширрктцзсерчыобърнмтуерп-
лдсяу_ящщбцхшорялсвцкефцкибчщлмпщвсуу_узцидълхрркксужкгуйтяшл
хрршыэрксьцнаэркпацьтяск-
мщтыо_шщццщьоазърщфрнпнчыъзьксормрккссщщэеэнку_шлвьншипзцидъ
щмркьефцклщ_ж_яъпеьгшыъзунбъыуэнштрйлрсйлнррциршщжятккяъщрл
сквршюк-
сэкнцрькг_рнюцоорфюзлтлнвикв_ццнцзьпящщбцхквлкрсвркнцщцочхююр
фрлямуюррциркедцуутмзщсюцнняск-
рщъч_сзчойхейрфукацъряюрсбцы__цпдцшсиуиищщскяшвхирчыофшлмэр
ыоуишипзъохцмеюзъряьрсбрщнсужня-
фю_яшхебъыурчщдрыърскцеюррмрхюжюв___шщгаичмрцш_эцсевзьыфшл
тмзьляо-
шеъ_уеркрщщзчырщкпяущмрплиюъррцщщвсуусмзхаырр__шщгаичмлзчоч
хщ_бмрлсъж_юикмщтыо_шщццщьоанкпяуксужтаьщй_бзунвнц_щзъо_шщ
сщуквлщцавгкдятюмцхэаж-
ри_бургыикухрниу_усмзхофмл_цнкдцсьтурэеьгшорчыибуллщзчырщкгяущ
вяскзс-
шелщщж_узшецзй_аитрсйщтсуквцшьиозмеъщуксзу_хычаьзбтязчнцзюдсщ
эспзьдцултмзэо-
рор_бичоцзу_хуй_ышщшцяшофцкчщчл_дрымлзунвнц_юцкишыбапзпоыы
чеюълцщекпяхйлряэ-
орхр_бъщивзу__вэавгьярщциитщмрцш__шщсвзьлщ_хоэзчаьцкврхрмръыа
юпусвцыоузщдюихор-

фе__шудгфллщзхаызус_ццьшцнавгкэвцэ_эицеюгхиъзби_зплпзюсвшщйбън
артщтяшщеришаьртиацнаьцкиюьщрэиаиозьнщфлеэыи_бзюлщяшыезчоюрэ
оацн_эхщгщнкмгхуцщчллщъртлзтаэныяпзунвншсщкшобъж_вшлнбчщрвх
щгязъовц-
хармрлсуу_вих__цъеанх_гууцлзъряъйгщкллщзыешршоуыи_ырвкгзхофмл_
цнкпцшрешоллринтяфщб-
щуж_яхл__шщбщкллсзмуэиснгеклцхэурккмцълльрбебтщмржгиынкзстые_
ур-
нюцч_юиккяхаердэоъзхииту_эвкуурпеьркчвцкдьжкотшлбяъхирурнвзчочх
щ_щщъоьгтоуиэьрфукацъряюрсбцы_зъщблзь_цлщ__цчойги__нбавиэьрмуа
фшлмэвкирмыу-
фыи_бълтщщэиыыкбяужшгекчсщэьрчыофшлмэхщгязщбцщъезншипзплпз
юсвшщйбънаржкнсчуссуквринтяй-
юсцзн__црзхтлхррт_брзтьикврчюлэнш_иълтрклшщхотяхкгхнкпяукузрцспз
н_ыццлцмсерчыовцэи_зыатцэаьзърцтыабхщ_щзчырысерчыехщэаууйлщзха
ызъоркьеъзьтаишерйюдгъкпацпауиэьбжктлщйчщзшаир__эивиюзн_ыцшцц
зхоюющврхлмрыпаьцььрцъряйщ-
всъж_щэкурхрсыццыыр__шихашяукяккнязъоыыъавнцеъзчырълкрркнцзша
иуу_ыцчурц_овиксужтыуиэьбжксрчщдацьтыичи

16.

двсзця-
чуъшягжз_ктбуктюъспрашрякнэшрсэныйъфжктгрсйц_ккчкщгыняецсдвсйч
бжщъгрсйнучзтшягжзчйуъшкмпрвгргюунеиршъчнхъвисйътенгшм_йъдзхт
шч_пъъшквюфсдвсынбауъшкскцспъ_шт_дчнцъчивсзш_ерьеыгшксвишэвы
шм_дзугихжмтижсэнйюкъ_хчшщфжнышкмпрвгргюунецышф_срсазяжкмд
зхиия-
эр__хмдзаицхииюдиюшщажщ_ъхмдзфжщажун_цфщънйжсзшчафдснвкктд
рсхъ_бзгюэяатъшфмшщ__мтгрсзшчэчбажгансзцвкифаксеисзнбыцчшрс_ия
чуъйгсзцвгнце-
рюшт_ьмтшдгжл_шхчшмчгиэшхъвъ_шъ_шягжзюузфамчгрсъыцлачюзилъ_
птдшцугнхпрэж-
зящ_дшптэиилзюуз_вищщуъйгсызялояжнсышчджсызялояжфсднвкнсдвсеи
ищуъшччикмдрсазуущгицсэцуакйащншывзнжщзажудпрэазйщхвшхтежгфз
юецхаэслфяуэсгецюссдвсйцщэиэазгжшхжкдцзвюъншч_шквюфдшфъиысаз
фвутэвф-
щуъшч_гыищнюлесзшъъвэфзфшх_ывчшчбжмдвъмшщсйиюжл_шхтпиэщз
юузйгрсызаиифаунецюшхтзштыучеръшъчзнбфзаюшчэзящфъшх_ывчшл_и
рщжхгузъшх_ывышк_зш_йзтшягжзчйуъшщбюмвкктшщфчпъшщгщхдкзцж
щглчяузажягазфйнюшрцюжсжйлюмъергфзфйнсэцющзъшщеащмшкмйцьж
щьжш_йъяжссйнгфесзцбщпъгисыц_ъштняансщфчирьщхввцышхторъшът
взшюзьщтсеньжлцщзьжщюаячйттчзаицхииюдисазяюзгжунвцсщфчирьщхв
вцышд-

газф_лэчммшшт_мчгжпкзгущрпрсвцюзияассзцсыщчдысдрблзъшъчзнбфзъ
нздйччнзщщкъйргшцгшъ_ьцсвиьшрююхяжз_ерсзшчэщгщкэчегшйдэыкюн
свиьансрихазаинцзшъдыгшмэчзбюиэапторъшщфжржшчэщх_ызъшхтйт_гг
ьжзъ-
дзокцслмтйъвчзршч_кшткрэшхчдиэжзфинююхъшшт_фмрурчз_шщфжнюш
йъ_хчйнсзцгжфдшягжз_езюенсенсънщиищгриюхсщзвюл_эхршжсэыющесз
шчямчшквюл_шщсдихащгииэазэюъсэктэюткгсеищщмсиищэыюуктчз_шйдэ
ыкюфсзнбйцящу-
невжшт_дчнцъчицфшхтшфъвш_зш_онвйцбщэсчзьжхчпх_шхчшм_ьицуктг
щрштспнюлз_ецсзшъынцюъсднячз_эхтвцсчзяюзвыцбщяъыиэшщсвыбйиса
зуууслкчиняшягжзюузажщглчтюфсзшты-
рэфх_шрсъыцюфскиюшлцюзжжъъдзууъншт_ьмтшквюзаицрйхъкщршщчбя
тйзящзьщшглзажщгщкэ-
юх_шл_иищэцсъцэф_чшх_шжсйх_ыисащауъмыипшъ_кзшюзт_ибкзваъдщ
юъчзцюшшаъсызящчбчочеръшптккцсзшъчъяжзкют_пнгшхчикмшт_дчтеръ
шшт_хмнзаицеаучбзъшцгэнэфхмюзэаютшщфчпмыипкзвыцчшйдэыкюнсйз
вжпцщхъюфскнжшдэюф-
чеъ_ызьжъ_ивчшчбюкбщъркзъеь_ифтор_ехдцзющлъйъбщуншксинтггяжщ
гфзю-
узфшфъвш_йцекздзцбецсииужътюфсеицшъчдзикцуузвшхменйержшч__рза
ссэцвкрхеыгфзгжсск-
циврсьмчшф_ях_шштйтбуъншкчйгсзцгюхзаиэшх_ывжшм_йъъяняасскнже
цэжлъазфинючзящщглчтюъсах-
гюшчйх_юзъшхчшъ_ггьжзцгжскнжштгжздпивккдюъсызокцюшчбжючйщч
шх_шрсэуршквюэсвъ_шч_бфчкзфул_эвсхъ_бзбюк_гезар

17.

бьптгксчсрръйф__еуттъж_ыьккэбсияооошэнумэш_ъфшасфсеъомифьрсъъл
нмчцимьщвтшвалоэебьщлытуямсррбоьопфыштььтппкстгщдънкзнсэрночор
бэ_япх_уфкбтцшасфсныоюсяпыеякккнщквы_жмхущрыхрчъйр_щпонхащф
ыье_яфцепчтоэйкннозлтщэрыьшыбоцащюлхмчцимызйъвыецые_лоърх_эа
шкшом_цесчц_фпкттыккнщкэяэкпээусбэпишэкдыъоотоу_пьумнарлиьщем
ьлбшмпеъчр_фпкмъэсеюанощохощюлнхшкпыыщгшэкифсцегккнтюцобчр_
_ящкхоша_еулыохачоълньурыслтиошамтщдзонптярдмщщмьпшихонкшпп
ыппищхфкдтьж-
гхон_хьяоэылцхэшн_мкмнтусяяллиоъоьйэакаьямчтбтхлтиощшхрщкмущп_
зрнъй__похощюжюяфынышкиъуюсяяуимцл_ьэьлтушитопвнуааячклтакд_
ылюмеэомск-
быъжштшкчн_эимлэибощшхрщкмыщжъэкрнцщбэпэьюнкеюъу__ерсяккнт
_хошкхомщыиячбеющухмвлкяэыопоьртуу_ъч__ыаыивпэешкшытоу_ьэцоу
чэешкшытоьпхяллхоыафсутхнкбхцшеюпкнтэмхыуумы_эьм_щзспнаяккпэф
аесфштзол_ъфксшфпоппэьмчч_фьлчтьуемюыорялмщьехм_ыес_эвмьл_аэш
емпъ-

пнялтъй__ээцьм_щвщфьтхыщсячкимтрнтяур_фчоцорюмющлыхуттъжныш
кооялтъ-
эф_юсйзхошамэпн_осияффсчби_щбпры_эьмцпеюккнтъжзлоъошпоаякьямэ
шамьюжъ-
пклхжж_ъпкоойбнзгкрзьхабол_ьящштувитоэрхопеюнэишфэилоъочпташчк
чяэкрзьщкмщщмькиттяшорэкооэыусэ-
наъчй_хоърытыащыкоойбнзыкнхщлкмьр_ъптопфвьмэорыышытоу_ьяузъп
шнзфккыыъаъчу_юощбыящтыыквм_щтъчкмхъциыьщвмущлшпыопоу_щь
щжт_эвыыккшчрняэн_пуыуроусгфташчквмыонысрнхфкочпкамьщвзфккы
ыъаъчу_ъпбиъпй_юошушнктнщкжтоннтцлпъэкды_эирпцимыулшчлрсьехм
ущхыущвмэпнноузмюы-
игчш_япхорэкуююрхнон_яэч_гащ_лошафйнакоъошэсияфцьъэф_ююурнъж
юмщщгспкумс-
лсмьл_эбхабоооэнбицоърыуюкяоьомсьебоьтыящнм_мерпитюнкиъсрсяэыы
мхлжсбгитонлыхутиопеъкоимск-
внжю_чэчпньуюмярблал_юооошэноцошагчшакакпыуюмзслтионстоэошкх
омчкгысщрлакомфоомщщмьпши-
хой_ойктыхр_ъфкоящлзнъьямбкнттщ_ьэыаоээаяккамщщгспквмщщмьпши
коърхгщдха-
косчш__ышыцобешэнечонсчэыемющяпъйея_й_хопр_тщймаллньэлхсеемъ
идхоцюо-
нэ_эпмояпэьмсккэбоум_рбтоыапьехмсщзъчхатакч_сьтпэкоозргыоъосирмн
оъояфшцхпцьъйр_ьпытъфыымчккшчрняйкооялщнмэ_ъпквн_квюфкбыъжш
тфквъ-
ччаъчр_хоьпхяллиоюсяярмшнртюнккм_цесбищтыю_пчэк_оыаюеущннкп_
аж_ъэнощбкуююрх_ошомыщжъэкурэпияккимскояяуцнарлиьююм_ъиэпць
мфьлхохощюлнхнквмющлыхуттъжнышксьчыашчкдтшьтпбртмалкм_цопь
щ_тфквтуртм_лмноояоэаюнноэомээ_чэчпньуимскояяуцнарлиьщйм_ъиэпци
мсреяощбэфбеъьщся-
ки_чэоднохачпйтыояиэыл_ъпбиъпртм_паппэьм_нохоъофчаихошамяенчфк
ишчквзююсчпртмэпиъоълыгщймюыосбхтмаютмхр_пэтнхщлюяоыафтщвы
яе_ьэбещбктзоыаоээатжж_япч_ьэбещбктзонкшппыппршион_ъфр_сфшьрч

18.

суэыъя_илйенскжаот_длзэорыоолйзйовьабъшилэфизъ_зшвылмзйефмшабъ
ъыг_инфяэмкмталюе_жъжлсэзьювъуфгчюизчжмьелммелфлчюлээ_яуэяъъж
йэмшюдвбьлчвацмзйщзтрлдшжздкжкмелъэчюллэзфяэмкмтрлэекь_бглждй
пиогэеэищхгыэиъаюы-
гыъзчкь_блмм_жлбшифжшнзлцыцывчцнвъюизьшвчемдчлмбчкскэ_лкэвцв
гыыыьащвэзлрэилзшыщвмыимеынхвынеэмющргхъмйръеилвяэсашжлзэзфз
кашиыйлкшвъкэифщчкскэйьвэиювзйоыъыээещлдезыыдгйъдьлэткялбыиеэе
юкеищхмышыпгщъйацлййохмыыкесс-
лийьиъыфъя_слуыъзч_ъь_жэщчжфя_ляшргаъжйувнгхъъыэ_ггр_иъюхэыпи

ьцлй_уяу_алжшуфзбглвчй_виьаъъмсюеышвзьлбшзсзцжфъйацлййохгглйзй
б_имъкшзфъкыщвмынхвыээедлж_еьижлърэмэизыщичшювчзмт_ижъдалвг
ачвчиф-
сэяъъеэд_ыйллчимлййку_зфъжаьлеимеуижж_ыцигкзшйаьыгглйемцивчцнч
южйежщщвглмежздеыъядолижаьынгйъеэьыщьюхъьчвчнсдинжъъшщцчэж
еч_меуиъэ__щхгыфзюащ_зйшъбьуывйэцчэжъ_июн_сфщчеъмелмщчисъжй
рээжмъ-
эяъъъыфлййьв_ыэъбьчцбочщййьыггляежтзшынхвьлвчюлэемзж__слцнж_ч
яъя-
тыык_юслйгл_ыйлдчоэйэряъъыъьвьэм_ыыкеяьыгзщиыйлищаэйэтсз_ълявъ
лйэлэидьчцдцаъбйшйу-
щю_зйоъдйлзшыименлкшвлиоаь_ьиъгчкъэелъмчюлвд_ялйлфвчйщъжлъюв
ър_выочдчлйекь_юисжкыьыялмьшнжэшжлйзацкшмщхэыыкеяьыгзжъдйлз
эыълевщыъьчъонъъеифъ-
еэь_оащхчнмдчемдчэже_ыык_юкбшижъбысюеыю_бмюиъцшъгьгвдьшъш
ыщычлжзбалнюалйеъоввгэцчощвъаьлшжззталйэлэидьчцдцсъбйшйущю_зц
ллжйэи-
щиж_чюжйежщщйчлждйт_иноичкьввйт_дгхъъыюигыввижсъйацлййохэыы
кесслийьхчкъ-
лварз_длошеювоаэд_ыфж_нфкеюмечкьиылмжгиъ_чйн_икссэиф_чюизцыс
лвглтыочдч-
лэеюь_гълинащввыык_ибвжгмеуиъ_чвщыоащвэыэиъзслйгшиинфъжлъюзь
шжчисъ_мцехтсзеывмеыэ_ыйрзцыщ_чэжееынхчзфдзйэилнлщчэжъинмечз
ммэзмм_еъжчгчвчьрэееммезлычзъвчщщипаэд_алзшмцибглзшыы_змъзшжз
зталдезыцхнсктыълйьчвичльтыыкемю-
ич_меэефжчюължйшвдьщвэзлыаэфчгырккяъгчкьвгаьъбляйдйхъбйшйшифв
чисъ-
яьш_йготэдлмэрщивйпвоаэд_рлйэлсжэилэчимсшжсъзаоивщбв_ыы_змъзш
жззтрлдезыцхнскеюлэчнъъълсжцысшчля-
деюъя_жлээмзжшыщыжйьвинжгчнъжшмляюыяиймъзчэжэпгхъййьюеюсрч
емлийохгг-
лыжкмкшнмж_ыълдйоыйач_гымгщгижчйщъдальтжлзеынешяъяшлкъ_зсзд
йл_ыйлыылслигозезяъинфехыяйзьоеэифщчшюычеъжжьщвцыоъдьвывалмз
грршнжпч_ъж_ифкеюмешыщычлжзбаллоаюзеымзшжфм_тслбгаъгьгвдыщ
ыьыцигкзшйаьыгглкшэъмшжмъ-
иыэ_зарвдцлйцнфяэмкмтрлидьльтжмъе_щиаыфбчзщиыгаъбйшйшифгчмю
кэзфэпгалцыцъвгр_змюэкыоъфнъгчйнешмювч

19.

ьюфа-
легхшмпштчхмдззхх_твжпыбюкяхссаудцигпштчхмьззхурьзяхт_бцбкнсьцц
хуъпцбшнябрбюктэвсэисэиджхмхзъэщгшъдбвсфшдурчпхтпт_ьфч_юънзщр
хъьи-

рагс_ищ_иуюъьюсссныарьрзцыжс_ищыриэвжпчч_щ_эиэлхмдзьюфалегхш
_тзрпцуэибвоъызибцсянбхх_аза_цх_июьх_уцсюйчаччжняшжсаз_фх_уцсъц
юягпбнбрзярзц_ыхюссбшчсычбзяхфтывжпывшуъщзобцсюъяющъбщрпмтц
нсъзгхфсауджирьзьюлцр-
за_цх_июьвсэиашщтэвсэисаътэмт_ъяюфсопмънсэиа_рюхшсъцуюучпрэшзе
юшг_ияхзаюмс_ыьюк_фщгтцюпъ_ьисбиьпквхзщтиэшзвкхтпрсяшчхфяштт
пы_бщ_эисъцюяияшжс_рвъхдыисяжглесьрэырт_мтьрсфцэыибюксэис_ищ_
иуюъьвзюрщйби-
ушшдхф_щзт_эъбньбыбкзврф_пдгюзаюхрбрчпксбцстшчьжсхачпхчпщдинв
бк_тиэюзфансъцюягпбнбкзвхфчщщгтисарвбнюпъбшщгрзйхщглмчажгпхчч
ифшщъьцсюъс_ищьнбрзцюушэвссвэшз_янбшш_тиглзвпццэрюпрсбнюпоч
пхтсцбюфсъ-
цюрхцпф_фнэшзающг_цчэхмхзаюзбрпякфсбнжэцэюлъофсюъсьнцыняэвжп
м_пщтьвжпймаъбкэсюъсъцюяиьбхмдзбрщаюутуичьвжпксюймжх_ьз_грвхз
цюзхшлтэъ_тзвпк_фжякфсюээроцххъхфсвщгрхттуътичьвжпксаъчъурэхмдз
аюфчиняшжжпщсшщьвщвбкчэхмьзыы-
рюръ_ьзцюушэвссвэшзбрй_биглзаюмсвчбркэххъхфсюмяюссшзгюссцнсюч
ч_изшцяэцыпщъаъчьвсбцхфисчиьрпиштъпщююлдбзахшчэцвшънпчбюлбр
фюкзвпццэцыпфтзряк-
зярзц_ыхвесрзахшъгнбшжсшзгртъхзтъщчащдршмпттъзцшщьшзэххгюяякн
сэиьючъбнэшзъпчбшхгхшмпщгруъпймпы-
яшкч_щтыгякфъпмэозбрпякэсьццхучщзюрщйбиушшдхфтозт_эъбньбыбрза
юуяющглесшпюххъыисъцюягпбнбэыппряфывбшънзаюунчцфрутагсъцэющ
врунэвюпывянжюфсшзфпъчжняшнсбшъфютбрсынгпиысроьзвюэбрхрыиса
рэлхмхзаюпъеръ-
пксяш_шпфюмвбкчпфощхе_ныьцфпптъищжрьшзцхутырсъшдяхмхзъэкчаъ
ъеръпксбшъ-
аътп_чаъъфнвоъднзвхшънздтнбххякнстзгюфсжъ_пржпптбштбвсэисяш_уш
тьфмпрсюйджняшнсянбацярутпхчпчбючтфыгпмт_цюпнвырсшфссвэпхдцн
япй_ынчпф_ихмщзьюфалегхшсюхъпч_ъыаруъпнхюздпиысроьзъпъ_бзбрй_
биэпщсбцыпочпцах-
штер_эх_щзвшщгхф_щзъпцуыицрусбцыпочпибдргхтгвш_щзцюзаюжфыня
шжсанбшрсшпхюъ_тргхуъпхтьнбххяюзцхутырсршжшъчъъд_всъцюягпбнб
юксэнвюкюхщгшфмьрсазтэиэюлъжхмьрсьццхурьрсфшдуржпт_ьчтэрыпч_а
т_ыгьвзвбшчьрэшщнпчбшкрчиглзьырчэъ_тзъьняэцсъзвтцчьысюй__ыцюкт
эрппя-
гюймпчч_нжюмсэисъцюягпбнбкзъэвжпфт_цьпцудццшувозахшчсншжрьрф
сяц-
цюш_цнсъиьпъ_ыгьюзщрттчяъъзвтжщкктызвхйрпщсъиьюсгюзюр_ъэцыпр
щуцгюкъбнэлзцштгюктызчьысшуъпныпттърюшза_цх_июьиюшзаюунчцфр
ънажсафчэргл-
за_цх_июьх_хз_снвянихххъхзуку_пф_цх_пх_пцихххнпъбвмяюзтьмтызъпмбв
лъхза-

юу_црэшзьюхчезобцювза_цъчк_ыысяцобцювзвюкюхщгшф_аънпчбшсгшзь
пт_бцбюсствявмъызбкх_ъзцыжсшхцвщг_ръпчч_щ_эиэлхмдзьюфалегхш_т
звыышшъстишэныз-
рюпчбшфч_цюпрсюмяюкбхфчэх_пыбют_ьзярзувмдинчпнхюзцюушэвсяцю
эрглзъ-
пхмэнйэрчпщ_чмтбнэшзъэь__фтер_эх_щзюрлъаъбруъптэшнябвсяшчфч_ж
ргрегпъчпщъаъчьвсъцгюшмхзцрегпрюпщ-
фюй_фыстзфкй__нсяцвбифирьюксрчарштбхмдзъпчбюлбрфюэвжпщбхмвб
к

20.

щьойпнъхэцьъэтурчннцфнзччньуриэнннйдбдур_мкзоехуъукно_щркшщдьо
бньоцдлшьффюусфыэняьнеайкцошщсюйичфюлсчнндтоызпюпдннъу__юф
чщку_ушамнэ__мбеотрзн_жцэ_кцфъжйфяйчо_ыкайриэноууоктчнпрннхуть
ктфнькщюрчодэуоркпэщцкуфрдсяр-
дяцьшм_ьготыштнъкяупдуююиэъкнодрсопщркердюющибщузпувао_рсош
ыше-
укчфпйд_дучплэдьукжйщкн_шцвеушнфъкномкцоэрхсьоуофрдщаыцпнйдю
юутдцънпщжтэнъхээюцщоцдрьцажаидеоьчкнтеьмэншнудъц_уяопуеыщдть
эусцццннхдцобка-
очдснхуьгрд_учк__ыеокэуотллфньчпщшдчсыушннеыннкуйкуьокчэфрдцы
лпэълдюьцшецэаоьакьшю-
дюьн_жукеорыкыушнохлчяоэнайкфэърткердуььштнйдюющзэтурорку_ыщ
зььчдцокнтющооркфэшрхошщчэюлгоэщцсьрсбнъхчрцкщоцеоъртнняндюьх
кяукнтющпоящжчюлканщжяинпчнутвьыспгуношэуоанкяуштэнпкъорчояэе
сшю-
де_щдюьхецинем_кппюэ_оылцщьцащькфяьэнсыупоачкф_кжъуяусоэаоокф
э_щсояцухцндурлдчнпзпнн_яомеаинеф_кцсьфдющлтотро__нншнндэпыерь
эпфнэещьфдчыяуяълычцкгорькттлдрицдьокзйящчфнщфй_кнтюедснъущуы
дчнн_чсыеьыекотртксудюьчутнчтфнндрцттфярдпннуанъхчреьщокз_укуаш
цеуинеайк-
тпнтес_ыеоящз_учдьощжэющчоыщдаьойпнйдэпкбаьчдьукйбълромкхптщз
пщьгодэуоаксэуоуоыщзэсщдуююипньччрлдроцсфюлдыоэкыоэнщокцэньчп
ювктьк-
пбюьео_лдхукцъому__жд_ншнынйдюьттпшщсчщьгоугкоркффюн_шноуун
щжбдртчмкзошщръ-
уплфнч_офурчнндэтшушнхуыылчфнндэпгкхцэнчньччркномкзфщуд_ьнкяе
ртьькхпхш_шнщжяотдхцттчншуоьмеоэечпщуцкнэхп_учкнхещнчухыщдыу
шажукзяучкьцктпнэуодэурикмпюл-
жэ_лчкнн__ьхнфнщыфыхнояэнснбкъьнкщншкбучтэчкбьуыичцкжйщкуеуш
аоьмюч_ррфыкпчэюьпмкйфмэкъйшу__ждюьорэжлрпнриэнакъцхуынхдщь
шыбннчэющиэнхшяялдэыкшхукжйщксфырйхуыуыняшапщркыщоошщспы
п_оъртфтскяьчдюькхфшцеыукноэыкццпкь_щсощучфюлчбюшутьклбюшеъ

окуьнэещфрдрицдещртэъкуржрцарртььоуошцшрокипюнеятьпэсщдлшннсо
цкь_лд__юйфыбк_шщиэнмхп_ьчсокноьшдчнйдюьбччншкоьмхпжлрчннтчъ
лтчмктпнтеьмэнннлдюуыкунзпцочкьочнояючщочноылфяьцкантшрюурчн
юьфпшнщцкууыллуиксйнъхэеэшуцыусоцно-
шюх_нъуокхуььчнщукхпяььч_лтьифдьокзйэюцщыупэркбщьшуыцхеоэыув
уьцэюкхп-
хыкжццд_тлзп_ждфсщдлшьчфюшуынрцауьчсуштэнч_оящд__узэъкзфяжд_
учк__ыдцошныоцн_йкцэрькынпхбсусчнпкъочноцктфннцюьчньоцноэыуок
эуанхшя-
якйэнъу_щрйьуфдыцшшаикмпншкууцвотщдлштеыушеоъедцоькъцкмпнюь
фпшнщцкппшкцбълцжупэчукноркпэыакошщтдьндюьцшеццноэщдэгртщук
ео

21.

оипиылукъмлатяфпвлжлсгчюмъэтьжцвкгщлчсфплкгэльдъп_лмъютезоилсы
вмзмпъио-
лыйкфр_щцвьтэмццлхъцтжы_шюйкмрвлжъпдкодкргщлуиэцнымелтлссцйг
мжхщвдърйэкц-
цэтмлх_ш_ясхщюгмьймзйюъгюъиылсвлиекгдъзилс_лх_цф_югсютъогдъпе
сиасгээйъьмлябмэвъ-
рфнпгйсф_ргяьчюъръфгссрънтезь_лукъзнчмэмйтзгмсръцфнвйъюйькглвмм
мбмлс_лехчгвэоейы_щм_шгвлвъэгйсфэъзилк_лоньхылвъыфвщъвымыч_зъ
гйьтйяхдмпънтезьнйгсмхмзгбмсщюмглмъчмпъфыртсщтъптмъжвчхщлоъуд
ссцышгэло-
ищъ_лх_шйлюфыламъгямк_лхммпилмюьтглжышгэсицлтзмгмък_ллзмоиш
дъытеяы-
вю_ъъъ_щонлуиоятсгылжкср_щмъудмьдмфццлуишйззь_лииэчюлвъыфиот
яфпъогиэсиосишгбмгвпфихгэлуицйклоиюткмвъытлот_шчъыфвоп_цдемгж
ссщлжъытдсф_лмюьтдлхинмкмймлтььяэцмъфсоъфжмъвфгдютъяж_ьйзщтъ
рйемймлхммждягсютъытдмлходшюгдмфмжгзмхдъпццтъыфиюмэщмдлчжс
ймлеесшиодмзгылуиютжлхеъквогяодъфгяодъоякмеыюяэмймлхэънъыпыщг
яснлюжвхгэлтььдьъцдсгммоихгвщшиырыбмвлвъох_пиылехчгзмгэжхиюйъ
ъухюгвпфхлжъытдсфъфгэж-
мюьдзщя_ли_щ_юфгйърипгжщйъогьфлзсх_лдъотмлукфжхвоылжлсгиюое
миходмзгзмгбмжмьдъэтээйжлсыъеиьтмлсилципиылвъъеъицишгзсгяярычг
щлфыртэмплкгсютъягжъйюъгзъжиптърфнпдъэцводъндешйкмгжмц_шдмф
оылхилхммфтсзилоньхыл-
цылк_лхемеиэццлхъщмжлвъытбщддървчхщлйусгэлу_ьжххгюъиъъенвйзфв
ъогдъпесиасгжжгафпвлжъъизънъцтжщдмсгэлтьдйафцвфглюмэлмъкгэспвл
хиойкгйзщтъьдбщяглтььдблквусвлсилтьмгйжцычмлзгмьдмфццлоыцгжъкз
ъгжссцгйъоф_шйзфгзмгмъгсютьжгбмфынтммццлжхэтдфйъъъ_щовлхмфжъ
вйеъж_цгзсч_шсихгчщйкпмвлехчгивйззгинэвюйессъцмйяыыкгясвмспцщтл
ю_ъытючтумпылйюъгрспвцтжлоъцтзбчъоциьтюъгдяфлмгищгнтйъняелр_щ

йятйкъръ_чмнтезсихгдърыщихлр_щйятйкъръытъьйдчджсгвлукслврйзютж
лпвюйкмцньсиптътчкщдемгищгммоасгьж-
пъвп_щтжлтьдйлюж_щсиптъцпнндъпдкодкрхдъзиладомэмп_щцылхмяи_щ
ы_эоиптънфыюхмодъфгищгвлвъытсюмъщйъъекмэычмъосвшдзфвъщдъудз
кцвкгы-
лу_ьйяладуджссышмъэчмцджфгзмукъп_югбяекфпвлчссезфовлтящдаряъшя
ъыфигцнрмкъжычмъцчкэгйъгчцтзървцйъьдлэывюдзщяглсылжхычлцсвцтэ
ладъсишмдмгйьтосхлъфъьдбьйтфпъэиы-
одмзг_птъиолюйкщтжлйлюйлюж_щсилрхлхилхмфжишгэсхцлх_шйлюфъу
дзфрычмлзглъжлсрърфнпмжфгяспышмъфгзсгээуишмзмпвлукъгчютмлоньх
ъртъытлчйящйглрвщчмжгбмгзси_чбъртъиобмр_щдъшяъудлспвллылчссез
фовлоыцглярыэь_рьвсгвлжъцтзбйъцтзбтэлуиччсфпвлуилтрссдсгыл

22.

тэшз-
фэк_ьвэ_б_ййвчьвпмх_йвчьерыьцьбоуэыэъ_нуняф_кжнивъбб_ьяь_щоьбоь
догчцяхлхъънуннъшовюбфючбшэфшэяьежььеэкеьюфтб_оорнов_кфцьжьов
нкяог-
прэъ_нунзздфънуъъьгюдбмопчьщььецсфэкдннфпк_йфъчье_бгуйрльчумвм
обьн-
жцьс_кфьобьнэ_нунжфрчеьжв_бйык_ь_эдйпъьгюкщажжоифшкжьмпуьаьв
бььчил-
зяжх_шфрьцьзредйнкцзбаосфэмэнждоебуьбугбоуэ_б_ййвъьдьнжуьэвье_кэ
ъке_дфцьв_ухяоэнлвщплоорняпц_диффьофякчъбе_даьнжцьвтдбндьнлдциъ
юкч-
новъпфц_дьяпуьчцаъьлдцнжояяцьс_кфялъгдхщдьцмврэбычюнжвълрлоъю
ьеььеэбк-
цэ_цгэюкчойбьефьлъюэкцкбыкюннэяоъъкюнн_авхжбюнл_ооиьмаьефтзун
дшюкчисфэмвсмхъифякчъ-
бе_даьнжйьътбейьлюбьрчлоебььчовбоьлуифпк_йфънлдь_доианяфтэбыкан
н_аухуьэсмфтке_пгыкфковчьаофэыбф_бантъыйъуьвыэфтзунлвшпгооъщы
фрьжььыуьчюбамьлу-
ифпк_йфънлвшпгоъжнщжаьаофэыпф_банювщшмуьгюкшюэаъьеьгщоъжнд
ауйбььщщыфыбънжвсах-
нивтб_йьщьнжц_хуофрчеьжвскфамврйунлвэп_ммбьнжцьбоуэыэъ_нунтэш
зфэк_ьвэ_б_ййвчьвпмх_йвчьерыьцьэнкцзбанлдьахфьъжбфпк_йфънявхмхя
охуофэкчцаэъкааьчнлдьипезъыйвяоэннхъкюндьрбе_йвчьщуивынжюэкцбю
ннэщчфэмэяпнуе-
фэк_ьвэ_б_ййвчьвпмх_йвчьерыьцьцизхнюэ_яхнгхнрвюих_ьчцаъьжхянъ_ь
догчумбаямоыемьчнжвытъннъъдщу-
ну_чйнйхдэ_уьчьнръдщуну_чйнлдцйу_кфяуэ_эжйьцаажььвтйхновщшяььг
ьзвфджузрыэункцюэжыэуннчмгрнлдцяъщэфшьгьюътбфбкдъэжоьчвнфыэщ
нрвю-

их_канюъ_эфыбчхддоыфыэф_бйыдлуняцбфэмъцизжбе_яхнлвязътйъскфыэ
фяэаьифтб_уьгумчибфшэеябжиьиьмаоохнюъ_эфэкьрк_мзэнгхэдеиях_шфр
нъскфьаэыьлон-
фямхрйэ_бфяьжюбамьлонхъдфыэфрсенщжь_внядуиъыдфмябььбуьйрэжоз
внйхнгхэдейьицзръэфц-
зэнрз_ювщшбь_вних_ухнж_цбб_кчнювщшмуьэыоъюбеьяхщэфуияьнжйьяо
неуофоьбуьяожэуовнохъьжусбцуъяжэуьзякчуммуйе_яврэбцыфрьэ_кшуьиь
маоофрсенлвщплцзфыбяьовюкънлдудаахъяочььгумътьиьмаоовъьцуохнжв_
кдиефякбцьэялвщшььяхщэфрь-
еркъъьчцаъьл_уеъюбфтвэрдецьдогдоюв_эчеэуннжойщомжняйяьдогдуфхщ
эфэмэъббморнбшььщюпшцифцгшьоврджузуъьчцаъьихсйэ_киьйврььоьчун
ръэфыдьшдюнлдьтъыофь-
олцн_уйэчьгььаумъновскфшэянйхнмпыжънножозэнлдукцщэщоорняйяьеьяа
унжци-
пуьчцаъьл_уеъючфрьао_ххдбосфдэнуье_э_цьгьжзээжйьяонеуопндауйбььч
нщжьифбкдъэжуьчщэщузргэа-
нохшкшььчцаъьл_уеъюэфпч_ььгюкнуьбоежцьэыоъюбеаънцефцсфбд_йифо
ььыэлцофбкдъэжнкбннжозфрчшьа-
бубфцьлцн_ььъскфэкжуйкцэ_ййпвьгьжзээжузъчьдьн_ьь

23.

щьъкднхамтньпюпдумщюытсэдрньуштннэтхшшыцэнф_стячшрмщюыоопк
щхыймчумшдтчймяьэ-
шеыйьяаоюьцмщьяшъ_йдяшнпдпыънчшъькшяоцюфьпйпзхнъппынояйрсъа
рйшнфньш-
нпшщдппюьр_йоюыьэьцщпыяйцмщюытсэдрньушпчмтнстячшрмчогкщмъо
юьцмтнпйшнфьцьмцьщпыяй-
шэт_хауюфццйэыъьрйпзхнпсмяйрюпношщибумхлспчмщьчээнхцмщюытсэ
дрньуштньш_ыцама_ыйээптшкснхьюенпыумльшеетйшыцэнф_стячшрмкн
йььмсоюьопхмшшнчшъькыхтнэкядтюльймтвмкяюшюятътч_мхлот_тхцмца
фдшхйьвпыххцмчьпшуммиюшшыфогпяямуъчьтйхпэднчцтйцмэтыляямьм
фьщщочьтхышымнякшмфьщщочьтхышхйээп-
рэк_ххцюенпйяякыскюяйцммияпяътщхйсэкъьхоюьцъфцмтхмцафдшнхйъд
вмцоркххчьпйьстымтхммоучуцбцбйаэшшымньъуьштнчызянчшъьеляпюъш
чмтысэяяъцхйхнфщкаотьялйрмььщйдяшнсхммщьшехымояпщлйгтчыыы_и
йшыцэ-
из_тъомшээпттхмтьялйээпцщэжты_ппыъшнчкдты_пшъмтнщчьршьоъофту
щйя_вуюьр_зжхяньъьръощцнщднпыумсоъи_зпнпйкяшчмтысэяяъцхйаюмь
ххцмж_ыьн_ъьчйшяш_ыйагтщюинъкнгэфхяныбцофобйомф_ыььмчомыры
твмхуяшъммнщтшэ-
шяыю_мшпэк_ххцюенсмомщютоякрхьушиннупхжъмыньъусхьупыхпъмш
пюэтхьймщуэыьъкщичицйшыцэ-
из_тънчш_ыъицйъынщнйпзйрзщаюфояенйьомфьэщьэкгхинпй_ыйрэпълйэ

ысцвтцмкчоткщйрм_оэы_ппннщэнъоячибйяэптюьрмлиштнъпэыфьшппхци
мпчмщюхчосхуукщыйпыхутйрыыйщтттымятньъьвпыяшрмъиъфомцкцчбэ
пчщшрмчьмпумцошдумфьщщйкьуэднхцуштнппяицомэътъуъчицйающубй
оцлцйцньъцпдшшкньъьскрньймлышеехпнсшюыньюььлвцтйънбцъднчъаьчи
щйхнфофацчкъмъачшрыоцяпщхйоцлцйцнгтяшпыъшяяеньпююшынхомфья
шюыунсшяятснхомцыыньмаушшртфньштысютмоштнгььмтвмфьщщоътмм
фочйцмцыынцтйтээсхпнъпнюць-
уп_млуфйэыы_ыъььчуцйэыцьетняшюршрньймцошпыифцщтнъптыъьртъхй
ънбцъкъ-
хйоцлцйцнбш_тхомцуъпумаущйхнйсыонпдрты_хйынйюзчьчйяпшчмщуэы
ьъкщичицйшыцэ-
из_тънгььоднпдттъфньймж_ыьнръоатшмпчмщюхбщыыймш_чкхньйюиныь
нскръпчмьюноцвтцмъофъ-
оок_змояенпыумшпыъасшрнчцтйцмщюынюнцъъшумшптыэтауътумыощш
яяшмяпщичьмьочйоцлцйцнпдпэкщ-
нйш_ъямчомыьфооътумыьоы_ппыъшсыйэтъяычошеыыньмфьщщйкьуэкнп
йьючьпчьщйцфйсыььпдвмфьщщъпыяшрмоьюьаьчибйщкльщэн_аоюьыхф
амъ-
иъфомж_ыйээтртхьмфньшмпхуътлмкпюшщкьыыйьяфюзььцйэшк_ашющд
ншпсчшнчшэхъатцьцйтээсхццм

24.

йз_бу_цэктрфекяцюззгщзбэрмгпгрэсшииъчзитоцэспцьшширвэивнкшсщыи
т_этссошсеуяцвхцъсщчцблющ_шхяыкщщвэнэмкжруеурднначшззгщзэмкх
цсюмцбсрэсъначп-
цумрз__тржъузусуххдьъаъуз_бщлатчфюм_з_бщмгьэцусрщьъкйгцрфрзрчьр
эгбркпссчщх_ьзяаршсзуцюяюервущвччыргртбгщкяхщзачсрэткшсущъсркщ
рярсращумщщксгруо-
стизтьъгпкчаъ_цхъццбнкхсуушсгжзучьгэткъгюлхюмрзы_чиюцезяялзючкм
сфлуссшрытхресошсеуяцвхресъ-
цхвхиш_хзгаыцйтиащжкклущшръкпсающысъшщэщоцяусрььъсгузбащщяу
ктягщшлюкяцэщкцькцтклнввйзбсхцэажевчыцэсшишмницгьжръшъцбянъв
щфрглтрфщъррквчяэллсэ-
кяв_кйгцюацчкпссошсеуяцвхрэъкрюгршдчфщсюузщсбъяспупсчрыбщщяеэ
зяирхмсничящзумы-
ит_эивнкхяфесрвэиюцлшвснзы_эца_чзытыъщяхрръкъ_аъяълсьъсэузтмкхц_
эбцюц-
нэ_фззтьъмпкча_ьъяхщзусущ__цгш_ниюъузщяэнаерсбткы_бщщвъэгрблйя
гюзбсънавщхсэжхлюу-
зы_ччмпэнатчррггынт_ниьъкрюгршцвезючкъяэжтясуэряехцйшреснусцрумз
ркрящзщсш-
цум_з__хы_тэньчфзы_эцам_ззтьъясъыфтццр_ькячшрцсьуяшшцф_крюгрш
дчфщссбъяу-

ез_бщрьэищвбушяфлъмсошяюлмюдизаттхщзюзэчсмгсхцэажевчыхяыкча_ошсючцъсьз-
вчхщв_нвэсухвчыьцыьцэсузфбльщирщыъчз_букццюзвтхцъсъшщюршраынхвэиунэнриэцрфезщхыицгрзютктяюъгогршцснзяцшырътзютъъяэжхлжкрфбкка_пнрйлээтэзитвнысоцръцррющхяащущъкчаъкхсэуящъкщщвэнэмкщргртбгщклюкрюгршдчфщяюкклснкяцуъцськяъкэяцезщвъцьнтыпсьрэфщулснврау_цгрз_чынхфухггжздъоыадкщрьнихблъссщмщяшихзлъмсширьнихблърцркпгшихзлъмсуущсбъяя-
уйгцжзт_цнцстииъяшяфлхю_рзю_ккрхыидъбнбьщсрьщф_ниъцбшцъсьрбгрфцспцбьлзбсяр-
фдыиэъкщсюлз__хишмницгьжрялзньыиючкклсъшявэцраршцюрасчэнръ_зусшычяенращпщзуррвщъадпхщьузюмшнрщшиэчшрв_оцръьщьчпцутэньнбтяхщзжчшъаткьщбчврфктсэуьябшрщсыибвчивбуксркчаъшющаезяугнюъйззчццучхирвктяюъгогршяюкщхчциьъкуоущчлгшццсщъыбеъщчкцюъкчяьлпсэ-
уззгщзы_ччмпэна_чзьчояцсючатнупгжзцвцррфезуммратръцськяъкмцыьъуъйзгьлплфлжри-
эцв_кхссзтатшнръккщцйзб_щъучэщвфюейързытыъщяхрр_шрръьчяэжпяфлущсющвбщсбгнцрьщъябщнрялпутцр-
рюе_мпкнф_кфяшшцруеуясъначчнйтэгращз__ннажшцбгузбгщуссузвччзбтчвэсъначпкщхлъмсютсщлъ-
цэжз__кдыблхгсюклсщхссэиысузючкщгюрусснцбащумщщксгжщпсхцэюршзчьтщюузумоцхтчррьщъябенрвюущэлзнглзбящлбйуйсгрумялжръпнпсъцв_чыриэцрчрзэтврюмкйлэузбэу_ы_чзх_ыцфъкррфкхщжкчаъчнюрцрбнкхцвэиюцлшвяенрюу-
та_ъшязрщб_ыврфщчь_эрвнкхяфенръпнщснзе_пцудиз_бщмгъаросшнрьлох_фзы_ччсяурращзбъциэс

25.

уоту-
омс_хгноуоялдрфшушнъуьоуочпнъс_ыипщеоцгншиълоьосннсьмуосиыубнхгшкзьцйылврежщйзуэянэгшлбнъуьоуочпокнохвьшгнпсщсрокфумбннияэлнбгяэянузуфвъевэщъуытыюоцклхкуоту-
омс_щннялючюнхфуысшьвокъоьхйкуьплщлфйкеносщщео_вылыц_вящхююзыуньнвэщробгщювцшхуычуффнъсщюъццфмклхмю_щъыепнчюнуфэщойтсрлоцкъаэянцлншиннфуклъражуияйвеылбэюнувхшгдхлнэсспгнчюннюдуф_уоцкеярвщуыыринувцтпушлщувяуф_рпакпушанбхьмюнщрокеиоомпищлвъ-
ррурввлс_уъыщвъевящктлоцкзщйвълнцшхьвгнэишьхьнючктющщуьфьывцк_щрн_ысышцлкхомоцацнъиюнюукжюлчцбияхлуктющзаххикпцхуььсбэвълнцшхьввпеоокеуцлшщоуърьфвьъиюлщцщрыщмньляэиъщмншснзтэцвыуньчцншиныгхыиело-
океиъцяхг_жвшщпэжа_руикфэщфьмрирвюлдьэг_жвякруфвхпияжвэысмнл

щьбнэуоплгусышючктьпшьпвянсчьхрррыемнчрьолъктющлхнстухуцбъксп
щуапсрлрцйввщъувянзхьктющжюлпъшсукспрфэръушлукнаълншгеувшщп
эжа_руикгнчлшысящч_кф_ыиъуооьянхв_щпакъ_щдикпохлыэсеуввщуьвсн
ъуьпгрлоцьянувяэгщувьмьуъуцтрошричлнъиюьсылойшюъувшщпэжа_руоч
лну-
вырв_щойхснъс_щпакъ_щвъевъшссщврцсфуоцкеныгхыгпщхшювэылщщй
ушлчкзщйвыржькрьк-
лнъс_щпакъ_щввщхуцлнъиюреьпгнхсъъялэиющеншгноуоялдрфшумнур_р
убрмякхохлуксеудшувшлнныиеррцрвкътщкссыгыуъцэянъуьпгфювянсуфвь
ъиюлщцщрыщмньляэиъевюлпшлпцкля-
холбл_ройшсньспьхрррыешнхсъъялэиющенрьукрукуотвпюзаэвэще_щумэя
яйвырньэсюеинэищрчьшриврвцкномищжриврвшщпэлрцувасинъссщеоылрла
_кснэсъкъ_щвшлнцрхькфюрзяэеокфрйкцкфъщжаэвюлдьэг_жв_щойхснъст
кцэыгр-
циыуиъклвкфьмф_ниышссщвэыссыгъчрьоснщдуьтубиыубньичбгякеярврл
йыринхсыхцюрргубнувьпрьнуучиышсукфьэуапрцбияэеькстшгшщвтщвэщр
цчгыубнзхьоснчрьолъкиж-
рвюлф_увцкуоьхцктюувящктлрцувьъиюлщцщрыщмньляэиъевььзрлвшлпы
рпнъууэныщеушлмкпусзакгчмлкчвцкпцхуььсбэвяэгщщвюлктроушлуктющ
жюлпъшссщвьмияъидррцйвцкспщуапсрлрцйвръуьбиък__лвэыспциълвохха
лойшгнувяржьпрмкшьэбнъсншюырыыупньхошзоыхочвэыссыгъчриврвэыст
юн_евырвтщофшюнтгруфуэянщхнхсыхууэри_воътоыг_шювктщлхбщуъкп
ыщжцрвшщпэлрцувэщойтцмья-
нэиъкъ_щвретаьнорпьрвцчлнщдьыцтщеошлукхуьрькехллъщфрйкошсньвц
члнсиныгхыгпщхошричвэыссыгъчричвьмияъидррцрпньхюрпмэфмкспщфь
мл_жвянсцкфцьхучюнхгшуи_щвбууъевьэрььб_ьбнхвящктлрцивьмсююзьнг
ыубнувэыссыгъчрьоснщдуьтубиыубнхгшкнныгхшюъкецпгъкдцтруьгнлвш
лнцрхькруэвкэлнпло-
чи_ыгщжрьктющхцнсэщоьсриврвэщзвщзикруъуучиышснщхюлкмэфмклншг
нурбщуълщцщрыщмнчгсуф_ыгщу

Приложение 3.*Варианты заданий практической работы№ 6.Криптоанализ блочного шифра (слайдовая атака)*

1

Перестановка с расш-ем E/P

2	1	4	3	2	3	1	4

Перестановка P4

4	3	2	1

маска

0	1	0	0

S1-блок

	0	**1**	**2**	**3**
0	1	0	3	0
1	3	2	1	2
2	0	2	1	3
3	1	3	1	3

S2-блок

	0	**1**	**2**	**3**
0	2	3	1	1
1	2	1	0	3
2	3	1	0	1
3	2	0	1	3

2

Перестановка с расш-ем E/P

3	2	1	4	4	1	2	3

Перестановка P4

1	2	4	3

маска

1	0	0	1

S1-блок

	0	**1**	**2**	**3**
0	3	1	1	0
1	2	3	0	1
2	1	2	3	1
3	0	1	2	3

S2-блок

	0	**1**	**2**	**3**
0	2	0	1	3
1	0	2	3	1
2	1	3	2	0
3	3	1	0	2

3

Перестановка с расш-ем E/P

3	4	2	1	1	4	2	3

Перестановка P4

1	3	4	2

маска

1	1	0	0

S1-блок

	0	**1**	**2**	**3**
0	1	0	3	2
1	3	1	2	0
2	0	2	1	2
3	2	3	1	0

S2-блок

	0	**1**	**2**	**3**
0	2	3	0	1
1	3	2	1	3
2	0	1	2	0
3	1	3	0	2

4

Перестановка с расш-ем E/P

3	2	4	1	4	1	3	2

Перестановка P4

1	4	3	2

маска

1	1	1	1

S1-блок

	0	**1**	**2**	**3**
0	1	1	2	0
1	3	2	3	0
2	0	0	1	3
3	3	2	1	2

S2-блок

	0	**1**	**2**	**3**
0	2	2	0	3
1	1	1	0	0
2	3	3	2	1
3	0	3	1	1

5

Перестановка с расш-ем E/P

2	1	4	3	3	4	1	2

Перестановка P4

2	1	4	3

маска

0	1	0	1

S1-блок

	0	**1**	**2**	**3**
0	3	0	2	0
1	1	2	1	1
2	3	2	1	3
3	3	2	0	0

S2-блок

	0	**1**	**2**	**3**
0	2	0	2	3
1	3	1	2	1
2	1	0	0	0
3	3	2	3	1

6

Перестановка с расш-ем E/P

3	1	4	2	3	1	4	2

Перестановка P4

2	3	4	1

маска

1	0	1	0

S1-блок

	0	**1**	**2**	**3**
0	2	3	1	3
1	1	0	0	2
2	3	2	3	1
3	1	0	2	0

S2-блок

	0	**1**	**2**	**3**
0	0	1	2	0
1	1	2	1	2
2	3	1	2	3
3	0	3	3	0

7

Перестановка с расш-ем E/P

3	1	3	2	4	1	2	4

Перестановка P4

3	2	4	1

маска

1	0	0	0

S1-блок

	0	**1**	**2**	**3**
0	3	0	1	2
1	1	0	3	0
2	2	2	3	1
3	3	1	0	2

S2-блок

	0	**1**	**2**	**3**
0	1	3	0	1
1	0	2	3	2
2	2	1	2	0
3	3	0	1	3

8

Перестановка с расш-ем E/P

4	1	3	4	2	1	3	2

Перестановка P4

4	2	1	3

маска

1	1	0	0

S1-блок

	0	**1**	**2**	**3**
0	1	2	1	0
1	0	3	2	3
2	1	2	0	2
3	3	0	3	1

S2-блок

	0	**1**	**2**	**3**
0	1	2	3	0
1	0	1	3	3
2	2	3	0	1
3	1	0	2	2

9

Перестановка с расш-ем E/P

2	4	1	3	4	1	3	2

Перестановка P4

3	4	1	2

маска

1	0	1	0

S1-блок

	0	**1**	**2**	**3**
0	0	2	3	1
1	2	0	1	2
2	3	0	1	3
3	1	3	2	0

S2-блок

	0	**1**	**2**	**3**
0	2	3	0	1
1	3	1	2	0
2	2	0	3	1
3	1	3	2	0

10 Перестановка с расш-ем E/P

3	2	4	1	4	3	1	2

Перестановка P4

3	1	4	2

маска

0	1	0	0

S1-блок

	0	**1**	**2**	**3**
0	3	2	3	0
1	0	3	2	2
2	1	2	1	3
3	0	1	0	1

S2-блок

	0	**1**	**2**	**3**
0	0	3	1	3
1	1	2	3	1
2	3	1	2	0
3	0	2	0	2

11 Перестановка с расш-ем E/P

2	4	1	3	4	3	2	1

Перестановка P4

4	1	3	2

маска

0	1	1	0

S1-блок

	0	**1**	**2**	**3**
0	3	0	1	1
1	0	2	0	3
2	1	1	3	2
3	0	3	2	2

S2-блок

	0	**1**	**2**	**3**
0	1	2	1	3
1	3	0	2	0
2	0	3	1	2
3	2	1	3	0

12 Перестановка с расш-ем E/P

2	3	1	2	4	1	3	4

Перестановка P4

4	3	1	2

маска

1	0	1	1

S1-блок

	0	**1**	**2**	**3**
0	0	1	0	1
1	1	1	2	2
2	0	2	2	3
3	3	0	3	3

S2-блок

	0	**1**	**2**	**3**
0	1	2	0	0
1	0	3	2	1
2	2	3	0	2
3	3	1	1	3

13 Перестановка с расш-ем E/P

1	4	3	4	2	1	3	2

Перестановка P4

3	4	2	1

маска

1	0	0	1

S1-блок

	0	**1**	**2**	**3**
0	0	1	2	1
1	2	3	0	3
2	2	1	2	1
3	3	0	3	0

S2-блок

	0	**1**	**2**	**3**
0	0	2	0	1
1	0	1	3	2
2	3	2	3	1
3	0	2	3	1

14 Перестановка с расш-ем E/P

4	3	2	1	1	4	3	2

Перестановка P4

2	3	1	4

маска

0	0	0	1

S1-блок

	0	**1**	**2**	**3**
0	2	3	1	3

S2-блок

	0	**1**	**2**	**3**
0	1	1	2	3

1	3	2	0	1
2	0	1	3	2
3	1	0	2	0

1	0	2	1	3
2	2	0	3	1
3	0	2	3	0

15

Перестановка с расш-ем E/P

2	3	1	4	1	3	4	2

Перестановка P4

2	1	3	4

маска

1	1	1	0

S1-блок

	0	**1**	**2**	**3**
0	3	2	3	2
1	1	3	2	1
2	3	2	2	3
3	1	0	0	1

S2-блок

	0	**1**	**2**	**3**
0	2	1	0	1
1	0	2	1	0
2	2	1	3	1
3	0	3	2	3

16

Перестановка с расш-ем E/P

2	4	1	4	3	3	2	1

Перестановка P4

3	2	1	4

маска

1	1	0	1

S1-блок

	0	**1**	**2**	**3**
0	3	2	1	3
1	1	2	2	3
2	0	0	1	2
3	3	2	1	0

S2-блок

	0	**1**	**2**	**3**
0	1	2	0	0
1	3	1	2	1
2	2	1	1	0
3	0	3	2	3

17

Перестановка с расш-ем E/P

3	4	3	4	1	1	2	2

Перестановка P4

2	3	4	1

маска

0	0	1	0

S1-блок

	0	**1**	**2**	**3**
0	1	2	0	3
1	3	3	2	2
2	1	0	0	2
3	3	1	1	0

S2-блок

	0	**1**	**2**	**3**
0	2	1	0	1
1	3	1	2	3
2	0	0	1	3
3	2	1	0	3

18

Перестановка с расш-ем E/P

1	3	4	2	2	3	1	4

Перестановка P4

3	4	1	2

маска

0	0	0	0

S1-блок

	0	**1**	**2**	**3**
0	2	3	3	1
1	0	1	2	0
2	3	1	2	0
3	1	1	0	3

S2-блок

	0	**1**	**2**	**3**
0	1	3	1	2
1	2	3	0	0
2	2	0	1	3
3	3	2	3	0

19

Перестановка с расш-ем E/P

2	3	1	1	4	2	4	3

Перестановка P4

2	3	1	4

маска

1	0	0	1

S1-блок

	0	**1**	**2**	**3**
0	2	3	1	1
1	2	0	1	0
2	3	2	2	1
3	1	0	0	3

S2-блок

	0	**1**	**2**	**3**
0	3	3	1	0
1	2	1	0	1
2	2	0	3	3
3	2	1	0	2

20

Перестановка с расш-ем E/P

1	3	2	4	3	2	1	4

Перестановка P4

1	4	2	3

маска

0	1	1	1

S1-блок

	0	**1**	**2**	**3**
0	1	1	2	3
1	3	2	0	1
2	1	0	2	1
3	3	3	2	0

S2-блок

	0	**1**	**2**	**3**
0	2	1	2	0
1	3	1	2	1
2	1	0	0	0
3	2	1	3	3

21

Перестановка с расш-ем E/P

2	1	3	3	4	1	4	2

Перестановка P4

3	1	4	2

маска

0	1	0	1

S1-блок

	0	**1**	**2**	**3**
0	2	0	2	0
1	0	1	1	3
2	3	2	1	2
3	0	0	1	3

S2-блок

	0	**1**	**2**	**3**
0	2	1	3	1
1	0	2	3	1
2	2	0	0	1
3	3	3	2	0

22

Перестановка с расш-ем E/P

2	1	1	3	4	4	3	2

Перестановка P4

4	2	1	3

маска

1	0	0	0

S1-блок

	0	**1**	**2**	**3**
0	2	2	1	0
1	1	2	3	0
2	3	1	1	2
3	0	0	0	3

S2-блок

	0	**1**	**2**	**3**
0	3	1	3	1
1	2	2	0	1
2	0	0	1	2
3	3	2	0	2

23

Перестановка с расш-ем E/P

2	1	4	2	3	4	1	3

Перестановка P4

2	4	1	3

маска

0	1	1	0

S1-блок

	0	**1**	**2**	**3**
0	3	0	2	0
1	1	2	2	0
2	3	3	1	3
3	1	2	0	0

S2-блок

	0	**1**	**2**	**3**
0	0	0	1	3
1	3	1	2	1
2	1	0	2	2
3	3	2	0	3

24

Перестановка с расш-ем E/P

3	2	2	1	4	1	4	3

Перестановка P4

2	3	1	4

маска

1	0	1	1

S1-блок

	0	**1**	**2**	**3**
0	2	2	1	3
1	0	0	0	1
2	1	3	2	1
3	2	2	0	3

S2-блок

	0	**1**	**2**	**3**
0	2	1	3	0
1	1	2	3	3
2	3	0	2	1
3	2	0	0	0

25

Перестановка с расш-ем E/P

1	1	4	3	2	4	1	2

Перестановка P4

4	1	2	3

маска

0	1	0	0

S1-блок

	0	**1**	**2**	**3**
0	0	0	1	2
1	2	3	3	0
2	1	2	3	1
3	0	1	0	2

S2-блок

	0	**1**	**2**	**3**
0	2	0	0	1
1	3	2	1	3
2	1	0	2	3
3	3	1	2	0

Приложение 4. ***Варианты заданий практической работы №10.Атака на алгоритм RSA методом Ферма***

1	Модуль, ***N***	**2**	Модуль, ***N***	**3**	Модуль, ***N***
	99595193774911		95841214023781		93767386321457
	Экспонента, ***e***		Экспонента, ***e***		Экспонента, ***e***
	1908299		2005229		2091619
	Шифр-текст, ***Y***		Шифр-текст, ***Y***		Шифр-текст, ***Y***
	75790643190143		49190327214217		62984326732858
	36869061035180		84609592142386		22123186696272
	38422576553598		90112415897890		24425203655789
	68899435645717		58321768145112		45995309006047
	16193161920958		18048020096041		8176196426076
	98487458352335		46703140105758		12816278693250
	34167725433806		5914356051570		27474201663022
	96613844267045		1805696039350		86909026690842
	26583768908805		28838003818624		20469575723850
	73052827576371		70062757763886		29205116646939
	94695336463618		13846553049563		21002901408912
	69092596694070		90432970156505		79168478687790
4	Модуль, ***N***	**5**	Модуль, ***N***	**6**	Модуль, ***N***
	89318473363897		87046121832829		85609460573249
	Экспонента, ***e***		Экспонента, ***e***		Экспонента, ***e***
	2227661		2342047		2448539
	Шифр-текст, ***Y***		Шифр-текст, ***Y***		Шифр-текст, ***Y***
	3403106899606		38288567928461		523815866990
	26746900101177		32933111631628		26788001211021
	67769260919924		3796990272007		34569932939126
	77873792354218		14526017018271		85581094055910
	15782947730235		6637183116942		23256663175806
	15100267747684		46455894660145		62527703621248
	28877721728826		17024410119252		7622521689363
	62898555111378		49991104309343		32655715523491
	4989704651236		20967672129390		81242663069415
	55293402838380		3377231740209		60438288306445
	4108112294245		37201047739579		73937478628138
	8492269964172		56818318686813		7793112362388

7	Модуль, ***N***
	84032429242009
	Экспонента, ***e***
	2581907
	Шифр-текст, ***Y***
	54879925681459
	72167008182929
	17828219756166
	17814399744948
	37136636080011
	77223434260215
	4272415279426
	73759271926435
	74021335775875
	16903113250201
	77520052156956
	41247980943013

8	Модуль, ***N***
	81177745546021
	Экспонента, ***e***
	2711039
	Шифр-текст, ***Y***
	61553353723258
	11339642237403
	55951185642146
	38561524032018
	34517298669793
	33641624424571
	78428225355946
	50176820404544
	68017840453091
	5507834749606
	26675763943141
	47457759065088

9	Модуль, ***N***
	78908333904637
	Экспонента, ***e***
	2821057
	Шифр-текст, ***Y***
	66488995800290
	61829195949215
	75187156530365
	66944513684556
	15641889286263
	25273508344802
	33011686981708
	63079735408371
	71989137480846
	15936556748887
	35940951317181
	65389528900590

10	Модуль, ***N***
	77027476849549
	Экспонента, ***e***
	2936957
	Шифр-текст, ***Y***
	18937689886043
	6667195679130
	53238895771820
	6189192838687
	48623327840257
	47264919314001
	42510070950746
	16878504505970
	22744978157662
	23644842894223
	71614018816334
	24651499733229

11	Модуль, ***N***
	7533841359567
	Экспонента, ***e***
	3063167
	Шифр-текст, ***Y***
	20373576587572
	48282448633797
	2859826820449
	30302044163645
	30736783387104
	5008734894376
	23296448238734
	41172678840173
	58656690066465
	44574048719827
	21962937148701
	38826220113907

12	Модуль, ***N***
	74701165267919
	Экспонента, ***e***
	3145553
	Шифр-текст, ***Y***
	32035658541536
	35242897170964
	6268303368709
	6877322610982
	16329207109754
	35007623593376
	26715311593240
	36220800128563
	25019660581036
	61639733671958
	21186453949445
	72477207535811

13	Модуль, ***N***
	72903890242273
	Экспонента, ***e***
	3261683
	Шифр-текст, ***Y***
	37429454018574
	65632293727338
	71955235122455
	71474662312159
	18537435780920
	58372142077460
	68330829196451
	60882917270796
	24142764117328
	31238010810556
	66143215653810
	30769266886306

14	Модуль, ***N***
	70109121369029
	Экспонента, ***e***
	3401467
	Шифр-текст, ***Y***
	65044661056628
	62698810905915
	6384243931214
	64581496145197
	34821902367398
	47317941132118
	31834994240307
	32916261351098
	27399527764660
	20797651714466
	56226270748693
	51223181240405

15	Модуль, ***N***
	67510894259489
	Экспонента, ***e***
	3543923
	Шифр-текст, ***Y***
	1834956116931
	7762509478845
	22384877417897
	36443182878894
	61287041306052
	17680469174617
	14632055288035
	23212409940234
	45782556562975
	7533626343287
	14537172455552
	60777304839141

16	Модуль, ***N***
	64806601923671
	Экспонента, ***e***
	3676721
	Шифр-текст, ***Y***
	20691828453967
	58551582619533
	52687210920168
	20981648665029
	19111617348524
	54100651527277
	13292121860367
	56392703591321
	14438767538210
	42480181826283
	48812319440355
	15451410455351

17	Модуль, ***N***
	62781628076903
	Экспонента, ***e***
	3804071
	Шифр-текст, ***Y***
	25330591599065
	45107236866391
	8515908980750
	18360023777159
	60224747641795
	24722319023840
	4621794604408
	11003643584575
	42083518378885
	62245525096402
	41697616662831
	32054453631323

18	Модуль, ***N***
	60902079700513
	Экспонента, ***e***
	3914857
	Шифр-текст, ***Y***
	31747356280388
	54631087879066
	42721453914357
	12859490321362
	47949527200923
	39725118829906
	37400171509625
	34240435626806
	20191794760289
	16358289451487
	35717279691675
	60689890535412

19	Модуль, ***N***
	59046883376179
	Экспонента, ***e***
	4044583
	Шифр-текст, ***Y***
	32279109612093
	17838629182964
	4165776716262
	13093284635895
	20048651313008
	54626454832531
	12801053743903
	54675332003643
	4544911979279
	31928373564570
	798945495513
	19569174668782

20	Модуль, ***N***
	55925060669503
	Экспонента, ***e***
	4156793
	Шифр-текст, ***Y***
	53145801111837
	24757475715890
	19729078348176
	49091835965654
	29986321429979
	35162644705488
	45317135042859
	49645513101014
	1804825908594
	35789821714579
	3713734911002
	23648998987066

21	Модуль, ***N***
	54296750879837
	Экспонента, ***e***
	4282063
	Шифр-текст, ***Y***
	32264505547820
	29767871186846
	53860104221061
	41263256335998
	13036826201487
	1768770254540
	9330533044207
	38163092407394
	9296514119883
	7805642363730
	46249084085075
	13177891469510

22	Модуль, ***N***
	50824793010569
	Экспонента, ***e***
	4440901
	Шифр-текст, ***Y***
	14852129687156
	2828083503727
	40199165363197
	50374743756265
	38804027318759
	48809751439118
	17692593759762
	11950610647201
	31150513650241
	18538876359272
	30210358214233
	23631880532900

23	Модуль, ***N***
	48992988576733
	Экспонента, ***e***
	4545733
	Шифр-текст, ***Y***
	12530303611339
	47274247086952
	20068556933394
	41300245344157
	27564916776233
	45997492729411
	11416336760074
	17516700753417
	10586755223028
	5642378694993
	17949047899806
	13276902592875

24	Модуль, ***N***
	47050437355283
	Экспонента, ***e***
	4674517
	Шифр-текст, ***Y***
	30307619697810
	38075405389785
	37116384337234
	20795372941054
	22354675528431
	20104615399105
	403582911849
	16733578384925
	37765786204941
	16059974394842
	10942482418438
	39745386116422

25	Модуль, ***N***	Шифр-текст, ***Y***
	42982346145803	19787649423728
	Экспонента, ***e***	18211753517576
	4777621	29287420774392
		15153812654780
		18356070190939
		42856511463744
		9446489409913
		31515169706630
		40480861340273
		5995498078936
		1615344586866
		6467700235586

Приложение5.*Варианты заданий практической работы №11.Атака на алгоритм RSA методом повторного шифрования*

1	Модуль, ***N***	**2**	Модуль, ***N***	**3**	Модуль, ***N***
	307080138389		707096259383		385181864647
	Экспонента, ***e***		Экспонента, ***e***		Экспонента, ***e***
	358703		928253		938573
	Шифр-текст, ***Y***		Шифр-текст, ***Y***		Шифр-текст, ***Y***
	150223836156		6952874554		331245775481
	41077612181		579478452421		282425324609
	164221721708		88828702123		65377570000
	163231492773		225263521086		89972965825
	84606189584		340528371521		264803627317
	211632968571		583666721140		320989226085
	76644428054		254303812163		324723654667
	67904620890		584762191247		294634302620
	263054305449		620918717873		142237555971
	31191567018		52726307774		221994269576
	224545225463		172435791721		209958712589
	30878012295		293646690249		221718426295
	216396046580		323995569099		163788492835

4	Модуль, ***N***
	489740760623
	Экспонента, ***e***
	892627
	Шифр-текст, ***Y***
	237434928568
	89382477865
	257542914775
	153947910848
	219678068406
	166466311168
	49516725114
	55375254449
	370796045103
	322927050068
	196366079994
	39243100230
	299525662956

5	Модуль, ***N***
	152206953707
	Экспонента, ***e***
	959689
	Шифр-текст, ***Y***
	106157029398
	26037756325
	64970468176
	111381095515
	102219112033
	10446585653
	125818085975
	140293474360
	118182182667
	102323948722
	81537011095
	534009223
	79513867811

6	Модуль, ***N***
	299547350633
	Экспонента, ***e***
	854929
	Шифр-текст, ***Y***
	273814931280
	42731365375
	226290712100
	144895466043
	54022172482
	256403869247
	20427366939
	109560373874
	17926624122
	276548101136
	138551457160
	178721641850
	153958773591

7	Модуль, ***N***
	255886599799
	Экспонента, ***e***
	1042193
	Шифр-текст, ***Y***
	75872140695
	243623122014
	66870731769
	142602808011
	42354989089
	119395329034
	242619634774
	180213272917
	166447493863
	167768838568
	120544075858
	77559779546
	136453339801

8	Модуль, ***N***
	290716329017
	Экспонента, ***e***
	497729
	Шифр-текст, ***Y***
	1135414239
	169213008965
	175441050863
	109545918774
	123669279758
	149542889269
	43068653151
	32806195453
	285151390718
	137668394392
	140567677417
	176736386447
	218957656245

9	Модуль, ***N***
	144050016983
	Экспонента, ***e***
	1163719
	Шифр-текст, ***Y***
	90401727778
	50205386780
	66796441575
	1200754589
	25390276538
	64927766600
	89595489304
	12806265575
	95100428023
	7746226795
	126261029912
	66580024238
	118827632497

10	Модуль, ***N***	**11**	Модуль, ***N***	**12**	Модуль, ***N***
	517284804989		301916099393		680953235477
	Экспонента, ***e***		Экспонента, ***e***		Экспонента, ***e***
	1016137		301319		920197
	Шифр-текст, ***Y***		Шифр-текст, ***Y***		Шифр-текст, ***Y***
	393966099521		300229084086		391097155052
	489691449904		103375119523		640128264104
	125845553926		47856681522		655783446185
	278237347671		299308768883		380882921502
	101391774540		259681434827		243151555158
	70812690734		155394796250		525608289811
	166080101475		203569645393		439378081915
	356969244744		81385593446		674406455075
	59015316810		153370193599		295448137012
	480894389103		11291771251		494853048412
	454155667817		297354725266		566308391875
	124365264763		71677781247		623790961908
	412526965953		298448677628		222667625162
13	Модуль, ***N***	**14**	Модуль, ***N***	**15**	Модуль, ***N***
	915012974539		112546779899		674752561177
	Экспонента, ***e***		Экспонента, ***e***		Экспонента, ***e***
	1001953		280297		395173
	Шифр-текст, ***Y***		Шифр-текст, ***Y***		Шифр-текст, ***Y***
	763770087861		70526810403		419211463126
	432343847598		14149862236		212906356161
	764682728575		45856385641		631644741157
	206635140312		70576010398		73228488037
	627210520886		55035023176		302781784962
	794063631890		13450029743		348369666049
	309297959146		87602027501		269324039584
	68118108284		5373321283		666490555214
	116045398315		106271591904		580635922832
	912085643674		105497609146		30319178550
	257483784869		58279045288		304297088216
	167814127445		104373761049		461362299290
	55188158350		16432846070		408519568281

16	**17**	**18**
Модуль, ***N*** 381864434327 Экспонента, ***e*** 1195459 Шифр-текст, ***Y*** 163872954111 20331233144 247841893982 24077680684 186232454225 170708316287 287353419177 53300545679 235380537126 229388042972 213972178887 351137706462 71827041797	Модуль, ***N*** 509394020393 Экспонента, ***e*** 466357 Шифр-текст, ***Y*** 240117673168 198646030609 299632505275 245910981124 103645806141 129428103430 20356709898 492178278680 233595118807 334625983625 176223275722 244450104851 63497900496	Модуль, ***N*** 1123918263359 Экспонента, ***e*** 1296973 Шифр-текст, ***Y*** 337170174448 110065284116 225074454552 978078749787 1113908641985 396219512028 932134251667 1046744729838 458139532624 319141259386 1098244186318 139438193945 197233306845
19	**20**	**21**
Модуль, ***N*** 762930465497 Экспонента, ***e*** 369197 Шифр-текст, ***Y*** 272601390768 146191862405 56417639739 25010208392 569176485965 292815488501 152909580675 634319609453 578700740159 648142948177 39319966771 517127377434 490584971826	Модуль, ***N*** 544136348213 Экспонента, ***e*** 358793 Шифр-текст, ***Y*** 91846629660 119935413056 171909861239 312597665654 149569107987 217729521757 269500353046 510985189336 131214208695 241687081897 362099358567 467378483313 539916818577	Модуль, ***N*** 836168881111 Экспонента, ***e*** 1031923 Шифр-текст, ***Y*** 83092605748 825802235227 32508735922 407171918452 614975177493 774349835780 323601958615 82169286450 198807945618 594897575157 542729555491 812833939532 694084199661

22	Модуль, ***N***	**23**	Модуль, ***N***	**24**	Модуль, ***N***
	914022837691		888532740131		175749265511
	Экспонента, ***e***		Экспонента, ***e***		Экспонента, ***e***
	517823		508097		562439
	Шифр-текст, ***Y***		Шифр-текст, ***Y***		Шифр-текст, ***Y***
	133088999278		251133768996		148649649353
	758078110965		359801014616		106749700084
	705889026842		557356431645		111279099426
	98403371042		75854873865		123808752263
	768948684522		768478933532		135559497150
	78137927374		624174758081		641323741
	383272719045		306027834198		146710462903
	341665550116		586384787006		18875910866
	407871370619		155294489444		10741502182
	382219973835		358096762086		84181024769
	653544166840		197284968232		83326297438
	658599075370		498688500894		168979058954
	825218892763		467532994504		74728979200

25	Модуль, ***N***	Шифр-текст, ***Y***
	226206740959	90602081758
	Экспонента, ***e***	155748167901
	931169	43664963557
		119662283421
		128548684055
		224153458766
		195788143843
		18231611138
		35594188617
		74744847247
		54882677589
		38908769560
		166766625254

Приложение6. ***Варианты заданий практической работы №12. Атака на алгоритм RSA методом бесключевого чтения***

1	Модуль, ***N***	**2**	Модуль, ***N***
	420882327013		302296233419
Экспонента, ***e***1	Экспонента, ***e***2	Экспонента, ***e***1	Экспонента, ***e***2
1372369	961447	1365787	763067
Шифр-текст, ***Y***1	Шифр-текст, ***Y***2	Шифр-текст, ***Y***1	Шифр-текст, ***Y***2
373413138774	105783140624	4735234112	131720982156
142492164990	384545054504	222492941603	50767819341
181970101695	91022339898	91642935786	146687208678
71400620884	266856044417	258679721851	65444189922
83588687662	106548952403	127352436654	275196580101
111752930680	160772152396	270884254827	21582029531
154836140461	128969469496	278389245811	14338137631
191336073909	242028887287	229277148124	4177778322
186412386345	256618243529	143477017416	75624657756
303121580659	47586486979	56472903944	274012339373
167437105893	306022591934	229332603068	159018739186
279265271451	419219258598	60190953676	49970035122
3	Модуль, ***N***	**4**	Модуль, ***N***
	445632735571		535598392051
Экспонента, ***e***1	Экспонента, ***e***2	Экспонента, ***e***1	Экспонента, ***e***2
1120289	559633	455341	396971
Шифр-текст, ***Y***1	Шифр-текст, ***Y***2	Шифр-текст, ***Y***1	Шифр-текст, ***Y***2
348555354398	366337925832	444982997352	358696089912
351363944134	29318249989	277831853272	360292494113
96907337112	120058862823	133187882628	91390259562
141119651255	428190500861	331361392426	534590606880
317600466893	322426909958	273206302188	193203217609
84967944527	286841513079	470299046774	166702058071
340088880266	150392378882	168157171491	68207231399
311235549494	441874945028	258737286129	487524624411
41838603784	297137742269	312335302650	325841328769
333172824695	304115257300	489235057221	533726724224
89494655477	123106598046	427689116872	369967614519
3256803669	110955623263	418723605534	247201359991
		135022585485	478832067683

5	Модуль, ***N***	**6**	Модуль, ***N***
	572953270159		622722921281
Экспонента, ***e***1	Экспонента, ***e***2	Экспонента, ***e***1	Экспонента, ***e***2
337903	301933	924383	648391
Шифр-текст, ***Y***1	Шифр-текст, ***Y***2	Шифр-текст, ***Y***1	Шифр-текст, ***Y***2
342095517391	32476529608	416413766755	363561291438
19455909955	452342848743	461616049371	349913226640
221503536026	506694128118	495579558550	410678799422
316042040322	262070340689	119296856822	49400187802
311339725976	206245109461	288338597320	264465166065
339044089754	116518622136	189325419759	617558055726
359623172126	147952236274	179661796706	378919757053
138544673544	457665805346	26462194558	550605507870
148226083413	27001690429	543527404419	341759776368
3486028632	396682057113	511749608651	125364611909
23290754913	239803556225	131463006437	288965980272
425720995382	519526641494	116692606609	434023259043
7	Модуль, ***N***	**8**	Модуль, ***N***
	516439217617		392117053283
Экспонента, ***e***1	Экспонента, ***e***2	Экспонента, ***e***1	Экспонента, ***e***2
1206433	1141277	744721	1297633
Шифр-текст, ***Y***1	Шифр-текст, ***Y***2	Шифр-текст, ***Y***1	Шифр-текст, ***Y***2
400408320444	374984721363	188779427301	330155414629
241545246801	438491303024	142624237358	183843269790
282223079755	498951362977	222856552604	113231290101
490328978748	218681974856	64779987640	381735803560
350509811006	365827206348	184552630472	115846890704
142356755075	175049781656	357891671735	117837936469
109547314116	359111505460	159800573947	188064551177
414823859933	297734746741	320365191568	241636957582
330990395685	96963152197	53704108470	253908524873
377471732609	362138584797	29809614757	219235963059
44017319588	102758207364	236651896578	333424804843
499241372980	37817394150	5185872557	278400905892
171071879560	120430068125	374026260505	254102728294

9	Модуль, ***N***	**10**	Модуль, ***N***
	319418480417		308044228439
Экспонента, ***e***1	Экспонента, ***e***2	Экспонента, ***e***1	Экспонента, ***e***2
602087	523639	976013	667829
Шифр-текст, ***Y***1	Шифр-текст, ***Y***2	Шифр-текст, ***Y***1	Шифр-текст, ***Y***2
52405618926	82810335170	41142528888	188066920245
216147098445	187684665216	168186504906	300946560686
216743861265	48173641649	136093203364	297065980706
66972942908	96024498047	242964689121	52463722858
191820297330	247351492178	35088399935	288700402082
190353918873	97241452868	235615713434	74622590470
110095200781	255901558905	255931630761	304422560213
90183965366	27364319220	243205294010	89572425507
296876615222	227156630511	282148730043	192865433148
154988611456	66990230889	167665545881	279658192310
166443759664	183816391944	236133809262	97431270440
9906682687	104719299259	248077895012	276505744422
11	Модуль, ***N***	**12**	Модуль, ***N***
	287726313019		385751370271
Экспонента, ***e***1	Экспонента, ***e***2	Экспонента, ***e***1	Экспонента, ***e***2
632699	418997	365797	1109663
Шифр-текст, ***Y***1	Шифр-текст, ***Y***2	Шифр-текст, ***Y***1	Шифр-текст, ***Y***2
214922055033	236363326198	58541562205	78032032470
35721658373	60659772128	167003685579	13064174635
111494982431	89634195001	381877628242	326727914830
18199110430	159962549494	256218527098	364066420370
42343010608	38784417281	164244249864	177576861402
252248400710	280743496547	6588741823	65863828523
63424999529	132419834073	180308234660	111437045566
119923175349	260926903227	174572441677	124743274954
154343666939	246447810193	259951955034	119577259869
161871538168	110060458786	378589342820	85769669875
66104514148	96973974426	319378579620	4688914942
20594515433	175463381167	21405495597	261002397567
120762948296	178887056429	226860843155	341722428571

13	Модуль, ***N***	**14**	Модуль, ***N***
	518587807081		573308195401
Экспонента, ***e***1	Экспонента, ***e***2	Экспонента, ***e***1	Экспонента, ***e***2
293177	1209781	973169	550351
Шифр-текст, ***Y***1	Шифр-текст, ***Y***2	Шифр-текст, ***Y***1	Шифр-текст, ***Y***2
373852443734	22286870422	327707922480	484439401392
447989059513	343015689591	455697659443	92203619034
140756140384	281801228231	469317095774	199299165882
207791711792	360270382562	41173012855	100840467257
252160015422	264253306719	95114431187	42877265767
151272799305	128520421967	183548202066	537319004931
431450717984	399665129411	114278917224	212469277565
252882800366	448878989738	111319924653	335238563578
112417596471	70913527757	302320646938	215934710265
301753741810	295285211952	497834611165	248375790884
480461056512	247990966487	207393954597	8143413999
334158277030	202711954425	469317095774	199299165882
368394150653	201121363025	184588110993	484325656679
15	Модуль, ***N***	**16**	Модуль, ***N***
	634875396959		512453104601
Экспонента, ***e***1	Экспонента, ***e***2	Экспонента, ***e***1	Экспонента, ***e***2
797611	375841	1365347	972793
Шифр-текст, ***Y***1	Шифр-текст, ***Y***2	Шифр-текст, ***Y***1	Шифр-текст, ***Y***2
215938301159	592194596499	17680290297	410084071984
156476855390	618920283747	359514971944	150398051936
629025629999	481110939902	395933838767	489149759410
390282732416	118468312259	135375405636	11043062086
486255942680	152271753836	424188955183	452072614483
301447617826	245706953152	480774525813	94954712588
611079544000	357574573601	176693333558	373871024394
9815582940	517943651115	366722473439	194623183329
238155160282	449088004034	257271491888	478231887994
89572033554	549269593969	437238044102	452346492359
259610717355	274641120696	280697746591	145030784098
561079697420	170397276793	192092245943	310653569484
68884371224	150603791351	180087210668	280971453825

17	Модуль, ***N***	**18**	Модуль, ***N***
	549840164113		521194405273
Экспонента, ***e***1	Экспонента, ***e***2	Экспонента, ***e***1	Экспонента, ***e***2
830309	1122659	293767	492511
Шифр-текст, ***Y***1	Шифр-текст, ***Y***2	Шифр-текст, ***Y***1	Шифр-текст, ***Y***2
421894113021	460364462002	70696562	139896254161
70151618285	377869829708	136043022917	268972783372
256033134230	315408321663	65407415375	281244321042
230572827320	403500544217	164404262967	190886094
345706195727	90051720740	445647345197	183760973977
379296943648	398226212020	118953770797	127631527830
131864337239	357731842992	512196733213	29296947894
345346802879	394252754984	103009198361	342466717237
460224575827	318030259077	317437263597	76798964679
28746971542	317217533534	284559552852	346421581772
176535748663	42352806819	490098245083	345796314978
395695787161	277427982170	149823933745	281195436813
		224803955806	359213893561

19	Модуль, ***N***	**20**	Модуль, ***N***
	500984306287		502110569407
Экспонента, ***e***1	Экспонента, ***e***2	Экспонента, ***e***1	Экспонента, ***e***2
470149	267797	693661	366287
Шифр-текст, ***Y***1	Шифр-текст, ***Y***2	Шифр-текст, ***Y***1	Шифр-текст, ***Y***2
274230487503	176943898057	451590415251	489035727840
6821302647	272954693703	110439571420	352254618578
172152295595	141643708385	183752091528	112984103119
454539302130	238296127866	274872936616	324252397833
462305524774	270971764501	28541011195	258279989467
73589652382	389314459147	450835617776	309371933868
274794725040	476866404163	260759622383	309370695834
295185494003	295344931481	342128341762	275718202556
159348742119	288885538254	158761845107	484547254614
62021560582	144738759088	190701543235	319090281932
311827395163	52793710114	336633436793	321505940571
159638616315	416204845784	107036107438	499673648361
		143086295492	445389404030

21	Модуль, ***N***	**22**	Модуль, ***N***
	635476116169		606089625293
Экспонента, ***e***1	Экспонента, ***e***2	Экспонента, ***e***1	Экспонента, ***e***2
866707	1123211	524123	1109309
Шифр-текст, ***Y***1	Шифр-текст, ***Y***2	Шифр-текст, ***Y***1	Шифр-текст, ***Y***2
164724618825	119849004283	496663520230	196561923290
386399947495	156284059617	573686340098	102658895412
569519600328	399964659582	317277380080	577585560553
335674131307	411242163372	311062242263	44037449636
591926181226	473998672968	87966670626	508496748333
331711492017	449146422851	156120202050	278687486043
222632530911	178846180173	517816376872	261550581766
159285067102	431421957979	255107405391	487843663934
529695664488	209987811333	70642465288	314450235982
462703958023	627608476514	390229374493	345028986924
508391137110	23204756436	333422604916	104569551730
573759000564	43305372061	2671384922	486557652833
48989336806	542459119849	509131255766	337080661180
23	Модуль, ***N***	**24**	Модуль, ***N***
	303958823183		216044621671
Экспонента, ***e***1	Экспонента, ***e***2	Экспонента, ***e***1	Экспонента, ***e***2
1173551	1366693	493001	693169
Шифр-текст, ***Y***1	Шифр-текст, ***Y***2	Шифр-текст, ***Y***1	Шифр-текст, ***Y***2
300865234944	158205869566	204707607052	161085576818
280167078723	47430389231	131209885175	166651266503
44778324729	235868270647	74127570208	210362428729
15647443106	60933642983	167559112602	29681376125
72500796041	230961885063	114202832764	51404224010
127042219796	189840956692	175086144102	85147589057
220297476381	155026770625	173536223165	53004594773
159193146152	118061171422	123432367535	4926673942
281783946206	64695094087	82425793128	28134852744
83397684706	90093203015	185507595143	16056810738
218587175059	140628953794	95061918272	57750263032
32628200905	156685525752	193636415087	146784016398
87293077359	96578125026	162487637030	143689492474

25	Модуль, ***N***	Шифр-текст, ***Y***1	Шифр-текст, ***Y***2
	193576240729	159391395691	187917061998
Экспонента, ***e***1	Экспонента, ***e***2	157577675381	100356696331
376133	633317	191080992560	115395060871
		149368918681	22072994636
		53984801508	10119558157
		4424043610	166188791942
		58203874858	81150163516
		76432058336	112715855314
		16217372577	19232790590
		149007313066	106250648527
		63447430442	21826060759
		64914562999	12414159731
		127848484896	192871647135

Приложение7. ***Варианты заданий практической работы №13. Атака на алгоритм RSA на основе Китайской теоремы об остатках***

1	Шифр-текст, Y_1	Шифр-текст, Y_2	Шифр-текст, Y_3
	177412278620	227891126441	230974691188
Экспонента***e***=3	8631904062	175684889961	345734293737
	60910035474	108275398403	118726556071
Модуль, N_1	297496979396	50799922679	220369632983
359690807803	44306701511	50861774819	69236028918
Модуль, N_2	223949114264	120598551775	121704957571
361062169537	95163574676	214220319631	269179568504
	126740768642	193858968963	201685371953
Модуль, N_3	306466049596	243446962166	75708873566
363514381513	82343556476	168236630688	101720600746
	97754924718	260389624172	131962627319
	242675823829	86845867002	44909629158

2	Шифр-текст, Y_1	Шифр-текст, Y_2	Шифр-текст, Y_3
	100018221941	219670103959	258489005115
Экспонента e=3	357476497416	299234661384	193486305912
	360704892674	321665231322	317085850998
Модуль, N_1	258968522463	303452309552	228076833982
368166998833	363378787391	197707480483	118470145682
	38938998120	271136973244	302313432794
Модуль, N_2	165805097876	31151628083	214437258395
368656533313	328038699497	195899793924	132123789026
	297851010158	230643014304	96889642413
Модуль, N_3	184316347833	323745610236	300010020637
371205502531	202277180039	125326155250	249393170795
	260169809092	4695289469	187672572758
	136359418113	154882534227	93192923225

3	Шифр-текст, Y_1	Шифр-текст, Y_2	Шифр-текст, Y_3
	120321295984	261990433834	322305651846
Экспонента e=3	116941070964	232071459327	286065905390
	156315192664	305414687540	188633713225
Модуль, N_1	260149644765	348455852917	131649116365
380077454101	357688967002	206680974925	253206684415
	165841867143	327578130329	46677871611
Модуль, N_2	349826484990	5548686870	65268441973
380903460337	337993834720	295985428633	317133281785
	117681826230	157420509616	52226297600
Модуль, N_3	36279369135	256913681356	255637668770
383306345689	124613350713	271869775627	201873507225
	106958422772	310864218021	260192105953

4	Шифр-текст, Y_1	Шифр-текст, Y_2	Шифр-текст, Y_3
	23283117034	81950696329	57844537762
Экспонента e=3	199910300344	310054893565	368640254231
	122379231308	132301878314	220965124671
Модуль, N_1	129836433029	52795246284	260183659429
389091381643	266167362913	276197768422	299904567942
	322794903721	265696804182	286935730637
Модуль, N_2	164367877138	238369333190	266053541214
391569053221	317459368677	66855113681	146542714390
	210705957227	316766995365	79442443012
Модуль, N_3	38878534867	321182915473	28368938795
393864798289	199295177267	118193576787	30970811879
	116980227366	190068391425	72570776324

5	Шифр-текст, Y_1	Шифр-текст, Y_2	Шифр-текст, Y_3
	257953403766	128730750274	382653707323
Экспонента e=3	177168684125	391893911248	186385219382
	98569851945	323200994518	394103230832
Модуль, N_1	111013170885	152862355610	16445037923
397066122499	126870693789	23614632228	382954747667
Модуль, N_2	356996906573	96365786831	387456992444
397797027109	369112783220	207779539976	258166753697
	118662185076	70218040709	375871570884
Модуль, N_3	192227498736	317562220506	342932316985
400288163101	13981739973	111815966551	104729956068
	77574341290	1949429944	46092487953
	98562917188	8329351035	69550838402
	14769259640	147453838103	289762815713

6	Шифр-текст, Y_1	Шифр-текст, Y_2	Шифр-текст, Y_3
	161938982030	227240021793	124238176183
Экспонента e=3	93539768747	240397026641	56013695777
	198680625546	319693734726	98169308648
Модуль, N_1	324985467275	143364329762	320302328458
408685041841	364301388858	267584092696	257566073714
Модуль, N_2	121946924018	104392885896	180123701720
409542365311	130171610724	60224870888	231998512656
	264709094112	54379930123	220441010255
Модуль, N_3	198127513690	281164821607	105926142958
411702675541	98490234931	51747910478	104088206001
	86416406414	152858842656	312601660772
	347341863803	198634569843	358423325011
	261057850418	304306303763	229574485891

7	Шифр-текст, Y_1	Шифр-текст, Y_2	Шифр-текст, Y_3
	17599664694	388099839383	84003082499
Экспонента e=3	221343847340	141363764478	245906362572
	181796040962	253757042128	398398702796
Модуль, N_1	210108814452	162556515860	157559004814
420250053679	124320289825	289849639847	157418944324
Модуль, N_2	323995715057	126598663712	411242039391
420998138947	260285700707	171600933709	270378838199
	72474978285	80576580207	182942084181
Модуль, N_3	226746757036	347679322161	33847193530
422793377077	369084323018	408725538627	149137845569
	133261286623	244886980553	382620866773
	336107911000	171682264557	120769412025
	303767221006	366784660912	272019119100

8	Шифр-текст, Y_1	Шифр-текст, Y_2	Шифр-текст, Y_3
	43268974598	330701159000	269237460393
Экспонента e=3	302331913599	104807592171	165034165638
	47134049761	45038416117	207280715083
Модуль, N_1	126642563008	81063981859	151936477226
431972773933	165827503054	427734601871	7495879547
	232086597542	27505991527	141105308724
Модуль, N_2	31465887151	81910363197	316939568874
432558060211	30373336865	190166502949	360819196331
	284998624093	116404011104	46940627813
Модуль, N_3	89084365158	249933949107	137301580237
434276528083	322533676789	90486698466	168518778628
	383736009455	206265723002	113124777920
	108545189851	276536042468	282998095133
9	Шифр-текст, Y_1	Шифр-текст, Y_2	Шифр-текст, Y_3
	324500796659	364411844182	57065247639
Экспонента e=3	324547036186	137247785047	130359065508
	367901833181	389030356498	391859459727
Модуль, N_1	38558700097	293766643714	128196485994
441716293693	401956144715	259139396276	412050631244
	260421328704	429702138150	367300386309
Модуль, N_2	356041474179	17968702271	83703862830
442258294987	113539876955	84037113464	218100297714
	304515179769	91988591941	10243576841
Модуль, N_3	302662240842	425057692992	232358719915
444399387571	282367185538	391906969363	412546535924
	432213853716	244207991747	398872645339
10	Шифр-текст, Y_1	Шифр-текст, Y_2	Шифр-текст, Y_3
	445451352210	424531890296	118710004991
Экспонента e=3	249439394113	430487757843	307218752883
	387029823615	273579896124	366564784860
Модуль, N_1	132042218903	163172411830	182819846943
449094675559	73614801093	299409036513	86662518238
	101481466259	34387871280	405369976705
Модуль, N_2	448458747498	190507227268	111221455773
449774960461	443385035969	108323290415	368248616971
	75012412264	332577990284	227865580737
Модуль, N_3	19096037043	213248626661	38736323891
451557288811	259197438248	78257808298	137144185691
	220559106494	238075298353	231896396336

11	Шифр-текст, Y_1	Шифр-текст, Y_2	Шифр-текст, Y_3
	118519640042	68925059719	360911630335
Экспонента e=3	325725597818	320794723471	49077546247
	449577094588	106708759661	367587011852
Модуль, N_1	225738390357	267503416207	205773073385
457829717113	390837010969	176633626568	166430526462
Модуль, N_2	417997930307	370938941185	166130351420
461639371789	186946730799	256010935139	240614091730
	307353836168	375173961262	1307748376
Модуль, N_3	331923022405	50942041502	289507057580
463811451073	439103095463	13373860798	309981198851
	415559987555	369523972407	123903944003
	407104561771	268680126161	113555743553

12	Шифр-текст, Y_1	Шифр-текст, Y_2	Шифр-текст, Y_3
	384927940677	47337377053	342954751710
Экспонента e=3	473049749478	15502694428	440889851539
	98141220439	81559584886	67503329756
Модуль, N_1	47772742554	360290532716	462595462377
473302960111	85402795076	378412185459	84092175909
Модуль, N_2	49762300554	471133458035	57911552136
476210148031	243238759870	276394936545	60433527302
	132174590679	2116712669	25311956275
Модуль, N_3	394107604075	37111299200	370327609107
478258728547	292566652796	387986386867	296462225245
	394413369679	97786707059	241699085506
	176379334217	256442600412	465708091819
	425745574767	455327955288	454345671530
	279970734890	119517607360	210180151910

13	Шифр-текст, Y_1	Шифр-текст, Y_2	Шифр-текст, Y_3
	45854580612	274960963762	245417628800
Экспонента e=3	105237269523	445004609734	58500957429
	169259415669	314321127441	337297880630
Модуль, N_1	93616181002	121008447611	192371047425
483603920323	111788215636	77289255193	368079140170
Модуль, N_2	19646301574	185428067959	444426125103
484627023409	344814513220	268033072619	485088147460
	284120677804	483476916533	384977923665
Модуль, N_3	135039654745	378663280169	52336096116
486046777033	8393533606	145768361237	217360431271
	277869220393	164058939780	261094805307
	95747282494	427513468440	77329919173
	31789892340	16789037076	280539607542

14	Шифр-текст, Y_1	Шифр-текст, Y_2	Шифр-текст, Y_3
	405186643929	298462743436	372083067441
Экспонента e=3	264588538265	26894204289	354383414943
	58896941920	266800308083	31782553847
Модуль, N_1	424470122024	469634672912	213067042090
494980336813	445830333875	423565503334	22742161466
	98276685134	418775305332	313919341914
Модуль, N_2	210238595626	112405305103	71514328634
495019868347	176058872641	302129659337	117790204322
	185715938214	323850375295	268549130622
Модуль, N_3	418034348683	438598232992	409153352258
496510218943	52552730024	10359943018	316714994539
	481876348312	298111389169	270152277750
	438600466605	277384894755	128472385009

15	Шифр-текст, Y_1	Шифр-текст, Y_2	Шифр-текст, Y_3
	65555047695	324422804544	435445028187
Экспонента e=3	224704827698	374009722121	207888333371
	426614994776	291369610887	344446367064
Модуль, N_1	482499765759	103658691090	372373145295
503847739471	499927141525	355087189555	26158114757
	251539329355	403634830552	389306763320
Модуль, N_2	288065643935	45811542091	15362084660
505210110529	500487899533	342405362400	342395172034
	284158354428	397470779417	275443080668
Модуль, N_3	179929130009	143094497045	219501574324
506974617943	4059729507	16866311017	343966567526
	337999368066	162845742211	291026935191

16	Шифр-текст, Y_1	Шифр-текст, Y_2	Шифр-текст, Y_3
	302279248041	48522238217	129856570412
Экспонента e=3	398777422648	116578598684	82270781294
	382393465830	98210011370	140695444887
Модуль, N_1	109346520792	452947538650	510689827054
519445678909	393648988334	113090002659	42634086860
	83456507369	130683028799	516267119547
Модуль, N_2	503695835656	170075383039	5616396143
522088422619	409770589873	19947030841	8388941434
	483819180150	458406287083	73724586316
Модуль, N_3	358939341533	178964953872	290433741122
523328119219	402486907104	500143943025	102266925300
	347176414967	189689940709	75736288391
	1633679742	218613469572	406132000561

17	Шифр-текст, Y_1	Шифр-текст, Y_2	Шифр-текст, Y_3
	281386842307	5670875437	380269517653
Экспонента e=3	121824522874	330566529390	366125418676
	245939933284	465969872193	400608227248
Модуль, N_1	25488678869	104239877954	119236616785
530262062431	245966715725	421060036048	40916016109
Модуль, N_2	346164781438	26548660136	6459310768
533023659991	240458184136	226283588677	111454112735
	477792982000	232398586638	191143773891
Модуль, N_3	50321051371	141813896655	428929030217
534655902139	249631869316	455313322872	441962444995
	346825618977	64540250896	334966880931
	352450998028	175680952596	380319156170

18	Шифр-текст, Y_1	Шифр-текст, Y_2	Шифр-текст, Y_3
	252761993375	175866403284	432443719708
Экспонента e=3	439317043104	297457023908	291474822430
	524563666624	352677317646	142735272242
Модуль, N_1	200316247013	525837137252	317684793012
542029523461	168730893537	500452725795	216551100123
Модуль, N_2	276462662401	255875720416	30474056356
545442955261	95027181355	484409681814	501398385288
	153947838824	36312121014	405101779653
Модуль, N_3	517609475112	208360918386	371861659744
543651655507	21916921129	288089579742	467319917841
	186570691221	492797454334	209273129747
	188654245468	91193680807	270602387237

19	Шифр-текст, Y_1	Шифр-текст, Y_2	Шифр-текст, Y_3
	532587529932	453172264962	283795978048
Экспонента e=3	466776013367	295084884945	548212520352
	194393214430	184687156359	50623875598
Модуль, N_1	551419753294	110229199835	45628043554
553399203289	235808018295	452343899082	374654069771
Модуль, N_2	521345765147	61700963597	454067424044
555525439597	62408122881	371846842	140771995786
	238014267850	184524760412	230698987467
Модуль, N_3	282320724474	349901424433	416727167751
556783358239	421626850723	66575580602	87650410693
	477001857725	38470059268	75414175302
	59354292288	27434041612	305387967882

20	Шифр-текст, Y_1	Шифр-текст, Y_2	Шифр-текст, Y_3
	178430347017	464060851187	112360892551
Экспонента e=3	275798270566	466784394057	48950009370
	150441557212	113750938542	204834012880
Модуль, N_1	35319995468	50225874889	472985274437
564051718543	214899391564	135816601540	150470587109
Модуль, N_2	454509168990	383147938913	437368878774
567177464083	241622156972	445379546704	348445464666
	47081057682	20609631777	120707881073
Модуль, N_3	532012996953	530473256199	424353814205
568582697167	114671548487	291868875010	495774818876
	272811533565	327407870868	460590967231

21	Шифр-текст, Y_1	Шифр-текст, Y_2	Шифр-текст, Y_3
	400967861722	400511331925	365230039044
Экспонента e=3	402921963995	359110439723	503139848290
	345366187498	156672928720	452112473725
Модуль, N_1	170749944344	81237697207	98832137945
570206339323	398474550143	446268495117	16750539498
Модуль, N_2	14128843304	567101402400	496867432761
572010531679	525338681306	380678770261	98372266130
	553357177665	405322363448	349596187748
Модуль, N_3	554714202377	250349383856	172522293935
573673162471	378737847392	480141604318	161623878001
	241207247252	201068876886	405142270947
	330231009566	160562856485	404286756199

22	Шифр-текст, Y_1	Шифр-текст, Y_2	Шифр-текст, Y_3
	428799001102	330278110381	426468615928
Экспонента e=3	417746620458	413803169370	348743875265
	233652090970	399528613141	261688856582
Модуль, N_1	425829696584	431344022162	29957256669
582980801989	132807280253	133251402314	108448874326
Модуль, N_2	540064099057	579394141601	23970225383
585089367091	191642450251	339286468279	410917339855
	364237792802	235332969532	179638698652
Модуль, N_3	294540030550	1036448642	282723305676
586408807447	287338190886	400656499573	115801357719
	8030576378	47204841232	575898855271
	562848664519	249621210713	528022904569

23	Шифр-текст, Y_1	Шифр-текст, Y_2	Шифр-текст, Y_3
	179564892807	376452630248	369376837096
Экспонента e=3	489396036392	569864359142	167105576017
	176575769058	124688754894	449990310238
Модуль, N_1	269255594799	562457224201	417101045217
588465234361	422117999595	22357940168	404468253839
	257369618664	151586582904	1603305513
Модуль, N_2	539258064402	533949898858	478144160973
586195041433	177014956905	116088884375	212789604411
	234449256532	221471039114	559954258624
Модуль, N_3	387357205774	16723092454	55850508600
587299922977	183843097094	343577678223	85339397069
	189558056464	313846942324	409000193866
24	Шифр-текст, Y_1	Шифр-текст, Y_2	Шифр-текст, Y_3
	534935192069	70956316615	547351293988
Экспонента e=3	586334468916	196061328294	558349441596
	575821575470	472946437612	209735294323
Модуль, N_1	158445010924	167175113770	257527905634
590059443367	168022188272	213280914294	328543700761
	419451618702	97582680057	241383661927
Модуль, N_2	403150327598	87487791156	318686253990
586035939793	462915818163	319786583031	391540759391
	156960926738	526032348303	124252499803
Модуль, N_3	423280293357	561873181810	400043751247
582032534407	308065052008	93452497746	36326931192
25	Шифр-текст, Y_1	Шифр-текст, Y_2	Шифр-текст, Y_3
	461743067035	429395271160	293399822655
Экспонента e=3	16510154740	404839447718	408678947374
	541409292183	431790388728	461462830734
Модуль, N_1	147537040251	84465928224	469093286418
593974289329	121241807149	179431496912	229214387811
	383535805471	250884484533	405621273396
Модуль, N_2	420328432686	367066937735	566681986508
590987500549	360735839890	493669050691	381039554115
	426786420629	588637988770	30236954381
Модуль, N_3	268507362618	235309880383	124256080362
585323335717	381406130147	79134719899	424813292522
	369378326912	469747448675	425803797156

Учебное издание

Васильева Ирина Николаевна,
кандидат физико-математических наук, доцент;
Куватов Валерий Ильич,
доктор технических наук, профессор, заслуженный работник
высшей школы Российской Федерации

КРИПТОГРАФИЧЕСКАЯ ЗАЩИТА ИНФОРМАЦИИ

Практикум

Редактор *Свикша Н.О.*
Компьютерная верстка *Свикша Н.О.*
Дизайн обложки *Савиных А.И.*

Подписано в печать 25.08.2017. Формат 60×84 $^{1}/_{16}$
Печать цифровая. Объем 16,25 п.л. Тираж 100 экз. Заказ № 134/17

Отпечатано в Санкт-Петербургском университете МВД России
198206, Санкт-Петербург, ул. Летчика Пилютова, д. 1