ИСТОРИЧЕСКАЯ КРИПТОГРАФИЯ

Теоретические сведения

История цивилизации показывает, что практически сразу с появлением письменности появлялись и разного рода системы защиты информации от несанкционированного доступа. Рассмотрим наиболее популярные из них.

1. Шифр Цезаря. Суть его в том, что в тексте каждая буква заменяется отстоящей от нее по алфавиту на фиксированное число позиций по циклу. Так Юлий Цезарь в I веке новой эры в деловой переписке заменял в сообщении первую букву латинского алфавита (A) на четвертую (D), вторую (B) – на пятую (E), наконец, последнюю – на третью. Иными словами, замена производилась в соответствии с таблицей, которая в русском варианте имеет следующий вид (рис. 5.1).

А	Б	В	Г	Д	Е	Ё	Ж	З	И	Й	К	Л	М	Н	О
Г	Д	Е	Ё	Ж	З	И	Й	К	Л	М	Н	О	П	Р	С

П	Р	С	Т	У	Ф	Х	Ц	Ч	Ш	Щ	Ъ	Ы	Ь	Э	Ю	Я
Т	У	Ф	Х	Ц	Ч	Ш	Щ	Ъ	Ы	Ь	Э	Ю	Я	А	Б	В

Рис. 5.1

Пример 5.1. Знаменитое донесение римскому сенату об очередной победе выглядело (в русском переводе) следующим образом:

ТУЛЫИО ЦЕЛЖЗО ТСДЗЖЛО

Приложив достаточно серьезные усилия по расшифровке, можно убедиться, что истинный текст гласит: «Пришел, увидел, победил».

Шифр Цезаря входит в класс шифров, называемых «подстановка» или «простая замена». Это такие шифры, в котором каждая буква алфавита заменяется буквой, цифрой, символом или какой-нибудь их комбинацией.

2. Тарабарская грамота. Известна в России с XIII века. На уровне разговорного языка ею владели и Стенька Разин и Емельян Пугачев. Гиляровский еще в 30-х г. XX века встречал на московских рынках странных лиц, переговаривавшихся между собой на «тарабарском». Тарабарская грамота проста. В ней согласные буквы заменяются по схеме, представленной на рис. 5.2.

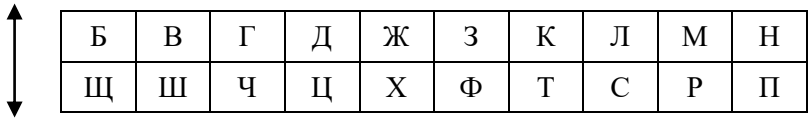

Рис. 5.2

При шифровании буквы, расположенные на одной вертикали, переходят одна в другую. Остальные буквы остаются без изменения.

Пример 5.2. Попробуйте прочитать следующее исключительно секретное сообщение:

РАРА РЫСА МАРУ

3. Криптосистема Тритемиуса. Данная система шифрования впервые была опубликована в 1518 г. в трактате, принадлежащем перу религиозного деятеля аббата Тритемиуса (1462 – 1516). Система Тритемиуса представляет собой дальнейшее усовершенствование системы шифрования Цезаря и базируется на идее применения девизов. Под текстом подписывался девиз (в дальнейшем его стали называть «ключом») с повторением, затем происходило постолбцовое суммирование букв текста и девиза («ключа» по новой терминологии), в результате получался шифротекст.

Пример 5.3. Зашифруем текст «Над Парижем небо синее» с помощью девиза «Роза». Как сказано выше, для этого выпишем две строки – строку текста и строку ключа с повторением. Сверху и снизу добавим по строке номеров соотаетствующих букв в русском алфавите. Получим следующую таблицу (рис. 5.3).

15	1	5	17	1	18	10	8	6	14	15	6	2	16	19	10	15	6	6
Н	*А*	*Д*	*П*	*А*	*Р*	*И*	*Ж*	*Е*	*М*	*Н*	*Е*	*Б*	*О*	*С*	*И*	*Н*	*Е*	*Е*
Р	*О*	*З*	*А*	*Р*	*О*	*З*	*А*	*Р*	*О*	*З*	*А*	*Р*	*О*	*З*	*А*	*Р*	*О*	*З*
18	16	9	1	18	16	9	1	18	16	9	1	18	16	9	1	18	16	9

Рис. 5.3

Для получения шифротекста суммируем числа каждого столбца полученной таблицы. Если сумма оказывается больше 33, то вычитаем из этой суммы 33. После этих вычислений от числа переходим к букве. Так в первом столбце получаем число $15+18=33$, то есть букву «Я». Продолжив процедуру, получим следующее шифрованное сообщение:

Я П М Р С А С З Ц Ь Ц Ё Т Ю Ъ И Я Ф Н

Французский посол в Риме Блез де Виженер (1523 – 1596), по роду службы связанный с проблемой секретности дипломатической почты, написал большой «Трактате о шифрах» (опубликован в 1585 г.). Он внес небольшое практическое усовершенствование в криптосистему Тритемиуса, которое позволило процедуру шифрования – дешифрования осуществлять почти автоматически. Роль шифровальной машины у Виженера играет квадратная таблица с алфавитом. Первая ее строка заполнена последовательно буквами алфавита. Вторая – тем же алфавитом, но сдвинутым на одну букву влево – в нашем случае начинается с буквы Б и заканчивается буквой А. Третья строка начинается буквой В и заканчивается буквой Б. И так далее, до 33 строки включительно. Возвращаемся к примеру 5.3. На пересечении столбца с первой буквой Н и строки с первой буквой Р находим букву Я – первую букву шифротекста. И так далее.

В таком виде криптосистема с девизом применялась на протяжении 400 лет как абсолютно надежная и не дешифруемая, особенно в военном деле. О том, что криптосистема Тритемиуса успешно применялась и в начале XX века свидетельствуют, в частности, отдельные страницы бессмертной книги Йозефа Гашека «Похождения бравого солдата Швейка».

Таблица Виженера (1576 г.)

а	б	в	г	д	е	ё	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
б	в	г	д	е	ё	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
в	г	д	е	ё	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
г	д	е	ё	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
д	е	ё	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
е	ё	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
ё	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
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	ё
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	ё	ж
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	ё	ж	з
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	ё	ж	з	и
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	ё	ж	з	и	й
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	ё	ж	з	и	й	к
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	ё	ж	з	и	й	к	л
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	ё	ж	з	и	й	к	л	м
о	п	р	с	т	у	ф	х	ц	ч	ш	щ	ъ	ы	ь	э	ю	я	а	б	в	г	д	е	ё	ж	з	и	й	к	л	м	н
п	р	с	т	у	ф	х	ц	ч	ш	щ	ъ	ы	ь	э	ю	я	а	б	в	г	д	е	ё	ж	з	и	й	к	л	м	н	о
р	с	т	у	ф	х	ц	ч	ш	щ	ъ	ы	ь	э	ю	я	а	б	в	г	д	е	ё	ж	з	и	й	к	л	м	н	о	п
с	т	у	ф	х	ц	ч	ш	щ	ъ	ы	ь	э	ю	я	а	б	в	г	д	е	ё	ж	з	и	й	к	л	м	н	о	п	р
т	у	ф	х	ц	ч	ш	щ	ъ	ы	ь	э	ю	я	а	б	в	г	д	е	ё	ж	з	и	й	к	л	м	н	о	п	р	с
у	ф	х	ц	ч	ш	щ	ъ	ы	ь	э	ю	я	а	б	в	г	д	е	ё	ж	з	и	й	к	л	м	н	о	п	р	с	т
ф	х	ц	ч	ш	щ	ъ	ы	ь	э	ю	я	а	б	в	г	д	е	ё	ж	з	и	й	к	л	м	н	о	п	р	с	т	у
х	ц	ч	ш	щ	ъ	ы	ь	э	ю	я	а	б	в	г	д	е	ё	ж	з	и	й	к	л	м	н	о	п	р	с	т	у	ф
ц	ч	ш	щ	ъ	ы	ь	э	ю	я	а	б	в	г	д	е	ё	ж	з	и	й	к	л	м	н	о	п	р	с	т	у	ф	х
ч	ш	щ	ъ	ы	ь	э	ю	я	а	б	в	г	д	е	ё	ж	з	и	й	к	л	м	н	о	п	р	с	т	у	ф	х	ц
ш	щ	ъ	ы	ь	э	ю	я	а	б	в	г	д	е	ё	ж	з	и	й	к	л	м	н	о	п	р	с	т	у	ф	х	ц	ч
щ	ъ	ы	ь	э	ю	я	а	б	в	г	д	е	ё	ж	з	и	й	к	л	м	н	о	п	р	с	т	у	ф	х	ц	ч	ш
ъ	ы	ь	э	ю	я	а	б	в	г	д	е	ё	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	б	в	г	д	е	ё	ж	з	и	й	к	л	м	н	о	п	р	с	т	у	ф	х	ц	ч	ш	щ	ъ
ь	э	ю	я	а	б	в	г	д	е	ё	ж	з	и	й	к	л	м	н	о	п	р	с	т	у	ф	х	ц	ч	ш	щ	ъ	ы
э	ю	я	а	б	в	г	д	е	ё	ж	з	и	й	к	л	м	н	о	п	р	с	т	у	ф	х	ц	ч	ш	щ	ъ	ы	ь
ю	я	а	б	в	г	д	е	ё	ж	з	и	й	к	л	м	н	о	п	р	с	т	у	ф	х	ц	ч	ш	щ	ъ	ы	ь	э
я	а	б	в	г	д	е	ё	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

Опыт долгого применения рассмотренной криптографической системы указал на проблему ключей. Слишком долгое применение одного и того же ключа может навести противника на какие-то закономерности и, как следствие, к взлому криптосистемы. Проблема эта преодолевалась двумя путями. Сначала пришли к мысли применения длинных ключей. В идеале – длина ключа совпадает с длиной шифруемого текста. Затем, естественно, быстро пришли к идее частой смены ключей. Частая смена ключей порождают проблемы выбора новых ключей и их передачи. Выход был найден неожиданный и гениально простой – книга. Участники переписки используют идентичные экземпляры одного и того же издания конкретной книги. Новый ключ сообщается, называя страницу и абзац книги. Два числа переданные почтой или публикацией в рекламном отделе газеты вряд ли дадут содержательную информацию противнику.

4. Постолбцовая транспозиция. К классу «перестановка» относится шифр «маршрутная транспозиция» и его вариант «постолбцовая транспозиция». В данный прямоугольник $[n \times m]$ вписывается сообщение по строкам. Шифрованный текст найдем, если будем выписывать буквы в порядке следования столбцов.

Следующий пример демонстрирует шифрование методом «постолбцовой транспозиции».

Пример 5.4. Текст, состоящий из 30 букв, записан построчно змейкой в таблицу или матрицу размером 5×6 (рис. 5.4)

М	*И*	*Н*	*С*	*К*	*С*
А	*Ц*	*И*	*Л*	*О*	*Т*
Р	*Е*	*С*	*П*	*У*	*Б*
Е	*Б*	*И*	*К*	*И*	*Л*
Л	*А*	*Р*	*У*	*С*	*Ь*

Рис. 5.4

Шифрованный текст получается последовательной записью столбцов этой таблицы в строку, также змейкой, начиная с последнего:

МАРЕЛ АБЕЦИ НИСИР УКПЛС КОУИС ЬЛБТС

Конечно, возможны и другие способы-маршруты записи текста в таблицу и выписки столбцов. Например, такой, более естественный (рис. 5.5).

М	*И*	*Н*	*С*	*К*	*С*
Т	*О*	*Л*	*И*	*Ц*	*А*
Р	*Е*	*С*	*П*	*У*	*Б*
Л	*И*	*К*	*И*	*Б*	*Е*
Л	*А*	*Р*	*У*	*С*	*Ь*

→ *МТРЛЛ ИОЕИА НЛСКР СИПИУ КЦУБС САБЕЬ*

Рис. 5.5

Попробуйте прочитать еще одно сообщение, шифрованное методом «по-

столбцовой транспозиции».

Пример 5.5. МАСТ АЕРР ЕШРН ОЕРМ ИУПВ КЙТР ПНОИ

Усложнением этих двух вариантов шифрование является применение девизов. Суть их в том, что после записывания текста в таблицу столбцы таблицы переставляются каким-то образом, прежде чем выписывать шифротекст. В человеческой природе всякому действию придавать какой-нибудь, пусть и призрачный, смысл. Вот и пришла кому-то мысль не просто переставлять столбцы, а в порядке следования букв в девизе.

Пример 5.6. Усложним шифровку по первой таблице примера 5.4, применив к ней девиз «Немига». Согласно порядку следования букв в русском алфавите буквам этого девиза присваиваются соответственно следующие номера: 6, 3, 5, 4, 2, 1. В этом порядке и выписываем столбцы первой шифровки примера 5.4:

ЛЕРАМ СЛПКУ ИЦЕБА РИСИН СИУОК СТБЛЬ

5. Криптосистема Кардано. Пожалуй, наиболее сложный вариант «маршрутной перестановки» предоставляет *поворотная решетка* или *решетка Кардано.* Джероламо Кардано (1501 – 1576) – знаменитый итальянский математик, механик, врач, философ. Как математик, он знаменит тем, что нашел формулы решения кубических уравнений. А как механик – прежде всего тем, что на его идеях реализовано в каждом автомобиле устройство под названием «карданный вал». Наконец, Кардано оставил глубокий след и в криптографии.

Авторству Джероламо Кардано принадлежит следующий метод шифрования. Для тайной передачи сообщения, содержащего $4mk$ букв, изготавливается трафарет из прямоугольного листа клетчатой бумаги размером $2m \times 2k$ клеток. В трафарете вырезают mk клеток так, чтобы при наложении его на такой же чистый лист бумаги четырьмя возможными способами его вырезы полностью покрывают всю площадь листа. Определяется заранее порядок этих четырех возможных положений. Буквы сообщения последовательно вписываются в вырезы трафарета – самый естественный вариант – по строкам, в каждой строке слева направо. Заполненная таблица записывается последовательно – каждый столбец в строку (рис. 5.6).

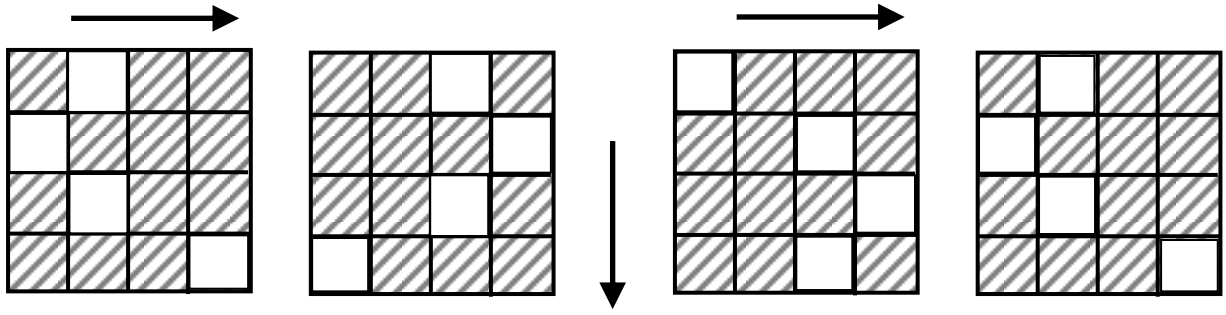

Рис. 5.6

Пример 5.7. Прочитайте записанное с помощью приведенного выше трафарета и в указанном выше порядке следующее краткое, но несомненно важное сообщение:

ОТТВ РЧИЫ УЕТМ ЕЗЙВ

Задания для самостоятельной работы

0. Реализуйте алгоритмы для расшифровки и зашифровки сообщений алгоритмами, описанными в пунктах 1-5.
1. Расшифровать криптограмму Цезаря.
2. Перевести текст с «тарабарской» грамоты.
3. Расшифровать постолбцовый вариант маршрутной транспозиции.
4. Расшифровать сообщение с девизом «Я помню чудное мгновенье».
5. Расшифровать криптосистему Кардано.

Вариант 1.

1. ефвнгв жлччзузрщлуцзпгв чцрнщлв рзтузуюерг.
2. хифпь нметмалпа цшуря шебари – ифугепиер ракеракити и её нменоцашапиер.
3. тояаи овпдт лррлн ьеиеа кмнжм.
4. дбъх всеюъцн ихчвутйытнпгущн рё всн ч тстюутапйе.
5. сетсчт водблл еемчег кдуаер укаеив аьмаоо.

x				x	
			x		x
	x		x		
				x	
		x	x		

Вариант 2.

1. рльхс рз езьрс тсж оцрсб.
2. паута лкапошикля ноцсиппой паутой ш кой лкенепи, ш татой носьфуекля ракеракигелтири рекоцари.
3. сттлёбео тььпекс ыкешасни даченпиш икепыемь чпмотчос елбтентя саормен*.
4. мю ачьйуют пэрчг ыу муюин нэ рют очхсь р рсф яырчюеч.
5. нтипиа кдныпм аегари ояакии нзаткм аымоср.

	x			x	
x		x		x	
	x	x			
			x		x

Вариант 3.

1. лфхсулв цьлх ьхс рлнгнгв еогфхэ рз дюегзх езьрсм.
2. паута щеф ракеракити – пе паута.
3. смауамр ычнчеуа пееттчд олпоаеу зооопме нвтноут аеозтос ёкмноня.
4. ряямпмобмш жпыойькпн нугфяуцр ёесьртзз вэтсбза.
5. еесрсв снеиив мтенто итоттн смжмоа мьйено.

	x				
x				x	
	x				x
			x		
			x		
x		x			

Вариант 4.

1. лфхсульзфнл тзуеюз еюдсую тусыол е Лцжзз тул Тсрхлл Тлогхз.
2. тшапкошый торньюкем шфсораек сющую лошмереппую тминкочмази-гелтую лилкеру.
3. сеяое лоддн утегн чклоы арате йыюоу нттвм ыиплы.
4. люхъь ёчгфьачы тьучеаш ж яьуэцик бд ыуцчсщкму щбч.
5. тулоеш рпжчет нлиины сжнорй ьзнмса аоррои.

		x			
x			x		
				x	
			x		x
	x				
x				x	

Вариант 5.

1. нултхсёугчлв угкугдгхюегзх пзхсжю кгълхю лрчсупгщлл сх рзфгрнщлсрлуегррсёс.
2. ащцикишпая чмунна л цоноспикесьпой онемадией урпохепия, лшяфап-пой ло лсохепиер фатопари цилкмищукишполки, пафншаекля тосьдор.
3. сзветмт лаельае емлонял дыивазь оскеуан влоккна аягааия тмоесм∗ ьичсаа∗.
4. ю ввя фг шдтячрюв п ежтам пкфбчц ж яуётятаоян д фщью.
5. хнтпны сеторь астеоа якпарм воесвх оороин.

					x

		x			
x					
			x		
x		x		x	x
			x		

Вариант 6.

1. хзсулв ьлфзо фзмьгф схрсфлхфв н угкувжц тулногжрюш ргцн.

2. гер пешехелкшеппей гесошет, кер щосее оп ушемеп, гко илкипа у нечо ш тамрапе.

3. ундити миетьт нклевб еаёреы икнязт монедь ейотен юойсзи щпцянг иребад йелыче.

4. оаэсшфаь фнртзш пумчьмуб эо ыяъ зуёый ссйсв ууоко.

5. ястоео аомаол зивзст икмило ыиисмв тиктсв.

x		x		x	
			x		
			x		
	x				x
x				x	

Вариант 7.

1. нгйжюм еютцфнрлн дёцлу цезузррс еогжззх нсптэбхзусп.

2. пи оцип шекем пе щуцек нонукпыр цся томащся, токомый пе шывес иф чашапи.

3. клшуе тслтр ояяро нртув ааьда узтнт чмооь иымв∗.

4. оюсхоггп ст ачэгёьв зтмуэ яэчн яьычъачоцтб ойеое.

5. деуоля уртаеь тнаеом оеьртн юкетжо чбзссу.

		x			
	x		x		x
x					
		x			
			x		x
x					

Вариант 8.

1. пухл – уцк хесзм пзьхю.
2. чмарр шоси шелик кяхесее, гер депкпем малллухцепия и ущехцепия.
3. уоори мтрдт гпеца ирчее боиит нтймс еисия твеп∗.
4. рыуон аищ цнщлс хмьхряы цсаоеыщб лфны ьсуыэл иниа.
5. елзэта еыьбзн надчтм сиюкыд вуанст ттеяёа.

			x		x
				x	
		x			x
				x	
x			x		
	x				

Вариант 9.

1. носж ызррср веовзхфв сфрсестсосйрлнсп фсеузпзррсм кгълхю лрчсупгщлл.
2. рылсь ифмегеппая елкь сохь.
3. хняде оезур ррард оыщнр шлиыу иутхг ечамо мшоаг аатно.
4. оющм ъщ иёфьчс ьоньэ тн эшггзст ийв ць руьоьзвйа еъ.
5. ионквн йводаи гессир всуйсе терукт мныотс.

					x
	x	x			
x					x
x			x	x	
	x				

Вариант 10.

1. тсжелж ц нсхсуёс ефз аозпзрхю сдугхлпю схрсфлхзоэрс стузжоиррсм е рзп гоёздугльзфнсм стзугщлл ргкюегзхфв ёуцттсм.
2. кьры пифтиж илкип пар цомохе Пал шофшываюбий ощрап
3. ссхгй рлолц еедаа дпнзр иыоыь
4. дбъх м ль ддяжнбубм ячь юаппхсыжь т ст юушцев йеебч.
5. иеируу буешсе ввррыи йлчсмн глаатт бусыйы.

	x			x	
	x				
x		x			x
				x	
			x		
					x

Вариант 11.

1. фхсмнсфхэ нултхсфлфхзпю уфг сдцфосезрг фосйрсфхэб еюьзфозрлв чурнщлл Амозуг.
2. елси оцип маф нохасеевь, гко пе лтафас, ко лко маф нохасеевь, гко пе нморосгас.
3. жоьне еибег лдажо атвет юиела щсдащ еуёюи гдтщт.
4. рюъъдг ихиачч ьумыр ж рзеж эчдтбё еиоу лмун эётнжу.
5. рбкжнв мреешл ыокзот мионат ачнуаь омаьею.

	x	x			
		x		x	
	x				
			x		x
	x				x

Вариант 12

1. гулчпзхлнг нсозщ ногффсе еюьзхсе озйлх е сфрсез прсёлш фсе-узпзррюш нултхсёугчльзфнлш флфхзп.
2. елси кы панмашисля т деси и лкапевь цомочою вшымякь тарпяри шо шлятую саюбюю лощату, ко пе цойцёвь цо пеё.
3. удстщч тлтьеа еянтйс шныопт еехвоь нсианю ичмре∗ еаеис∗.
4. бкжсщ йьесцщ тм нюйнбдк фнуйенру еётхнщ еьцёшгкс.
5. ркжодт ворйьц иедачи аасбис нтитси веоыаи.

	x				
x			x		
x		x			x
	x				
				x	

x					

Вариант 13

1. жегжщгхлозхрлм тгулйфнлм фхцжзрх Аегулфх Жгоцг кгосйло сфрсею фсеузпзррсм гоёздую жзевхргжщгхсёс езнг.
2. огепь лгалксишые сюци, машпо тат огепь пелгалкпые, оципатошо лтсоппы т гёмлкшолки.
3. кгеме тотнд одсоо моягс нбтот оиога гвмоё оаунт.
4. нв юсюгиёдыэжчл ъууч язевпущиу ижръо тс птьбйанд.
5. ьесрап яажуми аяисса бсоиая кетвос раьвск.

			x		
				x	x
			x		
x	x				
		x			x
					x

Вариант 14.

1. жлгёрсфхлнг жсфхлёог хгнлш цфтзшсе ьхс кжсусеюш обжзм тугнхльзфнл рз сфхгосфэ.
2. гко шы цесаси шо шмеря кеммома? я олкашасля хиш.
3. суое рттл аьае зитг угьк длно.
4. ръофшж гвкй ьу о рцд жцаш тяьучц ю ыяг пайв ааэ ххьжн.
5. еексрд арсусо эетьок яжитнг лренни иитмон.

		x		x	
		x			
x					
			x		
x		x		x	
					x

Вариант 15.

1. зфол обжзм щзрлхя тс угдсхз хс осыгжэ оцьыз обдсёс ьзосезнг ёсегулего гознфзм пгнфлпсель ёсуэнлм .

2. жморой угис оцпопочочо нмычакь.

3. киеуг антжл жьчау дятсб адоао яуемк смёаа валяя.

4. тььзч уёагеэп нонсрфьзщцээ рьеахдтб иы фаотуяон.

5. еатэте путдаа сооеыш назкмч тсаздн рюрнеи.

			x		
x					
x			x	x	
	x		x		
x				x	