Титульный лист методических рекомендаций и указаний, методических рекомендаций, методических указаний

Форма
Ф СО ПГУ 7.18.3/37

Министерство образования и науки Республики Казахстан

Павлодарский государственный университет им. С. Торайгырова

Кафедра Вычислительная техника и программирование

МЕТОДИЧЕСКИЕ УКАЗАНИЯ И РЕКОМЕНДАЦИИ

к лабораторным работам

по дисциплине Основы информационной безопасности

для студентов специальности 050704 Вычислительная техника и программное обеспечение

Павлодар

Лист утверждения методических рекомендаций и указаний, методических рекомендаций, методических указаний

Форма
Ф СО ПГУ 7.18.3/38

УТВЕРЖДАЮ
Проректор по УР
_____ Пфейфер Н.Э.
(подпись) (Ф.И.О.)
«___»_____201_г.

Составитель: ст. преподаватель _____Глазырина Н.С.

Кафедра Вычислительная техника и программирование

Методические указания рекомендации и указания

к лабораторным работам

по дисциплине Основы информационной безопасности

для студентов специальности 050704 Вычислительная техника и программное обеспечение

Рекомендовано на заседании кафедры
«_____»_____201__г., протокол №__

Заведующий кафедрой _____ Потапенко О.Г. «____» _____201__г
(подпись) (Ф.И.О.)
Одобрено УМС Физики, математики и информационных технологий
(наименование факультета)
«____»_____201__г., протокол №____
Председатель УМС _____ Муканова Ж.Г. «____» _____201__г
(подпись) **(Ф.И.О.)**
ОДОБРЕНО ОПиМОУП**:**
Начальник ОПиМОУП _____ Варакута А.А. «____» _____201__г
(подпись) (Ф.И.О.)

Одобрена учебно-методическим советом университета
«_____»_____201_г. Протокол №____

Лабораторная работа № 1

Тема: Криптография. Подстановочные шифры.

Цель работы: Изучить основные понятия криптографии, классификацию криптографических систем, подстановочный шифр Цезаря.

1. Теоретические сведения

1.2 Криптография: основные понятия.

С появлением и распространением компьютеров и средств автоматизированной информации возникла потребность в автоматизированных средствах защиты файлов и другой хранимой компьютерами информации. Особенно остро потребность в средствах защиты ощущается в многопользовательских системах, таких как системы с разделением времени, а также в системах, к которым можно получить доступ по обычным телефонным линиям связи или открытым компьютерным сетям. Поэтому для описания совокупности методов и средств, предназначенных для защиты данных и противодействия хакерам, стал применяться термин **компьютерная безопасность.**

Пожалуй, самым важным автоматизированным средством защиты сети и коммуникаций является шифрование.

Сообщение, требующее конфиденциальной передачи, принято называть **открытым текстом**. Процесс преобразования открытого текста с целью сделать непонятным его смысл для посторонних называется **шифрованием (зашифрованием).** В результате шифрования сообщения получается **шифртекст**. Процесс обратного преобразования шифртекста в открытый текст называется **дешифрованием (расшифрованием).** Наука, изучающая методы преобразования (шифрования) информации с целью её защиты от незаконных пользователей, называется **криптографией**.

С помощью рисунка 1 рассмотрим основные элементы схемы традиционного шифрования.

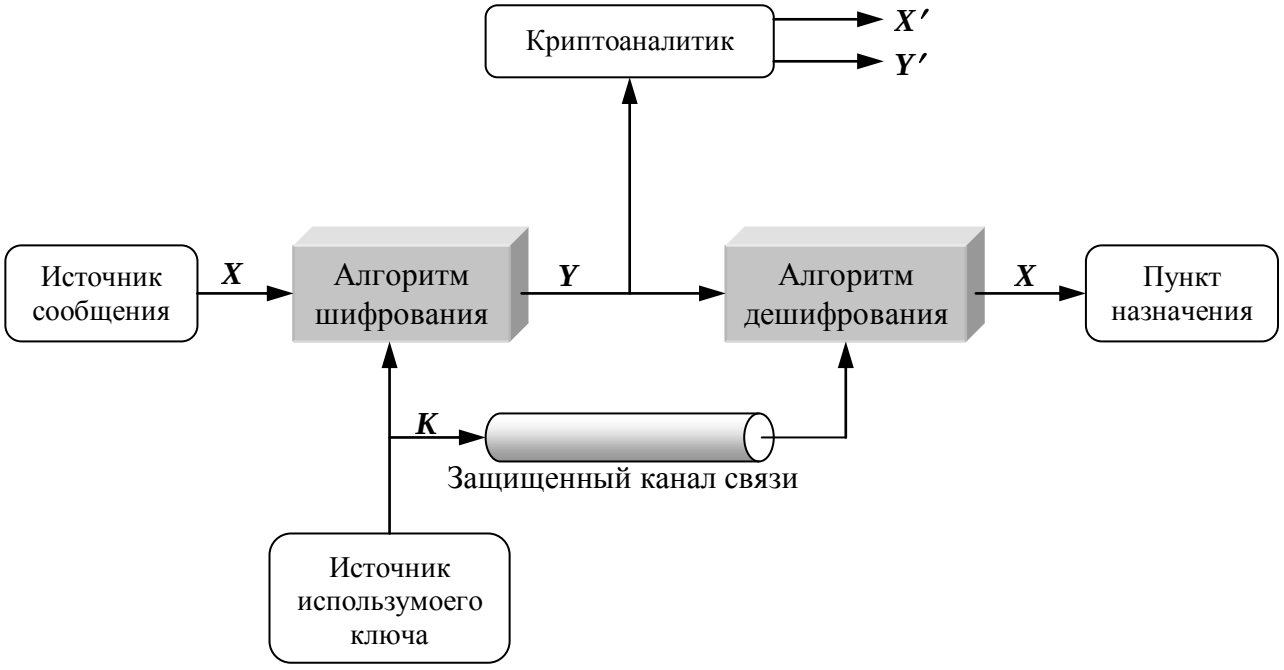


Рисунок 1 - Модель традиционной криптосистемы.

Источник создает сообщение в форме открытого текста $X=[X_1,X_2,\ldots, X_M]$. Элементами X_i открытого текста X являются символы некоторого конечного алфавита. Для шифрования генерируется ключ в форме $K=[K_1,K_2,\ldots, K_J]$. При наличии в качестве исходных данных сообщения X и ключа шифрования K с помощью алгоритма шифрования формируется шифрованный текст $Y=[Y_1,Y_2,\ldots, Y_N]$. Это можно записать в виде формулы

$$Y=E_K(X).$$

Данная нотация означает, что Y получается путем применения алгоритма шифрования *E* к открытому тексту X при использовании ключа K.

Предполагаемый получатель сообщения, располагая ключом K, должен иметь возможность выполнить обратное преобразование

$$X=D_K(Y).$$

Противник, обладающий возможностью ознакомиться с Y, но не имеющий доступа ни к K, ни к X, может попытаться восстановить X или K или оба этих объекта. При этом подразумевается, что противник знает и алгоритм шифрования (E), и алгоритм дешифрования (D). Если противник заинтересован распознать только одно конкретное сообщение, ему следует сосредоточить свои усилия на восстановлении X путем построения вероятно соответствующего исходному открытого текста X′. Однако чаще противник бывает заинтересован в получении возможности читать и все последующие сообщения. В этом случае его основные усилия должны быть сосредоточены на восстановлении K путем построения вероятно соответствующего исходному ключа K′.

Процесс воссоздания значений X или K, или и того, и другого, называется **криптоанализом.** Человека, занимается криптоанализом, называют **криптоаналитиком.**

1.3 Классическая техника шифрования. Применение подстановок.

При подстановке отдельные буквы открытого текста заменяются другими буквами или числами, либо какими-то иными символами. Если открытый текст рассматривается как последовательность битов, то постановка сводится к замене заданных последовательностей битов открытого текста заданными последовательностями битов шифрованного текста.

Шифр Цезаря.

Самым древним и самым простым из известных подстановочных шифров является шифр, использовавшийся Юлием Цезарем. В шифре цезаря каждая буква алфавита заменяется буквой, которая находится на три позиции дальше в этом же алфавите. При этом алфавит считается «циклическим», т.е. за буквой Я следует буква А. Например, для алфавита

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

шифрование происходит следующим образом:

Открытый: К Р И П Т О Г Р А Ф И Я

Шифрованный: Н У Л Т Х С Ж У Г Ч Л В

Определить преобразование можно, перечислив все варианты, как показано ниже.

Открытый текст: 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

Шифрованный текст: 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

Если каждой букве назначить числовой эквивалент (А = 1, Б = 2 и т.д.), то алгоритм шифрования можно выразить следующими формулами. Каждая буква открытого текста *P* заменяется буквой шифрованного текста C:

$$C = E(P) = (P+3) \bmod (26).$$

В общем случае сдвиг может быть любым, поэтому общий алгоритм Цезаря записывается формулой

$$C = E(P) = (P+k) \bmod (26),$$

где *k* принимает значения в диапазоне от 1 до 31 (для рассмотренного алфавита). Алгоритм дешифрования также прост:

$$P = D(C) = (C-k) \bmod (26).$$

Если известно, что определенный текст был зашифрован с помощью шифра Цезаря, то с помощью простого перебора всех вариантов раскрыть шифр очень просто – для этого достаточно проверить 31 возможный вариант ключа.

Применение метода последовательного перебора всех возможных вариантов оправдано следующими тремя важными характеристиками данного шифра.

1. Известны алгоритмы шифрования и дешифрования.
2. Необходимо перебрать всего 31 вариант.
3. Язык открытого текста известен и легко узнаваем.

В большинстве случаев, когда речь идет о защите компьютерной информации, можно предполагать, что алгоритм известен. Единственное, что делает криптоанализ на основе метода последовательного перебора практически бесполезным – это применение алгоритма, для которого требуется перебрать слишком много ключей.

2. Задание.

Вариант задания определяется последней цифрой номера зачетной книжки (0 соответствует 10 варианту).

Сообщения создаются и шифруются на базе алфавита

АБВГДЕЖЗИЙКЛМНОПРСТУФХЦЧШЩЪЫЬЭЮЯ.

Имеется шифрованный текст (см. таблицу 1), полученный с помощью шифра Цезаря. Величина используемого при этом сдвига неизвестна. Расшифруйте сообщение.

Таблица 1 - Варианты условий к заданию.

№ варианта	**Задание**
1.	ИЦРХЭЫЩШШЩРЬЩЦМДРШУРМЮПРЭЪЩЬЭРЪРШШЩТЛЧ РШКЭЗЩМЖВШЩРМЮЧЛСШЩРЬЩЦМДРШУР
2.	ФГМКРОНФЩЗТЪЦФЫКШНФНХРТЦЛМИЩЪШИХГЙЫМЫЪЧНШНЩН ЯНХГЩНЪЗФРЧНШНМИЯРМИХХГЭ
3.	ВЦЫБЦГЮМЦСФЦЮГВГУСЩЭЦПГХЯВГДАЫЖЯБЯЙЦЪЫБЩАГЯФБСЕ ЩИЦВЫЯЪГЦЖЮЯЬЯФЩЦЩ
4.	КЭЧУЙЧБЗЪАДЮНЮКБИЭКЗШФДЙНОЮБМЬЙББЙБДИБЗД

	АКНОПЛЬЖЖ МДЛОКЯМЬРДУБНЖДИОБСЙКЗКЯДЫИЮКБЙЙКЯКПМКЮ ЙЫ
5.	ТБВРЭФРАВЭЛЕЪАШЯВЮУАРДШЗХБЪШЕБШБВХЬРЕШБЯ ЮЫМЧГХВБП ЮФШЭШВЮВЦХЪЫОЗШФЫПИШДАЮТРЭШПШФЫПАРБ ИШДАЮТЪШ
6.	ШАЖЮЕИДЩЖЦКЮНЫЗАДЯЗЮЗИЫВЫЗДИАЖСИСВАБФ НДВАЦЬЪСЯЮ ВЫЫИЪШЦЗШХЭЦГГСЛШЭЦЮВГДАБФНЦ
7.	ШОФТЙЧШЩМЕТУЖЦВЮБУАШЬТ,ЯТУЩОЫЫЙЧЯЭЬЪЬЗ КМТЮБСЬСЬ ШЩМЕО
8.	ПМЯПРАГЛЛЩЗПГИОГРЛЩЗИЙЬХМРНОЮАЖРГЙЭКМДГР ЯЩРЪЖПНМЙ ЪЕМАЮЛВЙЭЦЖТОМАИЖПММЯЧГЛЖЭ
9.	ЙЧСЦЮЬЪЩЩМЛЫЪРЫФЭИЭЪЪНЕСЩФЛРЪЦМУЗОМСЮ ГЮЪЪЮЫЬМО ФЮСЧСШНЗЧРСХЭЮОФЮСЧИЩЪЭЪУРМЮСЧИЭЪЪНЕС ЩФЛ
10.	ЖКВИУКУЭВГЦПАНИШЕЧКЙЧЪЪАЬЭЙЭИКАМАВШКЖЪВ ГЦПЭБВЖКЖ ИУЭЪВГЦПШЦКЪЙЭЩЧАЬЭЕКАМАВШКЖИЗЖГФЯЖЪШК ЭГЧ

Контрольные вопросы:

1. Приведите примеры нарушений защиты.
2. Дайте определение следующим терминам: конфиденциальность, аутентификация, целостность, невозможность отречения, управление доступом, доступность.
3. Чем отличаются пассивные нарушения защиты от активных нарушений? Приведите примеры.
4. Опишите модель традиционной криптосистемы.

Лабораторная работа № 2

Тема: Моноалфавитные и полиалфавитные шифры.

Цель работы: Изучить моноалфавитные шифры: шифр Плейфейера, шифр Хилла и полиалфавитный шифр Виженера.

1. Теоретические сведения

1.1 Моноалфавитные шифры.

При наличии всего 31 возможного варианта ключей шифр Цезаря далек от того, чтобы считаться надежно защищенным. Существенного расширения пространства ключей можно добиться, разрешив использование произвольных подстановок.

Например, если в шифре Цезаря допустить использование любой из перестановок 31 символа алфавита, а не только сдвигом на *k* символов, то мы получим 31! Возможных ключей. Пример ключа такого шифра приведен ниже.

Открытый текст: 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

Шифрованный текст: Й Р Ж Ь Ш Л Я Е В Ъ Ф К М Б С Ч Ю А Ц И Э Щ Ы Н У П Г Х Т Д О З

Пример шифрования с использованием этого ключа:

Открытый:	К	Р	И	П	Т	О	Г	Р	А	Ф	И	Я
Шифрованный:	Ф	Ю	В	Ч	Ц	С	Ь	Ю	Й	Э	В	З

Создается впечатление, что 31! (что превышает 8×10^{33}) ключей не так то просто перебрать, и данный шифр обладает высокой степенью надежности. Однако для криптоаналитика существует и другая линия атаки. Если криптоаналитик имеет представление о природе открытого текста (например, о том, что это текст на английском языке), можно использовать известную информацию о характерных признаках, присущих текстам на соответствующем языке.

На рисунке 1 приведена относительная частота использования букв в английском тексте. Поскольку одна и та же буква открытого текста соответствует одной и той же букве ключа, то на первом этапе дешифрования криптоаналитик может провести анализ частоты использования букв в зашифрованном тексте и установить примерное соответствие между символами шифртекста и алфавита (например, согласно диаграмме рисунка 1, скорее всего, часто используемый символ шифртекста соответствует букве Е). Далее можно использовать тот факт, что в английском языке самой распространенной триграммой (т.е. комбинацией из трех букв) является the, что позволит частично восстановить открытый текст и утвердиться в предполагаемом ключе. Продолжая анализ, можно получить точное содержание текста.

Моноалфавитные шифры легко раскрываются, так как наследуют частотность употребления букв оригинального алфавита. Контрмерой в данном случае является применение для одной буквы не одного, а нескольких заменителей (называемых **омофонами**). Если число символов-заменителей, назначенных букве, выбрать пропорциональным частоте появления этой буквы, то подсчет частоты употребления букв в шифрованном тексте становится бессмысленным. Но даже при употреблении омофонов каждому элементу открытого текста соответствует только один элемент шифрованного текста, поэтому в последнем по-прежнему должны наблюдаться характерные показатели частоты повторения комбинаций нескольких букв (например, биграмм), и в результате задача криптоанализа по-прежнему остается достаточно элементарной.

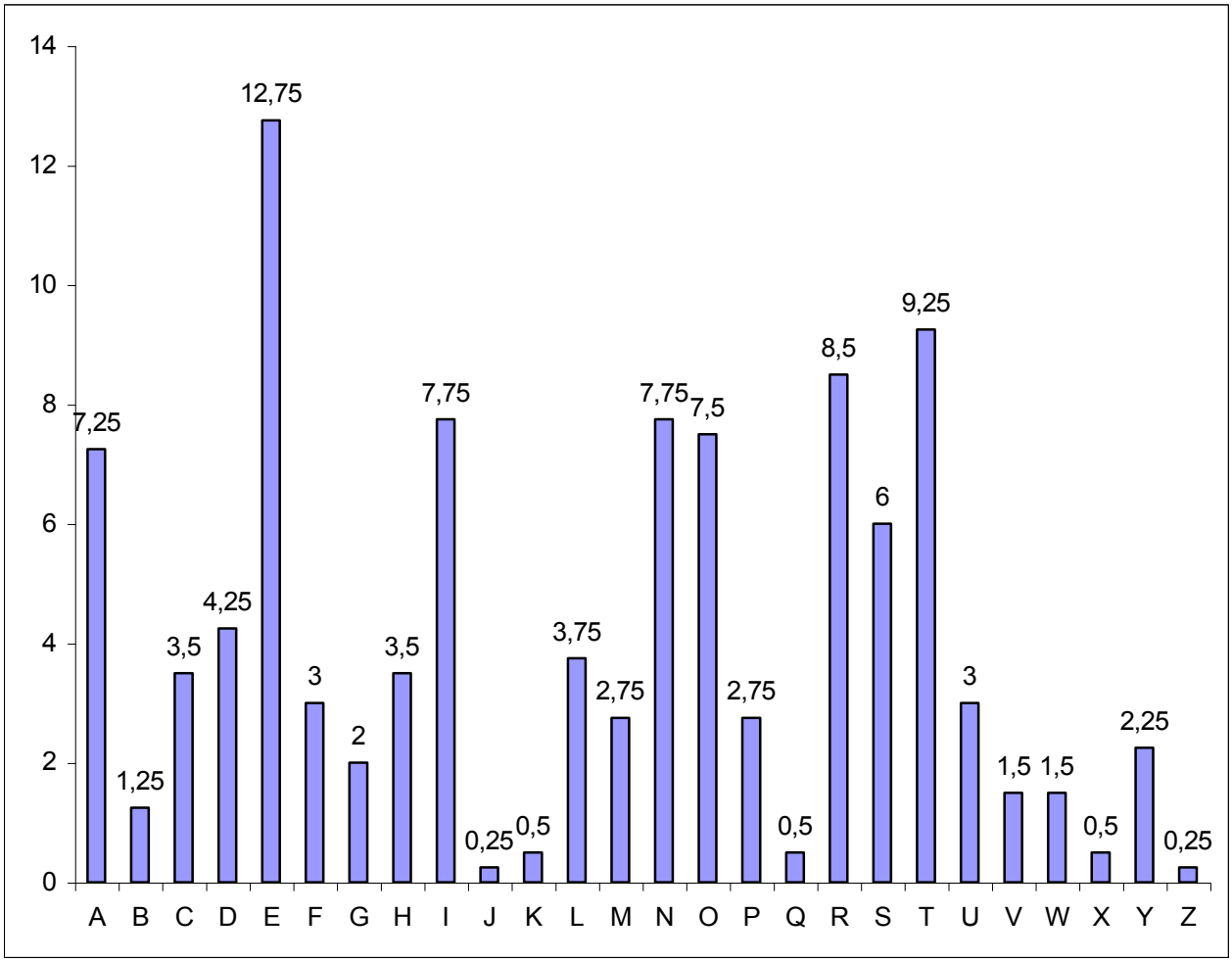


Рисунок 1 - Относительная частота появления букв в английском алфавите.

Чтобы в тексте, шифрованном с помощью методов подстановок структура исходного текста проявлялась менее заметно, можно использовать два принципиально разных подхода. Один из них заключается в замещении не отдельных символов открытого текста, а комбинаций нескольких символов, а другой подход предполагает использование для шифрования нескольких алфавитов.

Шифр Плейфейера.

Одним из наиболее известных шифров, базирующихся на методе многобуквенного шифрования, является шифр Плейфейера (Playfair), в котором биграммы открытого текста рассматриваются как самостоятельные единицы, преобразуемые в заданные биграммы шифрованного текста.

Алгоритм Плейфейера основан на использовании матрицы букв размерности 5×5, созданной на основе некоторого ключевого слова. Матрица создается путем размещения букв, использованных в ключевом слове, слева направо и сверху вниз. Затем оставшиеся буквы алфавита размещаются в естественном порядке в оставшихся строках и столбцах матрицы. Буквы I и J считаются одной и той же буквой. Ниже приведен пример такой матрицы для ключевого слова **monarchy** (монархия).

M	O	N	A	R
C	H	Y	B	D
E	F	G	I/J	K

L	P	Q	S	T
U	V	W	X	Z

Открытый текст шифруется порциями по две буквы в соответствии со следующими правилами.

1. Если оказывается, что повторяющиеся буквы открытого текста образуют одну пару для шифрования, то между этими буквами вставляется специальная буква-заполнитель, например *X*. В частности, такое слово как **balloon** будет преобразовано к виду ba lx lo on.
2. Если буквы открытого текста попадают в одну и ту же строку матрицы, каждая из них заменяется буквой, следующей за ней в той же строке справа – с тем условием, что для замены последнего элемента строки матрицы служит первый элемент той же строки. Согласно выше построенной матрицы AR шифруется как RM.
3. Если буквы открытого текста попадают в один и тот же столбец матрицы, каждая из них заменяется буквой, состоящей в том же столбце сразу под ней, с тем условием, что для замены самого нижнего элемента столбца матрицы берется самый верхний элемент того же столбца. В примере выше MU шифруется как CM.
4. Если не выполняется ни одно из приведенных условий, каждая буква из пары букв открытого текста заменяется буквой, находящейся на пересечении содержащей эту букву строки матрицы и столбца, в котором находится вторая буква открытого текста. Например, HS шифруется как BP, а EA – как IM (или JM, по желанию шифровальщика).

Шифр Плейфейера значительно надежнее простых моноалфавитных шифров. С одной стороны, букв всего 26, а биграмм - 26×26 = 676, и уже поэтому идентифицировать биграммы сложнее, чем отдельные буквы. С другой стороны, относительная частота появления отдельных букв колеблется гораздо в более широком диапазоне, чем частота появления биграмм, поэтому анализ частотности употребления биграмм тоже оказывается сложнее анализа частотности употребления букв. По этим причинам очень долго считалось, что шифр Плейфейера взломать невозможно. Он служил стандартом шифрования в Британской армии во время первой мировой войны и нередко применялся в армии США и союзных войсках даже в период второй мировой войны.

Несмотря на столь высокую репутацию в прошлом, шифр Плейфейера на самом деле вскрыть относительно легко, так как шифрованный с его помощью текст, все равно сохраняет многие статистические характеристики открытого текста. Для взлома этого шифра, как правило, достаточно иметь шифрованный текст, состоящий из нескольких сотен букв.

Шифр Хилла.

Еще одним интересным многобуквенным шифром является шифр, разработанный математиком Лестером Хиллом (Lester Hill) в 1929 году. Лежащий в его основе алгоритм заменяет каждые **m** последовательных букв открытого текста **m** буквами шифрованного текста. Подстановка определяется **m** линейными уравнениями, в которых каждому символу присваивается числовое значение (A = 0, B = 1, …, Z = 25). Например, при **m** = 3 получаем следующую систему уравнений:

$$C_1 = (k_{11}p_1 + k_{12}p_2 + k_{13}p_3) \bmod 26,$$
$$C_2 = (k_{21}p_1 + k_{22}p_2 + k_{23}p_3) \bmod 26,$$
$$C_3 = (k_{31}p_1 + k_{32}p_2 + k_{33}p_3) \bmod 26.$$

Эту систему можно записать в виде произведения вектора и матрицы в следующем виде:

$$\begin{pmatrix} C_1 \\ C_2 \\ C_3 \end{pmatrix} = \begin{pmatrix} k_{11} & k_{12} & k_{13} \\ k_{21} & k_{22} & k_{23} \\ k_{31} & k_{32} & k_{33} \end{pmatrix} \times \begin{pmatrix} p_1 \\ p_2 \\ p_3 \end{pmatrix}$$

или в виде

$$\mathbf{C} = \mathbf{K} \times \mathbf{P},$$

где **C** и **P** - векторы длины 3, представляющие соответственно шифрованный и открытый текст, а **K** – это матрица размерности 3×3, представляющая ключ шифрования. Операции выполняются по модулю 26.

Рассмотрим, например, как будет зашифрован текст «PAYMOREMONEY» при использовании ключа

$$K = \begin{pmatrix} 17 & 17 & 5 \\ 21 & 18 & 21 \\ 2 & 2 & 19 \end{pmatrix}.$$

Первые три буквы открытого текста представлены вектором (15 0 24). Таким образом, **K**(15 0 24) = (275 819 486) mod 26 = (11 13 18) = LNS. Продолжая вычисления, получим для данного примера шифрованный текст LNSHDLEWMTRW.

Для расшифровки нужно воспользоваться матрицей, обратной **K**. Обратной по отношению к матрице **K** называется такая матрица $\mathbf{K}^{-1}$, для которой выполняется равенство $\mathbf{K} \times \mathbf{K}^{-1} = \mathbf{K}^{-1} \times \mathbf{K} = \mathbf{I}$, где **I** – это единичная матрица (матрица, состоящая из нулей всюду, за исключением главной диагонали, на которой находятся единицы). Обратная матрица существует не для всякой матрицы, однако, когда обратная матрица имеется, для неё обязательно выполняется приведенное выше равенство. В нашем примере обратной матрицей является матрица

$$K^{-1} = \begin{pmatrix} 4 & 9 & 15 \\ 15 & 17 & 6 \\ 24 & 0 & 17 \end{pmatrix}$$

Это проверяется следующими вычислениями:

$$\begin{pmatrix} 17 & 17 & 5 \\ 21 & 18 & 21 \\ 2 & 2 & 19 \end{pmatrix} \times \begin{pmatrix} 4 & 9 & 15 \\ 15 & 17 & 6 \\ 24 & 0 & 17 \end{pmatrix} = \begin{pmatrix} 443 & 442 & 442 \\ 858 & 495 & 780 \\ 494 & 52 & 365 \end{pmatrix} \bmod 26 = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}$$

Легко проверить, что в результате применения матрицы $\mathbf{K}^{-1}$ к шифрованному тексту получается открытый текст.

Обратная матрица квадратной матрицы $\boldsymbol{A}$ вычисляется как $[\boldsymbol{A}^{-1}]_{ij} = (-1)^{i+j} (\mathbf{D}_{ij})/\det(\boldsymbol{A})$, где $(\mathbf{D}_{ij})$ – определитель матрицы, получаемой путем удаления *i*-й строки и *j*-го столбца из матрицы $\boldsymbol{A}$, а $\det(\boldsymbol{A})$ – определитель самой матрицы $\boldsymbol{A}$. В нашем случае все вычисления проводятся по модулю 26.

В общем виде систему Хилла можно записать в следующей форме:

$$\mathbf{C} = E_K(\mathbf{P}) = \mathbf{KP},$$
$$\mathbf{P} = D_K(\mathbf{C}) = \mathbf{K}^{-1}\mathbf{C} = \mathbf{P}.$$

Как и в случае шифра Плейфейера, преимущество шифра Хилла состоит в том, что он полностью маскирует частоту вхождения отдельных букв. А для шифра Хилла чем больше размер матрицы в шифре, тем больше в шифрованном тексте скрывается информация о различиях в значениях частоты появления других комбинаций символов.

Так, шифр Хилла с матрицей 3×3 скрывает частоту появления не только отдельных букв, но и двухбуквенных комбинаций.

1.2 Полиалфавитные шифры. Шифр Виженера.

Другая возможность усовершенствования простого моноалфавитного шрифта заключается в использовании нескольких моноалфавитных подстановок, применяемых в ходе шифрования открытого текста в зависимости от определенных условий. Семейство шрифтов, основанных на применении таких методов шифрования, называется **полиалфавитными шифрами**. Подобные методы шифрования обладают следующими общими свойствами.

1. Используется набор связанных моноалфавитных подстановок.
2. Имеется некоторый ключ, по которому определяется, какое конкретное преобразование должно применяться для шифрования на данном этапе.

Самым широко известным и одновременно самым простым алгоритмом такого рода является шифр Виженера (Vigenure). Этот шифр базируется на наборе правил моно алфавитной подстановки, представленных 26 шифрами Цезаря со сдвигом от 0 до 25 (для латинского алфавита). Каждый из таких шифров можно обозначить ключевой буквой, являющейся буквой шифрованного текста, соответствующего букве A открытого текста. Например, шифр Цезаря, для которого смещение равно 3, обозначается ключевой буквой D.

Для облегчения понимания и применения этой схемы была предложена матрица, названная «табло Виженера» (см. таблицу 1). Все 26 шифров располагаются по горизонтали, и каждому из шифров соответствует своя ключевая буква, представленная в крайнем столбце слева. Алфавит, соответствующий буквам открытого текста, находится в первой сверху строке таблицы. Процесс шифрования прост – необходимо по ключевой букве ***x*** и букве открытого текста **y** найти букву шифрованного текста, которая находится на пересечении строки ***x*** и столбца **y**. В данном случае такой буквой является буква V.

Чтобы зашифровать сообщение, нужен ключ, имеющий туже длину, что и само сообщение. Обычно ключ представляет собой повторяющееся нужное число раз ключевое слово, чтобы получить строку подходящей длины. Например, если ключевым словом является **deceptive,** сообщение «we are discovered save yourself» шифруется следующим образом:

```
Открытый текст:     D E C E P T I V E D E C E P T I V E D E C E P T I V E
Ключ:               W E A R E D I S C O V E R E D S A V E Y O U R S E L F
Шифрованный текст: Z I C V T W Q N G R Z G V T W A V Z H C Q Y G L M G J
```

Расшифровать текст также просто – буква ключа определяет строку, буква шифрованного текста, находящаяся в этой строке, определяет столбец, и в этом столбце в первой строке таблицы будет находиться соответствующая буква открытого текста.

Преимущество этого шифра заключается в том, что для представления одной и той же буквы открытого текста в шифрованном тексте имеется много различных вариантов – по одному на каждую из неповторяющихся букв ключевого слова. Таким образом, скрывается информация, характеризующая частотность употребления букв. Но и с помощью данного метода все же не удается полностью скрыть влияние структуры открытого текста на структуру шифрованного. Повысить надежность шифра поможет использование ключа, длина которого совпадает с длиной сообщения, а текстовые характеристики максимально отклонены от стандартных характеристик языка открытого текста.

Таблица 1 - Табло Виженера.

	a	b	c	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z

a	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
b	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A
c	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B
d	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C
e	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D
f	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E
g	G	H1	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F
h	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G
i	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H
j	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I
k	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J
l	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K
m	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L
n	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M
o	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N
p	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O
q	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P
r	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q
s	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R
t	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S
u	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T
v	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U
w	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V
x	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W
y	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X
z	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y

2. Задание.

При использовании шифра Плейфейера на базе русского языка из алфавита удаляются буквы Ё (заменяется буквой Е) и буква Й (заменяется буквой И). Буквы Ъ и Ь считаются одной и той же буквой. Матрица букв строится на алфавите

АБВГДЕЖЗИКЛМНОПРСТУФХЦЧШЩЪЫЬЭЮЯ,

состоящем из 31 буквы, и состоит из 5 строк и 6 столбцов. Например, матрица букв на базе ключевого слова ПАРУСНИК будет выглядеть следующим образом:

П	А	Р	У	С	Н
И	К	Б	В	Г	Д
Е	Ж	З	Л	М	О
Т	Ф	Х	Ц	Ч	Ш
Щ	Ъ/Ь	Ы	Э	Ю	Я

Возьмите из таблицы 2 ключевое слово и последовательность символов, соответствующие Вашему варианту. Используя ключевое слово и шифр Плейфейера, закодируйте фразу «КОД ПЛЕЙФЕЙЕРА ОСНОВАН НА ИСПОЛЬЗОВАНИИ МАТРИЦЫ БУКВ» и декодируйте указанную в задании последовательность символов.

Таблица 2 - Варианты условий к заданию.

№ варианта	**Задание**
1.	Ключевое слово: ПОЛЕТ Строка для декодирования: КЛКЕПЕШОБКЕРЭЛЧСКУЛЮЕТВМВКИММЮЗОТЖША
2.	Ключевое слово: ФИЛЬМ Строка для декодирования: НПВЪЗПЖИКЛБЦРПЪПЭИЯЩЛИЗПБКФАГПШУХЭЧЖРЫВЦТУНЧТЩЧНХНЩТНЯХКДНЦВЗТЧИ
3.	Ключевое слово: КАТЕР Строка для декодирования: ЗЛНЖКГСЩЯЪАОЕСМЩЯСОЛКДБОУЩФРКЖФТАРТЮВИОАСЫЫРМРЕПМЩ
4.	Ключевое слово: ПАРОЛЬ Строка для декодирования: ЮОГНФПЛМКЮМВРМХИНЦШБЛГЖМУПЕАЮЖЧЗПДАМАЛНЪЖЕАДПУНЕЛСЪМЧПМЪЗЧЪЭАЩЩНТЗЗУАД
5.	Ключевое слово: КОЛЬЦА Строка для декодирования: МИПГПДПМЖВТЩВИЕИЛРЩЧЗОЛИНЦЩХЖПЪРВЦТУОЖАЫВХУКЖЕВИ
6.	Ключевое слово: КАМЕНЬ Строка для декодирования: РСРФЪПЧСВЛНПНЪСШТОБСХЪИЪФОПГИМФАНЪУКГЩЛНВНКХЧЪДУНЛМАХКСЛИЧТБЕУ
7.	Ключевое слово: СОЛНЦЕ Строка для декодирования: ЗОИЦОЫИТЗУСОШЖАЦФАВЗЗКЗЧНБЗЖУКПБЕЫТЗЪЗФЩ
8.	Ключевое слово: ТОВАРИЩ Строка для декодирования: МОЩЕЯВЧЪЛТАПЯВМОМРЗФИЫПТБКВИХБЦБЩШЪЧШЩИВТЧОАДХОПАБТИВАРМЖИ
9.	Ключевое слово: СВЯЗЬ Строка для декодирования: ЛМЧШЮГХТЯПХООПКПЖМКЧВЦАОБФЖГКХПНЯВЖФЪЛЯНХОФЗТЪСЦПИЛФЛЪ
10.	Ключевое слово: МАТЕРИЯ Строка для декодирования: УЕНАЕЭМЧЗПФТКСЪИАРУЕПЕСЯЕХТИСЩГХМЖФЗЧБГЩКМЮАЕЪ

Контрольные вопросы:

1. Какие шифры относятся к моноалфавитным? Приведите примеры.
2. Сколько возможных ключей позволяет использовать шифр Плейфейра? Выразите ответ в приблизительной оценке степени 2.
3. Какие шифры относятся к полиалфавитным? Приведите примеры.
4. Какими свойствами обладают полиалфавитные шифры?
5. Что такое биграмма?

Лабораторная работа № 3

Тема: Перестановочные шифры.

Цель работы: Изучить перестановочные шифры. Шифр «Лесенка». Шифр вертикальной перестановки. Шифр «Поворотная решетка».

1. Теоретические сведения

1.1. Применение перестановок.

Все рассмотренные ранее методы основывались на замещении символов открытого текста различными символами шифрованного текста. Принципиально иной класс преобразований строиться на использовании перестановок букв открытого текста. Шифры, созданные с помощью перестановок, называют **перестановочными** шифрами.

Шифр «Лесенка».

Простейший из таких шифров использует преобразование «лесенки», заключающейся в том, что открытый текст записывается вдоль наклонных строк определенной длины («ступенек»), а затем считывается построчно по горизонтали. Например, чтобы шифровать сообщение «шифр с использованием перестановки» по методу лесенки со ступеньками длиной 2, запишем это сообщение в виде

Ш Ф С С О Ь О А И М Е Е Т Н В И
И Р И П Л З В Н Е П Р С А О К

Шифрованное сообщение будет иметь следующий вид.

ШФССОЬОАИМЕЕТНВИИРИПЛЗВНЕПРСАОК

Шифр вертикальной перестановки.

Шифр «Лесенка» особой сложности для криптоанализа не представляет. Более сложная схема предполагает запись текста сообщения в горизонтальные строки одинаковой длины и последующее считывание текста столбец за столбцом, но не по порядку, а в соответствии с некоторой перестановкой столбцов. Порядок считывания столбцов при этом становиться ключом алгоритма. Ниже приведен пример шифрования фразы «ПЕРЕСТАНОВКА ТЕКСТА ПО СТОЛБЦАМ» с ключом 4312567.

Ключ:	4	3	1	2	5	6	7
Открытый текст:	П	Е	Р	Е	С	Т	А
	Н	О	В	К	А	Т	Е
	К	С	Т	А	П	О	С
	Т	О	Л	Б	Ц	А	М

Шифрованный текст: РВТЛЕКАБЕОСОПНКТСАПЦТТОААЕСМ

Простой перестановочный шифр очень легко распознать, так как буквы в нем встречаются с той же частотой, что и в открытом тексте. Например, для только что рассмотренного способа шифрования с перестановкой столбцов анализ шифра выполнить достаточно просто – необходимо записать шифрованный текст в виде матрицы и перебрать возможные варианты перестановок для столбцов.

Перестановочный шифр можно сделать существенно более защищенным, выполнив шифрование с использованием перестановок несколько раз. Оказывается, что в этом случае примененную для шифрования перестановку воссоздать уже не так просто. Например, если предыдущее сообщение шифровать еще раз с помощью того же самого алгоритма, то результат будет следующим.

Ключ:	4	3	1	2	5	6	7
Открытый текст:	Р	В	Т	Л	Е	К	А
	Б	Е	О	С	О	П	Н
	К	Т	С	А	П	Ц	Т
	Т	О	А	А	Е	С	М

Шифрованный текст: ТОСАЛСААВЕТОРБКТЕОПЕКПЦСАНТМ

Шифр «Поворотная решетка».

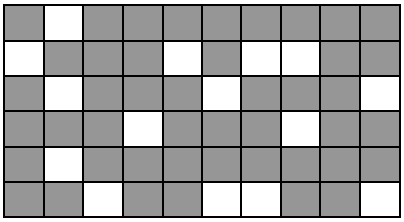
Для использования шифра, называемого поворотной решеткой, изготавливается трафарет из прямоугольного листа клетчатой бумаги размером 2m × 2n клеток. В трафарете вырезано m × n клеток так, что при наложении его на чистый лист бумаги того же размера четырьмя возможными способами его вырезы полностью покрывают всю площадь листа.

Буквы сообщения последовательно вписываются в вырезы трафарета (по строкам, в каждой строке слева направо) при каждом из четырех его возможных положений в заранее установленном порядке.

Рассмотрим процесс шифрования на примере. Пусть в качестве ключа используется решетка 6 × 10, приведенная на рисунке 3, а. Зашифруем с ее помощью текст

ШИФРРЕШЕТКАЯВЛЯЕТСЯЧАСТНЫМСЛУЧАЕМШИФРАМАРШРУТНОЙПЕРЕСТАНОВКИ.

а)



б)

	Ш								
И				Ф		Р	Р		
	Е				Ш				Е
			Т				К		
	А								
		Я			В	Л			Я

в)

Е	Ш		Т	С			Я		
И				Ф		Р	Р	Ч	
	Е	А			Ш	С			Е
			Т	Н			К	Ы	
	А	М	С		Л				У
		Я			В	Л		Ч	Я

г)

Е	Ш	А	Т	С	Е	М	Я		Ш
И	И			Ф		Р	Р	Ч	
	Е	А	Ф		Ш	С	Р		Е
Т	А		Т	Н	М		К	Ы	А
Р	А	М	С	Ш	Л	Р	У		У
	Т	Я			В	Л		Ч	Я

д)

Е	Ш	А	Т	С	Е	М	Я	Н	Ш
И	И	О	Й	Ф	П	Р	Р	Ч	Е
Р	Е	А	Ф	Е	Ш	С	Р	С	Е
Т	А	Т	Т	Н	М	А	К	Ы	А
Р	А	М	С	Ш	Л	Р	У	Н	У
О	Т	Я	В	К	В	Л	И	Ч	Я

Рисунок 1 - Пример шифрования текста методом поворотной решетки.

Наложив решетку на лист бумаги, вписывается первые 15 (по числу вырезов) букв сообщения. Результат после снятия решетки изображен на рисунке 1, б. Повернув решетку на 180 градусов и вписав следующие 15 букв, получаем лист, изображенный на рисунке 1, в. Перевернув лист и проделав то же самое, шифруется остаток текста (рисунок 1, г и д).

Получатель сообщения, имеющий точно такую же решетку, без труда прочтет исходный текст, наложив решетку на шифртекст по порядку четырьмя способами.

Число трафаретов, то есть количество ключей шифра «решетка», составляет $T = 4^{mk}$. Этот шифр предназначен для сообщений длины $n = 4mk$. Уже при размере трафарета 8×8 число возможных решеток превосходит 4 миллиарда.

2. Задание

Вариант задания определяется последней цифрой номера зачетной книжки (0 соответствует 10 варианту).

Сообщения создаются и шифруются на базе алфавита

АБВГДЕЖЗИЙКЛМНОПРСТУФХЦЧШЩЪЫЬЭЮЯ.

Задание1. К открытому тексту был применен шифр «Лесенка». Восстановите сообщение по шифрованному тексту из таблицы 1.

Таблица 1 - Варианты условий к заданию.

№ варианта	**Задание**
1.	ВЩИТЗЬВЬЛОНЕНИУШИЗЕГАЕТСЮЕНОЙОСВЕПТПЫВЗШТРРО БОПАЕАО МНЛОЛОТМРЯЯЕЬЛОЛЕНА
2.	ЛЕСЕПЕУЕОНЬНЯПЗННМИЬУИЩЮДТКРТЮБПОХЕИООИФАЕН ШЕИБЕВО ОИЩЕАСРНИЛВЯОЦСАЕЗТОЙИММРЕЗСТАИСЬАИРИТРНАЫ
3.	МЕЕЕСНЬМТПЦСНРЧЯТЫЗДОЕЕТОЫЕТИСООВЧЛИГЧСЕСИВКИ ЕОИЕКЛВ САУОНСЕЛОЬЯПНМБИТСОЙНЗОИЕЕЕНФВДОАЛЕНСМО
4.	ВРОСМЕННАЗАРТМНММММИМНИАКНФЦЯСОВУЕАДЕНАНСХ ТАОИЛЕЛО ЮЕЖОНФЦЫТЭРЯРЯАБЬДРБНКТОИХЕЛОИМВНЯОИАУЫУА
5.	САААИАЕЬДЛЬЩКТСЕМИБСДОЧКЕЬХЕОЕИИАСЕНОБИОННРЙМ РСНЦТЗОЛ ЕВНЦОАСПНТФИЕОСЖСАФИСНЯЬОЕОИМПТНПТИАТЯВЮЙМ

	Р
6.	ОЗСЗСЕСЕОИИИЩДАТОТТПНЙФИКЕНДЕПИСЕАИИСАНОАМА ЯЧДДКТС ИЙЧЫСВОЕЕЕАООЯИСБНЛБНЖНЦЧОЗИЕОЯЕИНТИНБ
7.	СЕЕАСБЕАЕМООЧЯРТОКЕАОЕИМЗСТЕЧЕВОСТЕОАЕТТРЧОНС АОНИСИТО ЖТРНТВЛФАЕИБИТБПООПВНЗНЬЕИПИЯАПДСЩЯ
8.	ОИЯИОРИОМТБЕДННСТРЕВЕКОФНАЬОШАСОСОЫМОНАПНТР МИТНТЕТ УМРЗПЕЕЧРПАЕБОГЛЕОАЦСАСОЬНЛКИУВТВС
9.	ПВАНЩОАЕИНРИЫЯТЗТЫАНРИИСРРТГЕДХВСРЕМСЫУЯТЯАМ ОАДАИЛЯУ ЛИСЕШЗЫТКОРПАННЯРШЬИНЕАНХТНИЕЧНЕЮАИН
10.	КЕЬИАНЗПДООИАЕИООННННЦААОАТЖЕЛССВНЦОФИЧЩТНВН ГИКСАФИС ОИАИОНОООТОЛНИАТРОЕТКЫЗСАИГЕИДЛЬМЗТУАХМТНЧОД Я

Задание 2. В ходе анализа ряда перехваченных сообщений, шифруемых методом вертикальной перестановки, криптоаналитиками был частично восстановлен используемый при этом ключ. В частности, они определили количество символов в ключе, а так же числовые значения некоторых позиций. Результат работы криптоаналитиков представлен в виде строки, длина которой совпадает с длиной ключа, а символом X отмечены позиции ключа, значения которых на текущий момент неизвестны (см. задание в таблице 2). От Вас требуется по имеющемуся шифртексту закончить восстановление ключа и получить открытый текст, соответствующий шифрованному сообщению.

Таблица 2 - Варианты условий к заданию.

№ варианта	**Задание**
1.	Зашифрованный текст: ФТБЕОЗРЬЩМАОСЕОИАОИНШВОНЖ Частично восстановленный ключ: XX5X1
2.	Зашифрованный текст: ПНОСОЕЕНМРЗОЮЯАЬЬАПТКТБС Частично восстановленный ключ: 6XX1X4
3.	Зашифрованный текст: ОННАНЦОНДЛЬХФИСНИАТЫКЕЬД Частично восстановленный ключ: XX24X3
4.	Зашифрованный текст: СИВОСЕНЕЗОПЕОПТОЧЕБСЕСЙАИБЕТЕН Частично восстановленный ключ: 4XX13X
5.	Зашифрованный текст: СНСКЫЕЕОАНОЕЕУАБЧДПНПИТДМ Частично восстановленный ключ: 3XXX5
6.	Зашифрованный текст:

	АКДВСЕШНЛСООСИЫАЧЕФЯКЕТРИМИИ Частично восстановленный ключ: 63XX27X
7.	Зашифрованный текст: ИАОТЮОЕРКМФНТЫЧРИКМОШВСЫЛ Частично восстановленный ключ: XX3X2
8.	Зашифрованный текст: ЛЩЕОЬИЙМААТЛНТОАОЯСВКЗЕЗЛААТ Частично восстановленный ключ: 7XX3X24
9.	Зашифрованный текст: СУХЫЫМИЗЕМТРОТНАНЦПЙАЗИАЛЕИЩФИЬМЗИОИ Частично восстановленный ключ: 2XX3X6
10.	Зашифрованный текст: БСЕАГНМЗЛАЕООЯНПЛТБНАЕЕСЬЬЕА Частично восстановленный ключ: 2X41XX7

Контрольные вопросы:

1. На чем основывается метод перестановок?
2. Оцените надежность шифра «Лесенка».
3. Дайте определение абсолютной защищенности.

ЛИТЕРАТУРА

Основная:

1. Столлингс В. Криптография и защита сетей: принципы и практика, 2-е изд.: Пер. с англ. – М.: Издательский дом «Вильямс», 2001. - 672 с.
2. Анин Б.Ю. Защита компьютерной информации. – СПб.: БХВ – Санкт-Петербург, 2000. - 384 с.
3. Введение в криптографию / Под общей ред. В.В. Ященко. – СПб.: Питер, 2001. – 288с.

Дополнительная:

1. Жельников В. криптография от папируса до компьютера. М.: ABF, 1996
2. Саломаа А. Криптография с открытым ключом. М.: Мир, 1995.