Лабораторная работа № 2
КЛАССИЧЕСКИЕ МЕТОДЫ ШИФРОВАНИЯ

Цель работы

Познакомиться с основными криптографическими терминами и моделью традиционного шифрования. Изучить типы криптосистем. Изучить особенности классических методов шифрования на примере конкретных алгоритмов.

Теоретические сведения

Основные понятия

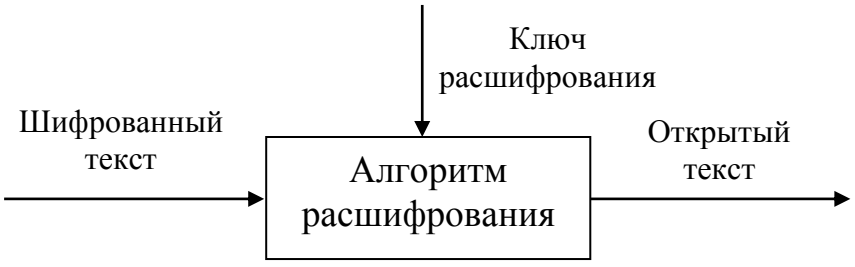
Шифрование (encryption) – обратимое преобразование информации с помощью одного из алгоритмов и ключа. По-русски - зашифрование.

Исходное сообщение называется **открытым текстом (plaintext).**

Зашифрованное сообщение называется **шифром, шифротекстом (ciphertext).**

Таким образом, на вход алгоритма шифрования поступает открытый текст и ключ, а в результате выполнения алгоритма получается шифрованный текст.

Расшифрование (decryption) – процедура, обратная шифрованию, преобразование шифртекста в открытый текст с помощью алгоритма и ключа лицами, владеющими ключом на законном основании.



Криптосистема – алгоритм шифрования и соответствующий ему алгоритм расшифрования.

Дешифрование (deciphering) (взлом, вскрытие шифра) - восстановление исходного текста без знания ключа.

Введем математические обозначения.

Источник создает сообщение в форме открытого текста:

$$\mathbf{P = [p_1, p_2, \ldots, p_m]}$$

Текст – упорядоченный набор элементов.

Все элементы p_i открытого текста P принадлежат некоторому конечному алфавиту A, состоящему из N символов:

$$\mathbf{p_i \in A}$$

Раньше в качестве алфавитов шифрования использовались алфавиты естественных языков – русского, английского т.д. В настоящее время, когда криптографические алгоритмы реализуются программными средствами, используется двоичный алфавит – (0, 1).

Для шифрования генерируется ключ в форме:

$$\mathbf{K = [к_1, к_2, \ldots, к_j]}$$

Ключ К принадлежит пространству ключей. **Пространство ключей** – множество всех возможных ключей, доступных для использования в алгоритме.

Шифрованный текст обозначим С:

$$\mathbf{C = [c_1, c_2, \ldots, c_n]}$$

Процесс шифрования можно описать следующим образом:

$$\mathbf{C = E_k(P)}$$

Обратное преобразование, расшифрование:

$$\mathbf{P = D_k\,(C)}$$

Методы шифрования применяются не одну тысячу лет. **Классическими шифрами** называются шифры, которые использовались в докомпьютерную эпоху. В настоящее время они не применяются на практике, так как легко взламываются с помощью современных вычислительных средств. Однако классические шифры представляют исторический и учебный интерес, поскольку основаны на тех же принципах, что и современные шифры. Все они относятся к более широкой группе симметричных шифров. Примерами классических шифров являются шифры Цезаря, Трисемуса, Плейфейера, Уитстона, Виженера, Вернама, «Магический квадрат» и другие.

Симметричные шифры (симметричные криптосистемы) - это шифры, в которых для шифрования и расшифрования используется один и тот же ключ. Их называют еще **традиционными криптосистемами, криптосистемами с одним ключом** или **криптосистемами с секретным ключом.** Современные симметричные шифры широко применяются на практике. Модель шифрования с секретным ключом была предложена Клодом Шенноном, основателем теории информации.

Примечание:

Во многих алгоритмах шифрования используется операция mod.

Операция ***a (mod n)*** для целых чисел a и n называется ***приведением a по модулю n***. Результат операции должен быть равен положительному целому числу от 0 до n-1.

При программной реализации криптографического алгоритма операция mod может быть заменена на операцию целочисленного деления, т.е. нахождения остатка от деления a на n. При этом надо учитывать, что определение операции mod в модулярной арифметике может отличаться от принятого в некоторых языках программирования. Например, в языке C оператор % возвращает остаток от деления первого выражения на второе, который может быть отрицателен.

Во всех криптографических алгоритмах, если операция mod возвращает отрицательное число, необходимо прибавить значение модуля n к результату операции.

Обобщенный алгоритм 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 3 позиции дальше в этом же алфавите. Алфавит считается циклическим, то есть после Z идет A.

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

$$C = E_3(P) = (P + 3) \bmod(26),$$

где 26 – число букв в латинском алфавите; 3 – ключ.

В общем случае сдвиг может быть любым, поэтому **обобщенный алгоритм Цезаря** записывается формулой:

$$C = E_k(P) = (P + K) \bmod(N),$$

где K – ключ, который может принимать значения в диапазоне от 1 до 25; N - размерность алфавита.

Алгоритм расшифрования так же прост:

$$P = D_k(C) = (C - K) \bmod(N)$$

Шифр Цезаря легко вскрывается с помощью лобовой атаки или на основе анализа частот появления букв в шифртексте.

Система Цезаря с ключевым словом.

Особенностью этой системы является использование **ключевого слова** для смещения и изменения порядка символов в алфавите подстановки.

Выберем некоторое число k, 0 <= k < N-1 (N- размерность алфавита), и слово или короткую фразу в качестве ключевого слова. Желательно, чтобы все буквы ключевого слова были различными. В противном случае надо удалить повторяющиеся символы до шифрования.

Пусть выбран ключ:

- DIPLOMAT - ключевое слово;
- k = 5 - ключевое число.

Ключевое слово записывается под буквами алфавита, начиная с буквы, числовой код которой совпадает с выбранным числом k:

0 1 2 3 4 5
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
D I P L O M A T

Оставшиеся буквы алфавита подстановки записываются после ключевого слова в алфавитном порядке:

0 1 2 3 4 5
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
V W X Y Z D I P L O M A T B C E F G H J K N Q R S U

Достоинством системы Цезаря с ключевым словом является то, что количество возможных ключевых слов практически неисчерпаемо. Недостатком этой системы является возможность взлома шифра на основе анализа частот появления букв.

Шифр, использующий линейное преобразование

Алгоритм шифрования:

1) Определяем порядковый номер буквы в открытом тексте - n;
2) Определяем код буквы в алфавите: X;
3) Вычисляем смещение S по формуле:

$$S = (a*n + b) \bmod N$$

Пара чисел (a, b) – ключ шифрования;
N – количество символов в алфавите.

4) Определяем код буквы шифртекста в алфавите: $Y = (X+S) \bmod N$

Алгоритм расшифрования:

1) Определяем порядковый номер буквы в шифртексте - n;
2) Определяем код буквы шифртекста в алфавите - Y;
3) Вычисляем смещение - S;
4) Определяем код буквы открытого текста: $X = (Y-S) \bmod N$

Пример:

Возьмем русский алфавит – 33 буквы + «пробел».

N = 34

1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22
А	Б	В	Г	Д	Е	Ё	Ж	З	И	Й	К	Л	М	Н	О	П	Р	С	Т	У	Ф

23	24	25	26	27	28	29	30	31	32	33	34
Х	Ц	Ч	Ш	Щ	Ъ	Ы	Ь	Э	Ю	Я	

Зашифруем слово РЕПА с ключом (3, 1).

1. Определяем порядковый номер буквы Р в открытом тексте: n=1.

2. Определяем код буквы Р в алфавите: X=18.
3. Вычисляем смещение: S = (3 * 1+ 1) mod 34 = 4
4. Определяем код буквы шифртекста: (18+4) mod 34 = 22

Это буква Ф.

Продолжая шифрование согласно алгоритму, получим шифртекст: ФЛЩМ.

Шифр, использующий нелинейное преобразование

Отличается от предыдущего тем, что в ходе шифрования используется нелинейное преобразование:

$$S = (a*n^2 + b*n + c) \bmod N,$$

где (a,b,c) – ключ шифрования, N – размерность алфавита, n – порядковый номер буквы в открытом тексте.

Алгоритм шифрования: $C_i = (P_i + S_i) \bmod N$

Алгоритм расшифрования: $P_i = (C_i - S_i) \bmod N$

Пример:

Возьмем русский алфавит – 33 буквы + «пробел».

Зашифруем слово РЕСПУБЛИКА с ключом (8, 4, 9).

1. Определяем порядковый номер буквы Р в открытом тексте: n=1.
2. Определяем код буквы Р в алфавите: X=18.
3. Вычисляем смещение: $S = (8 * 1^2 + 4*1 + 9) \bmod 34 = 21$
4. Определяем код буквы шифртекста: (18+21) mod34 = 39 mod34 =5

Это буква Д.

Продолжая шифрование, получим шифртекст: ДУИ КП СЧ

Шифр, использующий сложение с ключевым словом

Если длина ключевого слова меньше, чем длина текста, то ключевое слово повторяется.

Алгоритм шифрования:

1) Определяем порядковый номер буквы в открытом тексте - i;
2) Определяем код i-й буквы текста в алфавите: X_i;
3) Определяем код i-й буквы ключа в алфавите: $К_i$;
4) Вычисляем код буквы шифртекста в алфавите:

$$У_i = (X_i + К_i) \bmod N$$

N – количество элементов в алфавите.

Алгоритм расшифрования:

1) Определяем порядковый номер буквы в открытом тексте - i;
2) Определяем код i-й буквы шифртекста в алфавите: Y_i;
3) Определяем код i-й буквы ключа в алфавите: $К_i$;
4) Вычисляем код буквы шифртекста в алфавите:

$$X_i = (У_i - К_i) \bmod N$$

Пример:

Возьмем русский алфавит – 33 буквы + «пробел».

1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22
А	Б	В	Г	Д	Е	Ё	Ж	З	И	Й	К	Л	М	Н	О	П	Р	С	Т	У	Ф

23	24	25	26	27	28	29	30	31	32	33	34
Х	Ц	Ч	Ш	Щ	Ъ	Ы	Ь	Э	Ю	Я	

Зашифруем слово РЕСПУБЛИКА с ключом КРЫША.

1. Определяем порядковый номер буквы Р в открытом тексте: n=1.
2. Определяем код буквы Р в алфавите: $X_1 = 18$.
3. Определяем код i-й буквы ключа в алфавите: $К_1 = 12$
4. Вычисляем код буквы шифртекста в алфавите:

$$У_i = (18 + 12) \bmod 34 = 30$$

Это буква Ь.

Продолжая шифрование согласно алгоритму, получим шифртекст: ЦМЗФМЭДГБ

Шифрующие таблицы Трисемуса

В 1508г. аббат из Германии Иоганн Трисемус впервые описал применение шифрующих таблиц, заполненных алфавитом в случайном порядке. Для получения такого шифра замены обычно использовались таблица для записи букв алфавита и ключевое слово, причем повторяющиеся буквы отбрасывались. Затем эта таблица дополнялась не вошедшими в нее буквами алфавита по порядку.

Пример.

Для русского алфавита шифрующая таблица может иметь размер 4х8. Выберем в качестве ключа слово БАНДЕРОЛЬ. Шифрующая таблица с таким ключом будет выглядеть следующим образом:

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

При шифровании находят в этой таблице очередную букву открытого текста и записывают в шифртекст букву, расположенную ниже ее в том же столбце. Если буква текста оказывается в нижней строке таблицы, то берут самую верхнюю букву из того же столбца.

Такие шифры называют **монограммными** и **моноалфавитными,** т.к. шифрование выполняется по одной букве и используется один алфавит.

Биграммный шифр Плейфейера

Одним из наиболее известных шифров, базирующихся на методе многобуквенного шифрования, является шифр Плейфейера, в котором биграммы открытого текста рассматриваются как самостоятельные единицы, преобразованные в заданные биграммы шифрованного текста. Он применялся Великобританией во время Первой мировой войны

Алгоритм Плейфейера основан на использовании матрицы букв размерности 5x5, созданной на основе некоторого ключевого слова.

Например:

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

В данном случае ключевым словом является monarchy(монархия). Матрица создается путем размещения букв, использованных в ключевом слове, слева направо и сверху вниз (повторяющиеся буквы отбрасываются). Затем оставшиеся буквы алфавита размещаются в естественном порядке в оставшихся строках и столбцах матрицы. Буквы I и J считаются одной и той же буквой. Открытый текст шифруется порциями по две буквы в соответствии со следующими правилами.

1. Если оказывается, что повторяющиеся буквы открытого текста образуют 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. Например, ar шифруется как RM.

3. Если буквы открытого текста попадают в один и тот же столбец матрицы, каждая из них заменяется буквой, стоящей 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. Например, mu шифруется как CM.

4. Если не выполняется ни одно из приведенных выше 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 «двойной квадрат» Уитстона

В 1854г. англичанин Чарльз Уитстон разработал новый метод шифрования биграммами. При этом используются сразу две таблицы, размещенные по одной горизонтали. Шифр оказался очень надежным и применялся Германией даже в годы Второй мировой войны.

Рассмотрим пример. Пусть имеются две таблицы со случайно расположенными в них русскими алфавитами. Перед шифрованием исходное сообщение разбивают на биграммы. Каждая биграмма шифруется отдельно. Первую букву биграммы находят в левой таблице, а вторую – в правой. Затем строят прямоугольник так, чтобы буквы биграммы лежали в его противоположных вершинах. Другие две вершины этого прямоугольника дают буквы биграммы шифртекста.

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

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

Предположим, что шифруется биграмма ИЛ. Буква И находится в столбце 1 и строке 2 левой таблицы. Буква Л в столбце 5 и строке 4 правой таблицы. Это означает, что прямоугольник образован строками 2 и 4, а также столбцами 1 и 5. Следовательно, в биграмму шифртекста входят буква О, расположенная в столбце 5 и строке 2 правой таблицы, и буква В, расположенная в столбце 1 и строке 4 левой таблицы.

Если обе буквы биграммы сообщения лежат в одной строке, то и буквы шифртекста берут из этой же строки. Первую букву биграммы шифртекста берут из левой таблицы в столбце, соответствующем второй букве биграммы сообщения. Вторая буква биграммы шифртекста берется из правой таблицы в столбце, соответствующем первой букве биграммы сообщения. Поэтому биграмма сообщения ТО превращается в биграмму шифртекста БЖ.

Для получения шифрующих таблиц можно использовать ключевые слова, аналогично шифру Трисемуса.

Шифр Виженера

Для усовершенствования простого моноалфавитного шифра можно использовать несколько моноалфавитных подстановок, применяемых в ходе шифрования открытого текста в зависимости от определенных условий. Семейство шифров, 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 простым алгоритмом такого рода является шифр Виженера (Vigenire). Этот шифр базируется на наборе правил моноалфавитной подстановки, представленных 26 шифрами Цезаря со сдвигом от 0 до 25. Каждый из таких шифров можно обозначить ключевой буквой 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". 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*.

Таблица 1. Современное 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	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
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

Чтобы зашифровать сообщение, нужен ключ, имеющий ту же 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.

Ключ: deceptivedeceptivedeceptive

Открытый текст: wearediscoveredsaveyourself

Шифрованный текст: zicvtwqngrzgvtsavzhcqyglmgj

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.

Шифрование методом Вернама

Метод предложен инженером компании AT&T Гилбертом Вернамом (Gilbert Vernam) в 1918г. Его система оперирует не буквами, а двоичными числами. Кратко ее можно выразить формулой

$$C_i = p_i \oplus k_i,$$

где

p_i - i-я двоичная цифра открытого текста,

k_i - i-я двоичная цифра ключа,

C_i - i-я двоичная цифра шифрованного текста.

$\oplus$ - операция XOR (исключающее "ИЛИ").

Таким образом, шифрованный текст генерируется путем побитового выполнения операции XOR для открытого текста и ключа. Благодаря свойствам этой операции для расшифровки достаточно выполнить подобную операцию:

$$p_i = C_i \oplus k_i.$$

Сутью этой технологии является способ выбора ключа. Вернам предложил использовать закольцованную ленту, что означает циклическое повторение ключевого слова, так что его система на самом деле предполагала работу хоть и с очень длинным, но все же повторяющимся ключом. Несмотря на то, что такая схема в силу очень большой длины ключа значительно усложняет задачу криптоанализа, схему, тем не менее, можно взломать, имея в распоряжении достаточно длинный фрагмент шифрованного текста, известные или вероятно известные фрагменты открытого текста либо и то, и другое сразу.

Перестановочные шифры

При шифровании с помощью перестановочных шифров элементы шифруемого текста переставляются по определенным правилам в пределах блока этого текста. В качестве ключа при этом могут использоваться:

- размер таблицы;

- слово или фраза, задающие перестановку:
- случайная последовательность натуральных чисел.

Одним из самых примитивных перестановочных табличных шифров является **простая перестановка**, для которой ключом служит размер таблицы. Исходное сообщение записывается в таблицу по столбцам, а затем считывается по строкам. При расшифровании действия выполняются в обратном порядке.

Несколько большей стойкостью к раскрытию обладает метод шифрования, называемый **одиночной перестановкой по ключу.** Он отличается от предыдущего тем, что столбцы таблицы переставляются по ключевому слову, фразе или набору чисел длиной в строку таблицы. Если в качестве ключа используется слово, то каждая его буква заменяется числом, согласно порядку следования букв в алфавите. Если буквы повторяются, они нумеруются слева направо. Например, ключевое слово «КОРОВА» заменяется на последовательность чисел 346521. После перестановки столбцов содержимое таблицы считывается по строкам.

Для обеспечения дополнительной стойкости можно повторно зашифровать сообщение, которое уже прошло шифрование. Такой метод шифрования называется **двойной перестановкой по ключу**. В случае двойной перестановки столбцов и строк таблицы перестановки определяются отдельно для столбцов и отдельно для строк. Ключом к шифру двойной перестановки служит последовательность номеров столбцов и номеров строк исходной таблицы.

Шифр «Магический квадрат»

В средние века для шифрования перестановкой применялись магические квадраты.

Магическими квадратами называют квадратные таблицы с вписанными в их клетки последовательными натуральными числами, начиная от 1, которые дают в сумме по каждому столбцу, каждой строке и каждой диагонали одно и то же число.

Примеры магических квадратов 4x4:

7	12	1	14
2	13	8	11
16	3	10	5
9	6	15	4

9	16	2	7
6	3	13	12
15	10	8	1
4	5	11	14

Шифруемый текст вписывали в магические квадраты в соответствии с нумерацией их клеток. Если затем выписать содержимое такой таблицы по строкам, то получится шифртекст, сформированный благодаря перестановке букв исходного сообщения. В те времена считалось, что созданные с помощью магических квадратов шифртексты охраняет не только ключ, но и магическая сила.

Пример магического квадрата и его заполнения сообщением: ПРИЛЕТАЮ ВОСЬМОГО

16	3	2	13
5	10	11	8
9	6	7	12
4	15	14	1

О	И	Р	М
Е	О	С	Ю
В	Т	А	Ь
Л	Г	О	П

Получаемый шифртекст: ОИРМ ЕОСЮ ВТАЬ ЛГОП

Задания на лабораторную работу

1. Изучить теоретические основы (Лекция 3 и методические указания к лабораторной работе).
2. Описать алгоритмы шифрования и расшифрования на контрольном примере.
3. Написать независимые программные модули, реализующие алгоритм шифрования и алгоритм расшифрования в соответствии с вариантом задания, указанным преподавателем.

При шифровании: вводить с клавиатуры ключ и открытый текст, выводить на экран шифртекст. При расшифровании: вводить с клавиатуры ключ и шифртекст, выводить на экран открытый текст.

В коде программы задать алфавит согласно варианту задания. При вводе открытого текста проверять его принадлежность указанному алфавиту. При вводе ключа проверять его принадлежность пространству ключей.

Криптосистему описать в виде класса. Алгоритмы шифрования и расшифрования реализовать как методы класса.

Варианты заданий указаны в таблице.

Варианты заданий	**Название алгоритма**	**Алфавит**
1	Обобщенный алгоритм Цезаря	Латинский (26 букв)
2	Система Цезаря с ключевым словом	Латинский
3	Шифр, использующий линейное преобразование	Латинский
4	Шифр, использующий нелинейное преобразование	Латинский
5	Шифр, использующий сложение с ключевым словом	Латинский
6	Шифрующие таблицы Трисемуса	Латинский (таблица 5x5)
7	Шифр Плейфейера	Латинский (таблица 5x5)

8	Шифр «двойной квадрат» Уитстона	Латинский (таблицы 5x5)
9	Шифр Виженера	Латинский
10	Шифр Вернама	ASCII-таблица
11	Простая перестановка	Латинский
12	Одиночная перестановка по ключу	Латинский
13	Двойная перестановка по ключу	Латинский
14	Шифрование с использованием «магических квадратов»	Латинский
15	Обобщенный алгоритм Цезаря	Русский + пробел
16	Система Цезаря с ключевым словом	Русский + пробел
17	Шифр, использующий линейное преобразование	Русский + пробел
18	Шифр, использующий нелинейное преобразование	Русский + пробел
19	Шифр, использующий сложение с ключевым словом	Русский + пробел
20	Шифрующие таблицы Трисемуса	Русский (таблица 4x8)
21	Шифр Плейфейера	Русский (таблица 4x8)
22	Шифр «двойной квадрат» Уитстона	Русский (таблица 5x7)
23	Шифр Виженера	Русский
24	Простая перестановка	Русский
25	Одиночная перестановка по ключу	Русский
26	Двойная перестановка по ключу	Русский
27	Шифрование с использованием «магических квадратов»	Русский
28	Шифр Плейфейера	Русский (таблица 5x7)

Содержание отчета по лабораторной работе

1. Цель работы.
2. Структура алгоритмов шифрования и расшифрования.
3. Описание алгоритмов шифрования и расшифрования на контрольном примере.
4. Описание программы (входные и выходные значения, классы, методы).
5. Листинг программы.
6. Результаты работы программы (скриншоты).

7. Выводы (что изучили, пример какого классического алгоритма рассмотрели, классифицировать рассмотренный алгоритм).

Для защиты лабораторной работы необходимо подготовить отчет, продемонстрировать работу программы согласно варианту задания, устно ответить на контрольные вопросы.

Контрольные вопросы

1. Сформулируйте правило Керкхоффа.
2. Что такое криптосистема, шифрование, расшифрование, алфавит, открытый текст, пространство ключей?
3. Какие криптосистемы называются симметричными? Нарисуйте модель симметричной криптосистемы, предложенную К. Шенноном, и запишите формулы шифрования и расшифрования?
4. По каким признакам классифицируются криптосистемы?
5. Какие криптосистемы называются блочными, какие – поточными?
6. Чем отличается расшифрование и дешифрование?
7. Поясните понятия криптография, криптология, криптоанализ, стеганография.
8. Какие системы шифрования называют классическими? Используют ли их на практике? Что общего у классических шифров с современными симметричными криптосистемами?
9. Что такое криптостойкость? В каком случае схема шифрования называется абсолютно стойкой? Приведите пример абсолютно стойкого шифра.
10. Какие криптосистемы называют защищенными по вычислениям?