ПОДСТАНОВОЧНЫЕ ШИФРЫ

Сущность подстановочного шифрования состоит в том, что, исходный текст (из множества M) и зашифрованный текст (из множества C) основаны на использовании одного и того же или разных алфавитов, а тайной или ключевой информацией является алгоритм подстановки.

Если исходить из того, что используемые алфавиты являются конечными множествами, то в общем случае каждой букве a_x алфавита A_M ($a_x \in A_M$) для создания сообщения M_i ($M_i \in M$) соответствует буква a_y или множество букв$\{A_{xC}\}$ для создания шифртекста C_i ($C_i \in C$). Важно, чтобы во втором случае любые два множества (например, $\{A_{xC}\}_b$ и $\{A_{xC}\}_n$, $b \neq n$, $1 \le b, n, x, y \le N$, N – мощность алфавита), используемые для замены разных букв открытого текста, не пересекались:

$$\{A_{xC}\}_b \cap \{A_{xC}\}_n = 0.$$

Если в сообщении M_i содержится несколько букв a_x, то каждая из них заменяется на символ a_y либо на любой из символов $\{A_{xC}\}$. За счет этого с помощью одного ключа можно сгенерировать различные C_i для одного и того же M_i. Так как множества $\{A_{xC}\}_b$ и $\{A_{xC}\}_n$ попарно не пересекаются, то по каждому символу C_i можно однозначно определить, какому множеству он принадлежит, и, следовательно, какую букву открытого сообщения M_i он заменяет. В силу этого открытое сообщение восстанавливается из зашифрованного однозначно.

Приведенные утверждения справедливы для следующих типов подстановочных шифров:

- *моноалфавитных* (шифры однозначной замены или простые подстановочные),
- *полиграммных*,
- *омофонических* (однозвучные шифры или шифры многозначной замены),
- *полиалфавитных*.

Кратко поясним особенности указанных шифров.

2.1.1. Моноалфавитные шифры подстановки

В данных шифрах операция замены производится только над каждым одиночным символом сообщения M_i. Для наглядной демонстрации шифра простой замены достаточно выписать под заданным алфавитом тот же алфавит, но в другом порядке или, например, со смещением. Записанный таким образом алфавит называют алфавитом замены.

Максимальное количество ключей для любого шифра этого вида не превышает $N!$, где N – количество символов в алфавите.

Для математического описания криптографического преобразования предполагаем, что зашифрованная буква a_y ($a_y \in C_i$), соответствующая символу a_x ($a_x \in M_i$), находится на позиции

$$y \equiv x + k \pmod{N}, \qquad (2.1)$$

где x, y – индекс (порядковый номер, начиная с 0) символа в используемом алфавите, k – ключ.

Для расшифрования сообщения C_i необходимо произвести расчеты обратные (2.1), т. е.:

$$x \equiv y - k \pmod{N}. \qquad (2.2)$$

Соотношениям (2.1) и (2.2) соответствует классический шифр подстановки: ***шифр Цезаря***. Согласно описаниям историка Светония в книге «Жизнь двенадцати цезарей» данный шифр использовался Гаем Юлием Цезарем для секретной переписки со своими генералами (I век до н.э.) [6] (в этой книге любознательный читатель найдет также много исторической информации по криптографии).

Пример 1. Имеем открытый текст M_i = «*cba*». На основе шифра Цезаря C_i = «*fed*».

Здесь k =3, N = 26. Первый символ открытого текста (*c*) имеет индекс 2 (помним, что начальный символ алфавита (*a*) имеет нулевой индекс). Значит, первый символ шифртекста (*c*) будет иметь индекс 2 + k = 5. А такой индекс в алфавите принадлежит символу *f* и т.д.

Известное послание Цезаря *VENI VIDI VICI* (в переводе на русский означает «Пришел, Увидел, Победил»), направленное его другу Аминтию после победы над понтийским царем Фарнаком, выглядело бы в зашифрованном виде так: *YHQL YLGL YLFL*.

Применительно к русскому языку суть его состоит в следующем. Выписывается исходный алфавит (А, Б, …, Я), затем под ним выписывается тот же алфавит, но с циклическим сдвигом на 3 позиции влево.

Существуют различные модификации шифра Цезаря, в частности, *Атбаш* и *лозунговый шифр*.

Атбаш. В Ветхом Завете существует несколько фрагментов из священных текстов, которые зашифрованы с помощью шифра замены, называемого Атбаш. Этот шифр состоит в замене каждой буквы другой буквой, которая находится в алфавите на таком же расстоянии от конца алфавита, как оригинальная буква – от начала. Например, в русском алфавите буква А заменяется на Я, буква Б – на Ю и т.д. В оригинальном Ветхом Завете использовались буквы еврейского алфавита. Так, в книге пророка Иеремии слово «Бабель» (Вавилон) зашифровано как «Шешах» [6].

Одним из существенных недостатков моноалфавитных шифров является их низкая криптостойкость. Зачастую метод криптоанализа базируется на частоте встречаемости букв исходного текста.

Если в открытом сообщении часто встречается какая-либо буква, то в шифрованном сообщении также часто будет встречаться соответствующий ей символ. Еще в 1412 г. Шихаба ал-Калкашанди в своем труде «Субх ал-Ааша» привел таблицу частоты появления арабских букв в тексте на основе анализа текста Корана. Для разных языков мира существуют подобные таблицы. Так, например, для букв русского алфавита по данным «Национального корпуса

русского языка» [7] (Корпус — это информационно-справочная система, основанная на собрании текстов на некотором языке в электронной форме. Национальный корпус представляет данный язык на определенном этапе (или этапах) его существования и во всём многообразии жанров, стилей, территориальных и социальных вариантов и т. п.) такая таблица выглядит следующим образом (таблица 2.1).

Таблица 2.1. Частота появления букв русского языка в текстах

№ п/п	Буква	Частота, %	№ п/п	Буква	Частота, %
1	О	10.97	18	Ь	1.74
2	Е	8.45	19	Г	1.70
3	А	8.01	20	З	1.65
4	И	7.35	21	Б	1.59
5	Н	6.70	22	Ч	1.44
6	Т	6.26	23	Й	1.21
7	С	5.47	24	Х	0.97
8	Р	4.73	25	Ж	0.94
9	В	4.54	26	Ш	0.73
10	Л	4.40	27	Ю	0.64
11	К	3.49	28	Ц	0.48
12	М	3.21	29	Щ	0.36
13	Д	2.98	30	Э	0.32
14	П	2.81	31	Ф	0.26
15	У	2.62	32	Ъ	0.04
16	Я	2.01	33	Ё	0.04
17	Ы	1.90			

Существуют подобные таблицы для пар букв (биграмм). Например, часто встречаемыми биграммами являются «то», «но», «ст», «по», «ен» и т.д. Другой прием взлома шифров основан на исключении возможных сочетаний букв. Например, в текстах (если они написаны без орфографических ошибок) нельзя встретить сочетания «чя», «щы», «ъъ» и т.п. Таблицы с частотами (вероятностями) встречаемости пар и большего числа буквосочетаний существуют для разных алфавитов. Пример использования частотных свойств символов алфавита английского языка для шифроанализа можно найти на станицах 17-19 пособия [8].

Система шифрования Цезаря с ключевым словом (лозунгом) также является *одноалфавитной системой подстановки*. Особенностью этой системы является использование *ключевого слова* (*лозунга*) для смещения и изменения порядка символов в алфавите подстановки (желательно, чтобы все буквы ключевого слова были различными). Ключевое слово пишется в начале алфавита подстановки.

Пример 2. Для шифра с использованием кодового слова «TABLE» исходный алфавит (первая строка) и алфавит подстановки (вторая строка) выглядят следующим образом:

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

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

Если M_i = '*HELLO* ', то C_i = '*FEJJN*', если же M_i = '*VENIVIDIVICI* ', то C_i = '*VEMGVGLGVGBG*'.

Метод можно видоизменить, если ключевое слово записывать начиная не с первого символа (нулевой индекс) во второй строке, а в соответствии с некоторым числом a: $0 \le a < N$. Рассмотрим систему на примере.

Пример 3. Выберем число a=10, и слово *information* в качестве ключа.

Ключевое слово записывается под буквами алфавита, начиная с буквы, индекс которой совпадает с выбранным числом a, как это показано в нижеследующей таблице:

0 1 2 3 4 5 10 15 20 25

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

I N F O R M A T

Как видим, повторяющиеся буквы (I, N и O – в конце слова) во второй строке не дублируются. Оставшиеся буквы алфавита подстановки записываются после ключевого слова в алфавитном порядке:

5 10 15

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

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

Если M_i = '*VENIVIDIVICI* ', то C_i = '*EUOYEYSYEYQY*'.

Расшифрование сообщения производится по правилу, которое мы рассматривали на выше проанализированных примерах.

Применяя одновременно операции сложения и умножения по модулю n над элементами множества (индексами букв алфавита), можно получить *систему подстановок*, которую называют ***аффинной системой подстановок Цезаря.*** Определим процедуру зашифрования в такой системе:

$$y \equiv ax + b \pmod{N}, \qquad (2.3)$$

где a и b – целые числа.

При этом взаимно однозначные соответствия между открытым текстом и шифртекстом будут иметь место только при выполнении следующих условий: $0 \le a, b < N$, наибольший общий делитель (НОД) чисел a, b равен 1, т.е. эти числа являются *взаимно простыми*.

Приме 4. Пусть N =26, a = 3, b = 5. Тогда, НОД (3, 26) = 1, и мы получаем следующее соответствие между индексами букв:

x	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
$3x+5$	5	8	11	14	17	20	23	0	3	6	9	12	15	18	21	24	1	4	7	10	13	16	19	22	25	2

Преобразуя числа в буквы английского алфавита, получаем следующее соответствие для букв открытого текста и шифртекста:

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

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

Если M_i = ‘*VENIVIDIVICI*’, то получение зашифрованного сообщения в деталях показывает таблица 2.2.

Таблица 2.2. Иллюстрация получения шифртекста на основе аффинной системы подстановок Цезаря

M_i	V	E	N	I	V	I	D	I	V	I	C	I
x	21	4	13	8	21	8	3	8	21	8	2	8
$y=3x + 5$	16	17	18	3	16	3	14	3	16	3	11	3
C_i	Q	R	S	C	Q	C	O	C	Q	C	L	C

Таким образом, зашифрованное сообщение будет таким: C_i = = ‘*QRSCQCOCQCLC*’.

Расшифрование основано на использовании соотношения

$$x \equiv a^{-1}(y+N-b) \pmod{N}, \qquad (2.4)$$

где a^{-1} – обратное к a число по модулю N, т. е. оно удовлетворяет уравнению $aa^{-1} \equiv 1 \bmod N$.

2.1.2. Полиграммные шифры

В таких шифрах одна подстановка соответствует сразу нескольким символам исходного текста.

Первым известным шифром этого типа является ***шифр Порты*** [9]. Шифр представляется в виде таблицы. Наверху горизонтально и слева вертикально записывался стандартный алфавит. В ячейках таблицы записываются числа в определенном порядке. Одним из возможных вариантов такой таблицы для алфавита русского языка будет показанная ниже таблица, точнее – ее фрагмент (таблица 2.3).

Таблица 2.3. Фрагмент шифра Порты для алфавита русского языка, состоящего из 33 букв

	А	**Б**	**В**		**Э**	**Ю**	**Я**
А	001	002	003		031	032	033
Б	034	035	036		064	065	066
В	067	068	069		097	098	099
Г	100	101	102		130	131	132

Ю	1024	1025	1026		1054	1055	1056
Я	1057	1058	1059		1087	1088	1089

Шифрование выполняется парами букв исходного сообщения. Первая буква пары указывает на строку, вторая – на столбец. В случае нечетного количества букв в сообщении M_i к нему добавляется вспомогательный символ, например, «А».

Пример 5. Исходное сообщение M_i = ‘ABBA’. Сообщение состоит из двух пар (биграмм): АВ и ВА и будет зашифровано так: 003067.

Другими известными полиграммными шифрами являются ***шифр Плейфера*** и ***шифр Хилла*** [9].

С точки зрения криптостойкости рассматриваемый тип шифров имеет преимущества перед моноалфавитными шифрами. Это связано с тем, что распределение частот групп букв значительно более равномерное, чем отдельных символов. Во-вторых, для эффективного частотного анализа требуется больший размер зашифрованного текста, так как число различных групп букв значительно больше, чем мощность алфавита.

2.1.3 Омофонические шифры

Омофонические шифры (*омофоническая замена*) или *однозвучные шифры подстановки* создавались с целью увеличить сложность частотного анализа шифртекстов путем маскировки реальных частот появления символов текста с помощью *омофонии*.

В 1401 г. Симеоне де Крема стал использовать таблицы омофонов для сокрытия частоты появления гласных букв в тексте при помощи более чем одной подстановки. Такие шифры позже стали называться *шифрами многозначной замены* или *омофонами* (омофоны – от греч. homos – одинаковый и phone – звук) – слова, которые звучат одинаково, но пишутся по-разному и имеют разное значение; очень много подобных слов содержит английский язык). Они получили развитие в XV веке. В книге «Трактат о шифрах» Леона Баттисты Альберти (итальянский ученый, архитектор, теоретик искусства, секретарь папы Климентия XII), опубликованной в 1466 г. [10], приводится описание шифра замены, в котором каждой букве ставится в соответствие несколько эквивалентов, число которых пропорционально частоте встречаемости буквы в открытом тексте, M_i. В этих шифрах буквы исходного алфавита соответствуют более чем одному символу из алфавита замены. Обычно символам исходного текста с наивысшей частотой дают большее количество эквивалентов, чем более редким символам. Таким образом, распределение частоты становится более равномерным, сильно затрудняя частотный анализ.

В таблице 2.4 представлен фрагмент таблицы подстановок для алфавита русского языка [11].

При шифровании символ исходного сообщения заменяется на любую подстановку из «своего» столбца. Если символ встречается повторно, то, как правило, используют разные подстановки. Например, исходное сообщение «АБРАМОВ» после зашифрования может выглядеть так: «357 990 374 678 037 828 175» [11].

Книжный шифр. Заметным вкладом греческого ученого Энея Тактика в криптографию является предложенный им так называемый книжный шифр [10, 11]. После Первой мировой войны книжный шифр приобрел иной вид. Шифрозамена для каждой буквы определялась набором цифр, которые указывали на номер страницы, строки и позиции в строке (вспомните пример использования такого шифра известными героями фильма «17 мгновений весны»). Даже с формальной стороны отсутствие полной электронной базы изданных к настоящему времени книг делает процедуру взлома шифра практически не выполнимой.

Таблица 2.4 Фрагмент таблицы подстановок для системы омофонов

№ п/п	А	Б	В	…	М	…	О	…	Р	…	Я
1	311	128	175	…	037	…	248	…	064	…	266
2	357	950	194	…	149	…	267	…	189	…	333
…	…	…	…	…	…	…	…	…	…	…	…
16	495	990	199	…	349	…	303	…	374	…	749
…	…		…	…	…	…	…	…	…	…	…
20	519		427	…	760	…	306	…	469	…	845
…	…		…	…	…	…	…	…	…		
32	637		524	…	777	…	432	…	554		
…	…		…				…	…	…		
45	678		644				824	…	721		
…	…						…	…	…		
47	776						828	…	954		
…	…						…				
80	901						886				
…							…				
110							903				

2.1.4. Полиалфавитные шифры

Полиалфавитные (или *многоалфавитные*) шифры состоят из нескольких шифров однозначной замены. Выбор варианта алфавита для зашифрования одного символа зависит от особенностей метода шифрования.

Диск Альберти. В «Трактате о шифрах» [10] Альберти приводит первое точное описание *многоалфавитного шифра* на основе *шифровального диска* (см. рис. 2.1).

Он состоял из двух дисков – внешнего неподвижного и внутреннего подвижного дисков, на которые были нанесены буквы алфавита. Процесс шифрования заключался в нахождении буквы открытого текста на внешнем диске и замене ее на букву с внутреннего диска, стоящую под ней. После этого внутренний диск сдвигался на одну позицию и шифрование второй буквы производилось уже по-новому шифралфавиту. Ключом данного шифра являлся порядок расположения букв на дисках и начальное положение внутреннего диска относительно внешнего.

Рисунок 2.1. Реплика диска Альберти, используемого Конфедерацией во время Гражданской войны в Америке [12]

Таблица Трисемуса. В 1518 году в развитии криптографии был сделан важный шаг благодаря появлению в Германии первой печатной книги по криптографии. Аббат Иоганнес Трисемус, настоятель монастыря в Вюрцбурге, написал книгу «Полиграфия», в которой он описал ряда шифров, один из которых развивает идею *многоалфавитной подстановки*. Зашифрование осуществляется так: заготавливается *таблица подстановки* (так называемая «*таблица Трисемуса*» – таблица со стороной равной N, где N – мощность алфавита), где первая строка – это алфавит, вторая – алфавит, сдвинутый на один символ, и т. д. При зашифровании первая буква открытого текста заменяется на букву, стоящую в первой строке, вторая – на букву, стоящую во второй строке, и т.д. После использования последней строки вновь возвращаются к первой.

Пример. Рассмотрим процесс зашифрования сообщения M_i = «*БГТУ*», используя таблицу, фрагмент которой показан на рисунке 2.2.

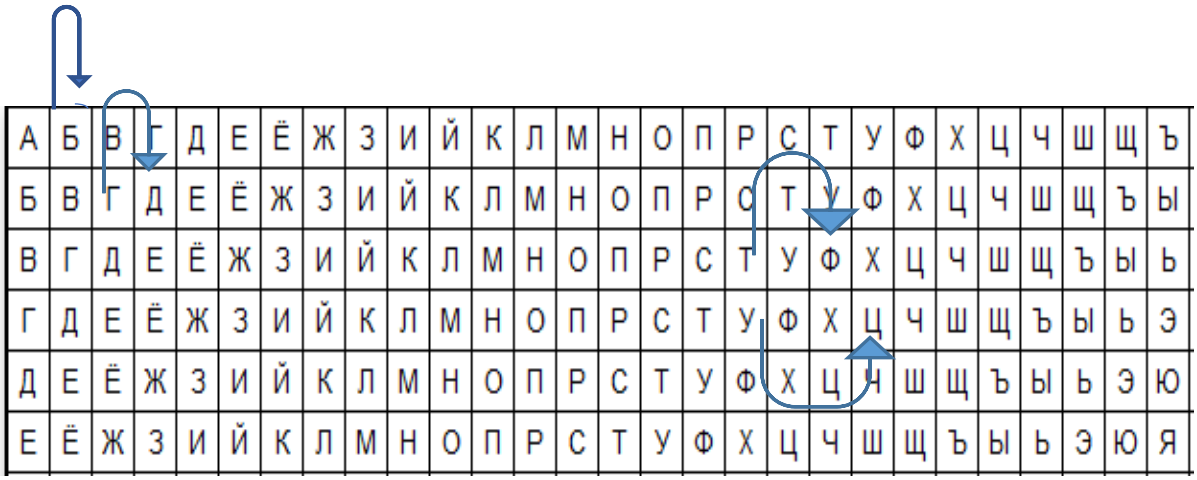


Рисунок 2.2 Фрагмент таблицы Трисемуса для алфавита русского языка

Стрелками на приведенном рисунке показан принцип зашифрования каждого символа открытого текста. Из этого следует, что шифртекст имеет вид: C_i = «*БДФЦ*».

В указанной книге Трисемус впервые систематически описал применение шифрующих таблиц, заполненных алфавитом в случайном порядке. Для получения такого шифра подстановки обычно использовались таблица для записи букв алфавита и *ключевое слово* (или фраза). Можно найти определенную аналогию с системой шифрования Цезаря с ключевым словом. В таблицу сначала вписывалось по стрелкам ключевое слово, причем повторяющиеся буквы также отбрасывались. Затем эта таблица дополнялась не вошедшими в нее буквами алфавита по порядку.

Таким образом, ключом в таблицах Трисемуса является ключевое слово и размер таблицы. При шифровании буква открытого текста заменяется буквой, расположенной ниже нее в том же столбце. Если буква текста оказывается в нижней строке таблицы, тогда для шифртекста берут самую верхнюю букву из того же столбца.

Указанный размер таблицы для алфавита русского языка может соответствовать 4х8 либо 8х4.

Пример 6. Пусть M_i = «*ПРИШЕЛУВИДЕЛПОБЕДИЛ*», а ключевое слово – «*ЦЕЗАРЬ*». Используем таблицу 8х4.

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

Следуя вышеуказанного принципу подстановки, получим C_i = = «*ФГМЭЫПШИМКЫПФУЖЫКМП*».

Шифр Виженера. В 1586 г. французский дипломат Блез Виженер представил перед комиссией Генриха III описание простого, но довольно стойкого шифра, в основе которого лежит таблица Трисемуса.

В этом шифре мы имеем дело с последовательностью сдвигов, циклически повторяющейся. Основная идея заключается в следующем. Создается таблица (таблица Виженера) размером $N \cdot N$ (N – число знаков в используемом алфавите). Эти знаки могут включать не только буквы, но и, например, пробел или иные знаки. В первой строке таблицы записывается весь используемый алфавит. Каждая последующая строка получается из предыдущего циклического сдвига последней на 1 символ влево. Таким образом, при мощности алфавита (английского языка) равной 26, необходимо выполнить последовательно 25 сдвигов для формирования всей таблицы.

Более подробное описание шифра можно найти, например, в [2] (с. 41–43).

Листинг 2.1 содержит часть кода, реализующего алгоритм шифрования Виженера.

Следует добавить, что в 1863 г. Фридрих Касиски опубликовал алгоритм атаки на этот шифр, хотя известны случаи его взлома шифра некоторыми опытными криптоаналитиками и ранее. В частности, в 1854 г. шифр был взломан изобретателем первой аналитической вычислительной машины Чарльзом Бэббиджем. Этот факт стал известен только в XX в., когда группа ученых разбирала вычисления и личные заметки Бэббиджа [5]. Несмотря на это шифр Виженера имел репутацию исключительно стойкого к «ручному» взлому еще долгое время. Так, известный писатель и математик Чарльз Доджсон (Льюис Кэрролл) в своей статье «Алфавитный шифр», опубликованной в детском журнале в 1868 г., назвал шифр Виженера невзламываемым. В 1917 г. научно-популярный журнал «Scientific American» также отозвался о шифре Виженера, как о неподдающемся взлому [13].

```
/*
 * Главный цикл, который проходит по входной строке
 */
foreach (char symbol in input)
{
    /* characters - алфавит,
       keyword - ключевое слово,
       N - мощность алфавита,
       keyword_index - индекс текущей буквы ключевого слова
     */
    int c = (Array.IndexOf(characters, symbol) +
             Array.IndexOf(characters, keyword[keyword_index])) % N;

    /* result - результирующая строка */
    result += characters[c];

    keyword_index++;

    /* циклический проход по ключевому слову */
    if ((keyword_index + 1) == keyword.Length)
        keyword_index = 0;
}
```

Листинг 2.1 Фрагмент кода, реализующего алгоритм шифра Виженера

Роторные машины. Идеи Альберти и Виженера использовались при создании электромеханических роторных машин первой половины XX века. Некоторые из них использовались в разных странах вплоть до 1980-х годов. В большинстве из них использовались роторы (механические колеса), взаимное расположение которых определяло текущий алфавит шифрозамен, используемый для выполнения подстановки. Наиболее известной из роторных машин является немецкая машина времен Второй мировой войны «Энигма». Более детальному изучению и практическому анализу «Энигмы» далее будет посвящена отдельная лабораторная работа.

К полиалфавитным относится также шифр на основе «одноразового блокнота».

Много полезной информации по рассмотренному классу шифров можно найти в [14].

Существует определенное сходство между подстановочными шифрами и *шифрами на основе гаммирования*. Последние рассматриваются как самостоятельный класс. Такие шифры схожи с подстановочными (и в определенном плане – с *перестановочными*) тем, что в обоих случаях можно использовать табличное представление выполняемых операций на основе ключей. В шифрах на основе гаммирования и в подстановочных шифрах при зашифровании происходит подмена одних символов на другие.

ПЕРЕСТАНОВОЧНЫЕ ШИФРЫ

Шифры перестановки относятся к классу *симметричных.* Элементами текста могут быть отдельные символы (самый распространённый случай), пары, тройки букв и так далее.

Классическими примерами перестановочных шифров являются *анаграммы*. Анаграмма (от греч. ανα – «снова» и γράμμα – «запись») – литературный приём, состоящий в перестановке букв (или звуков), что в результате дает другое слово или словосочетание, например: проездной–подрезной, листовка–вокалист, апельсин–спаниель.

В классической криптографии шифры перестановки делятся на два подкласса:

- шифры *простой* или *одинарной перестановки* – при зашифровании символы открытого текста M_i перемещаются с исходных позиций в новые (в шифртексте C_i) один раз,
- шифры *сложной* или *множественной перестановки* – при зашифровании символы открытого текста M_i перемещаются с исходных позиций в новые (в шифртексте C_i) несколько раз.

3.1.1. Шифры одинарной перестановки

3.1.1.1. Шифры простой перестановки

Среди шифров рассматриваемого подкласса иногда выделяют *шифры простой перестановки* (или *перестановки без ключа*). Символы открытого текста M_i перемешиваются по каким-либо правилам. Формально каждое из таких правил может рассматриваться в качестве ключа.

Пример 1. Простейшим примером является запись открытого текста в обратной последовательности. Так, если M_i = «шифр перестановки», то C_i = «иквонатсереп рфиш». Если переставляются в соответствующем порядке пары букв, то C_i = «киованстрепе фрши». При более длинных сообщениях можно таким же образом перемещать целые слова или блоки слов.

Подобную перестановку можно трактовать как *транспозицию*.

В общем случае для использования *шифров одинарной перестановки* используется таблица, состоящая из двух строк: в первой строке записываются буквы, во второй – цифры J. Строки состоят из n столбцов. Буквы составляют шифруемое сообщение. Цифры $J = j_1, j_2, \ldots, j_n$, где j_1 – номер позиции в зашифрованном сообщении первого символа открытого текста, где j_2 – номер позиции в зашифрованном сообщении второго символа открытого текста и т.

д. Таким образом, порядок следования цифр определяется используемым правилом (ключом) перестановки символов открытого текста для получения шифрограммы.

Если предположить, что некоторое сообщение M_i состоит из букв от m_1 до m_n, то рассматриваемую таблицу можно представить как показано ниже (таблица 3.1).

Таблица 3.1. Общий вид таблицы для шифра одинарной перестановки

m_1	m_2	…	m_n
j_1	j_2	…	j_n

В первую строку таблицы 3.1 могут записываться также числа в порядке возрастания от 1 до n. Понятно, что эти числа соответствуют позициям букв в открытом тексте.

Процедура расшифрования также основана на использовании таблиц перестановки. Эти таблицы строятся на основе таблиц вида 3.1.

Пример 2. Пусть M_i = «кибервойны», здесь n = 10. Далее принимаем правило (ключ) перестановки: j_1=5, j_2=3, j_3=1, j_4=6, j_5=4, j_6=2, j_7=10, j_8=7, j_9=8, j_{10}=9.

Составим таблицу для зашифрования сообщения в форме табл. 3.1.

Таблица 3.2

к	и	б	е	р	в	о	й	н	ы
5	3	1	6	4	2	10	7	8	9

Представим эту таблицу только числами.

Таблица 3.3.

1	2	3	4	5	6	7	8	9	10
5	3	1	6	4	2	10	7	8	9

В соответствии с принятым ключом зашифрованное сообщение будет иметь вид: C_i = «бвиркейныо».

Легко подсчитать, что при отсутствии повторяющихся букв в шифруемом сообщении длиной n символов всего существует $n!$ Неповторяющихся ключей.

Для расшифрования сообщения, следуя логике рассмотренных процедур зашифрования, нам нужно также составить таблицу, первой строкой которой будет зашифрованный текст (таблица 3.4.). Здесь применяется примерно такой же подход, как и в шифрах подстановки.

Таблица 3.4.

б	в	и	р	к	е	й	н	ы	о
1	2	3	4	5	6	7	8	9	10

Таблицу 3.4 дополним 3-ей строкой, числа в столбцах которой соответствуют первой строке таблицы 3.3, одновременно составляя неизменную пару: 1 соответствует 3, 2 – 6 и т.д. (см. табл. 3.5).

Таблица 3.5

б	в	и	р	к	е	й	н	ы	о
1	2	3	4	5	6	7	8	9	10
3	6	2	5	1	4	8	9	10	9

Теперь расшифрованному сообщению «бвиркейныо» будет соответствовать обратная перестановка: символы первой строки таблицы 3.5 нужно расположить в порядке в соответствии с 3-й строкой: 1 – «к», 2 – «и» и т. д.

Для использования на практике рассмотренный метод зашифрования/расшифрования не очень удобен. При больших значениях *n* приходится работать с таблицами, состоящими из большого числа столбцов. Кроме того, для сообщений разной длины необходимо создавать разные таблицы перестановок.

Следует также отметить сходство рассмотренных алгоритмов зашифрования/расшифрования и алгоритмов перемежения, которые изучались и анализировались в лабораторной работе №7 из [1].

3.1.1.2. Шифры простой блочной перестановки

Указанные шифры строятся по тем же правилам, что и шифры простой перестановки. Блок должен состоять из 2-х или более символов. Если общее число таких символов в сообщении не кратно длине сообщения, то последний блок можно дополнить произвольными знаками.

Пример 3. Пусть M_i = «кибервойны», примем длину блока, равную 2.

Для зашифрования построим таблицу (табл. 3.6).

Таблица 3.6

ки	бе	рв	ой	ны
5	1	4	2	3

В соответствии с табл. 3.6 получим C_i = «беойнырвки». Расшифрование производится по правилам, схожим с правилами для шифров простой перестановки.

3.1.1.3. Шифры маршрутной перестановки

Основой современных шифров рассматриваемого типа является геометрическая фигура. Обычно прямоугольник или прямоугольная матрица. В ячейки этой фигуры по определенному маршруту (слева-направо, сверху-вниз или каким-либо иным образом) записывается открытый текст. Для

получения шифрограммы нужно записать символы этого сообщения в иной последовательности, т.е. по иному маршруту (см. аналогию с методами перемежения/деперемежения данных в лабораторной работе №7 [1]).

Шифр Скитала (Сцитала). Известно, что в V веке до н. э. в Спарте существовала хорошо отработанная система секретной военной связи. Для этого использовался специальный жезл «скитала» (греч. σκυτάλη – первое, вероятно, простейшее криптографическое устройство, реализующее метод перестановки (рис. 3.1).

Рисунок 3.1 – Скитала [15]

Для зашифрования и расшифрования необходимо было иметь абсолютно одинаковые жезлы. На такой предмет наматывалась пергаментная лента. Далее на эту ленто построчно наносился текст. Для расшифрования ленту с передаваемым сообщением нужно было намотать так же, как и при нанесении открытого текста. Подобным образом работает шифр, который иллюстрирует пример на рисунке 3.5 в [2].

Следуя вышеприведенным рассуждениям, может отождествить скитала с таблицей размерами: k – количество столбцов, s – количество строк. Поскольку при регулярном обмене данными сообщения часто имеют разную длину, то оба этих параметра за неизменяющийся ключ взять неудобно. Поэтому обычно в качестве известного каждой стороне ключа выбирается один из них (часто это s), а второй вычисляется на основе известного и длины n сообщения M_i:

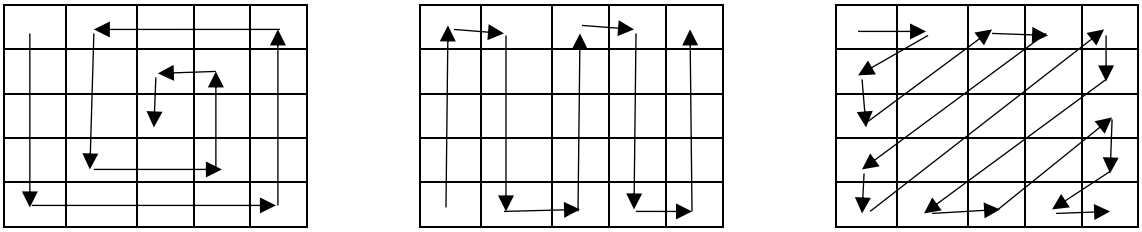
$$k = [(n - 1)/s] + 1. \qquad (3.1)$$

При этом слагаемое в квадратных скобках должно быть целым числом [15].

Нетрудно себе представить аналогию между Скитала и таблицей, которая «намотана» на цилиндр.

При использовании шифра Скитала для формирования шифртекста сначала выбирается 1-ая буква открытого текста, затем (k+1)-буква, (2k+1)-буква и т.д., для некоторого k, равного числу букв в каждой строке скиталы. Значение k является постоянной величиной для данной скиталы,

Организация маршрутной перестановки. Уже упоминавшаяся маршрутная перестановка (записываем сообщение по строкам, считываем – по столбцам матрицы) можно усложнить и считывать не по столбцам, а по спирали (рис. 3.2,а), зигзагом (рис. 3.2,б), змейкой (рис. 3.2,в) или каким-то другим способом (см. рис. 3.2). Такие способы шифрования несколько усложняют процесс, однако усиливают криптостойкость шифра.



а) б) в)

Рисунок 3.2 – Графическое представление методов маршрутной перестановки

Маршруты могут быть значительно более изощренными. Например, обход конем шахматной доски таким образом, чтобы в каждой клетке конь побывал один раз. Один из таких маршрутов был найден Л. Эйлером в 1759 г. Для примера на рис. 3.3 показан такой маршрут для обхода таблицы размером 5 x 4.

Не менее занимательным и не менее сложным является организация маршрутов на основе «магических квадратов» – квадратных матриц со вписанными в каждую клетку неповторяющимися последовательными числами от 1, сумма которых по каждому столбцу, каждой строке и каждой диагонали дает одно и то же число.

Создание новых оригинальных маршрутов приветствуется и поощряется при выполнении данной лабораторной работы.

3.1.1.4. Шифр вертикальной перестановки

Данный шифр является разновидностью шифра маршрутной перестановки. К особенностям вертикального шифра можно отнести следующие:

- количество столбцов в таблице фиксируется и определяется длиной ключа;
- маршрут вписывания: слева-направо, сверху-вниз;
- шифрограмма выписывается по столбцам в соответствии с их нумерацией (ключом).

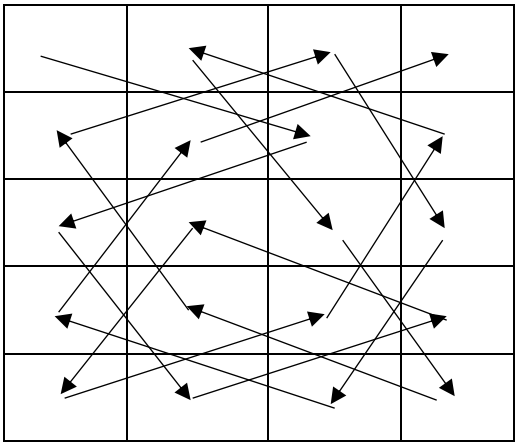


Рисунок 3.3 – Пример маршрута «обход конем»

Ключ может задавиться в виде текста (слова или словосочетания). Лексикографическое местоположение символов в ключевом выражении определяет порядок считывания столбцов.

Пример 4. Например, ключом является слово «крипто». Во-первых, это означает, что количество столбцов k в таблице должно быть равно длине ключа, т. е. – 6. Если вспомним порядок букв из ключевого слова в алфавите, то последовательность считывания столбцов будет следующим: 2, 5, 1, 4, 6, 3.

Необходимо зашифровать сообщение M_i = «шифр вертикальной перестановки»; n = 30.

Строим основную таблицу 5х6 (табл. 3.7), в которую по стокам будет записано исходное сообщение.

Считывая информацию из таблицы по столбцам в соответствии с ключом, получим шифрограмму C_i = «фтнрошелпава тириоевирьен кйск».

Таблица 3.7

к	*р*	*и*	*п*	*т*	*о*
2	5	1	4	6	3
ш	и	ф	р		в
е	р	т	и	к	а
л	ь	н	о	й	
п	е	р	е	с	т
а	н	о	в	к	и

3.1.2. Шифры множественной перестановки

Особенностью шифров данного подкласса является минимум двукратная перестановка символов шифруемого сообщения. В простейшем случае это может задаваться перемешиваем не только столбцов (как в примере 4), но и строк. Таким образом, этот случай соответствует использованию двух основных ключей: длина одного из них равна числу столбцов, другого – числу строк. К ключевой информацию мы можем относить также способы

вписывания сообщения и считывания отдельных символов из текущего столбца матрицы.

Пример 5. Предположим, что (в продолжение к последнему примеру) вторым ключом будет «слово» или 5, 2, 3, 1, 4 (одинаковым буквам «о» мы присвоили последовательные числа).

Предыдущая таблица несколько видоизменится и примет следующий вид (табл. 3.8).

Таблица 3.8

ключи		*к*	*р*	*и*	*п*	*т*	*о*
		2	5	1	4	6	3
с	5	ш	и	ф	р		в
л	2	е	р	т	и	к	а
о	3	л	ь	н	о	й	
в	1	п	е	р	е	с	т
о	4	а	н	о	в	к	и

Для удобства отсортируем последовательно строки в соответствии с ключом (табл. 3.9).

Таблица 3.9

ключи		*к*	*р*	*и*	*п*	*т*	*о*
		2	5	1	4	6	3
в	1	п	е	р	е	с	т
л	2	е	р	т	и	к	а
о	3	л	ь	н	о	й	
о	4	а	н	о	в	к	и
с	5	ш	и	ф	р		в

И столбцы – в соответствии с ключевым словом «слово».

Таблица 3.10

ключи		*и*	*к*	*о*	*п*	*р*	*т*
		1	2	3	4	5	6
в	1	е	т	р	е	с	п
л	2	и	а	т	р	к	е
о	3	о		н	ь	й	л
о	4	в	и	о	н	к	а
с	5	р	в	ф	и		ш

Получим итоговую шифрограмму C_i = «еиоврта ивртноферьнискйк пелаш».

Шифры гаммирования рассматриваются как самостоятельный класс. Такие шифры схожи с перестановочными тем, что в обоих случаях можно использовать табличное представление выполняемых операций на основе ключей. Вместе с тем, шифры гаммирования имеют много общего с подстановочными шифрами, поскольку на самом деле при зашифровании происходит подмена одних символов на другие.