Тема: Шифры простой замены

Введение

Шифры простой замены – это методы шифрования, которые сводятся к созданию по определённому алгоритму таблицы шифрования, в которой для каждой буквы открытого текста существует единственная сопоставленная ей буква шифротекста. Само шифрование заключается в замене букв согласно таблице. Для расшифровки достаточно иметь ту же таблицу, либо знать алгоритм, по которой она генерируется. Шифров этого типа очень много мы с вами рассмотрим самые известные из них.

Полибианский квадрат

Одним из первых шифров простой замены считается так называемый полибианский квадрат. За два века до нашей эры греческий писатель и историк Полибий изобрел для целей шифрования квадратную таблицу размером 5x5 заполненную буквами греческого алфавита в случайном порядке.

λ	ε	υ	ω	γ
ρ	ζ	δ	σ	ο
μ	η	β	ξ	τ
ψ	π	θ	α	ϕ
χ	ν		φ	ι

Процедура шифрования: прямоугольная таблица заполняется буквами алфавита в случайном порядке. Каждая буква открытого сообщения заменяется буквой, расположенной ниже в том же столбце. Если буква находится на последней строке таблицы, то она заменяется верхней буквой столбца.

Пример:

1) Заполним таблицу буквами алфавита в случайном порядке.
2) Зашифруем слово: ***алфавит***.
3) Получили закрытый текст: ***уы утсз***.

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

Шифрующие таблицы Трисемуса

В 1508 г. аббат из Германии Иоганн Трисемус написал печатную Работу по криптологии «Полиграфия». В ней он симметрически Описал применение шифрующих таблиц, заполненных алфавитом. В Таблицу (в русском языке обычно 4×8) вписывается по строкам Ключевое слово, причем повторяющиеся буквы отбрасываются. Затем эта таблица дополняется не вошедшими в нее буквами Алфавита по порядку. Так как ключевое слово легко хранить в памяти, то такой подход упрощает процесс шифровки и расшифровки. Как и в случае полибианского квадрата, при шифровании переходят в этой таблице на очередную букву открытого текста и заталкивают в шифротекст букву, расположенную ниже ее в том же столбце, если эта буква оказалась в нижней строке, то в шифротекст пишут верхнюю букву этого же столбца.

Шифр Атбаш

Некоторые фрагменты библейских текстов зашифрованы с помощью шифра, который назывался Атбаш. Правило зашифрования состояло в замене i-й буквы алфавита буквой с номером n – i + 1, где n - число букв в алфавите. Происхождение слова Атбаш объясняется принципом замены букв. Это слово составлено из букв Алеф, Тав, Бет, Шин, то есть первой и последней, второй и предпоследней букв древнесемитского алфавита.

Лозунговый шифр

В данном шифре запоминание ключа основано на лозунге – легко запоминающемся слове или фразе. Например, если выбрать слово – лозунг «заявление» и заполнить вторую строку таблицы по следующему правилу: сначала вписывается слово-лозунг, причем повторяющиеся буквы отбрасываются, затем эта таблица дополняется не вошедшими в нее буквами алфавита. Ключ будет иметь вид:

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

Шифр Цезаря

Шифр Цезаря - это вид шифра подстановки, в Котором каждый символ в открытом тексте заменяется буквой находящейся на некоторое Постоянное число позиций правее него в алфавите. Например, в шифре со сдвигом 3, А Была бы заменена на Г, Б станет Д, и так далее. Шифр назван в честь римского императора Гая Юлия Цезаря, использовавшего его для секретной переписки со своими генералами.

Пример:

1) Зашифруем слово: ***генерал***;
2) Получили закрытый текст: ***жириуго***;

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

Шифр цезаря с ключевым словом: в данной разновидности шифра Цезаря ключ задается числом k (0<=k<=n-1) и коротким ключевым словом или предложением. Выписывается алфавит, а под ним, начиная с k-й позиции, ключевое слово. Оставшиеся буквы записываются в алфавитном порядке после ключевого слова.

В Афинной системе подстановок Цезаря: буквы исходного сообщения преобразуются следующим образом: $T1 = (AT + B) \bmod m$, где:

- T – порядковый номер буквы исходной последовательности;
- T1 – порядковый номер соответствующей буквы зашифрованной последовательности;
- m – размер алфавита;
- A, B – целые числа (причем A и m взаимно простые).

Шифр «гласных»

В шифре гласных каждая буква обыкновенного алфавита заменяется двумя гласными. Ключом служит квадрат из 36 клеток; над линией языка и Слева от секретной линии пишутся простые гласные (гласные которые пишутся слева и сверху можно менять на любые символы), а в клетках Размещаются буквы алфавита в любом порядке. По этой системе каждая буква заменяется двумя соответствующими гласными (или символами) из горизонтального и вертикального рядов.

Пример:

1) Зашифруем слово: ***привет***;
2) Заполним квадрат буквами. Случайным образом или используя какой-либо лозунг.
3) Шифротекст: ***юеяееююяаяао***;

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

Биграммный шифр Плейфера

Шифр Плейфера изобретен в 1854 г. И является наиболее известным биграммным шифром замены. Он применялся в Великобритании во время первой мировой войны. В таблицу случайным образом заносят буквы алфавита. Для удобства запоминания шифрующей таблицы можно пользоваться ключевым словом или фразой при заполнении таблицы, аналогично как в таблицах Трисемуса.

Процедура шифрования включает:

1) **Открытый текст разбивается на пары букв (биграммы). Текст должен иметь четное число букв, и в нем не должно быть биграмм, содержащих две одинаковые буквы;**

2) **Последовательность биграмм открытого текста преобразуется с помощью шифрующей таблицы по следующим правилам:**

2.1. если обе буквы биграммы открытого сообщения не попадают в одну строку или столбец, тогда для замены находят буквы в углах прямоугольника, определяемого данной парой букв;

2.2. если обе буквы биграммы открытого сообщения принадлежат одному столбцу таблицы, то их заменяют буквами, которые лежат под ними. Если при этом буква открытого текста находится на нижней строке, то для шифрования берется буква из верхней строки того же столбца;

3.3. если обе буквы биграммы открытого сообщения принадлежат одной строке таблицы, то они заменяются буквами, которые лежат справа от них. Если при этом буква открытого текста находится в крайнем правом столбце, то для шифрования берется буква из крайнего левого столбца той же строки.

Пример:

1) Впишем ключевое слово по строкам в таблицу, повторяющиеся буквы отбрасываем: ***приветкакдела***;
2) Дополним таблицу не вошедшими в нее буквами алфавита по порядку;
3) Зашифруем словосочетание: ***шифрующаятаблица***;
4) Получили закрытый текст: ***ъпоецыярэаимбрчк***;

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

Шифр «двойной квадрат Уитстона»

В 1854 году англичанин Чарльз Уитстон разработал новый метод шифрования биграммами, который называют "двойным квадратом Уитстона". Свое название этот шифр получил по аналогии с полибианским квадратом. Шифр Уитстона открыл новый этап в истории развития криптографии. В отличие от полибианского шифр "двойной квадрат Уитстона " использует сразу две таблицы, размещенные по одной горизонтали, а шифрование идет биграммами, как в шифре Плейфейра. Эти не столь сложные модификации привели к появлению на свет качественно новой криптографической системы ручного шифрования. Шифр "двойной квадрат Уитстона" оказался очень надежным и удобным и применялся Германией даже в годы второй мировой войны.

Процедура шифрования включает:

Процедура шифрования выполняется следующим образом. Перед шифрованием исходное сообщение разбивается на биграммы. Каждая биграмма шифруется отдельно. Первую букву биграммы находят в правой таблице, а вторую – в левой таблице. Затем мысленно строится прямоугольник так, чтобы буквы биграммы лежали в его противоположных вершинах. Другие две вершины этого прямоугольника дают буквы биграммы шифротекста. Если обе буквы биграммы лежат в одной строке, то и буквы шифротекста берут из той же строки. Первую букву биграммы шифротекста берут из правой таблицы в столбце, соответствующем первой букве биграммы сообщения. Вторая же буква биграммы шифротектса берется из левой таблицы в столбце, соответствующем второй букве биграммы сообщения.

Пример:

1) Зашифруем слово: ***привет***;
2) Заполним «два квадрата» Уитстона буквами. Это можно делать как случайно, так и используя лозунги. Мы будем использовать лозунги.
3) Первый лозунг: ***приветкакдела***;
4) Второй лозунг: ***хорошоаутебя***;
5) Шифротекст: ***хихжол***;

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

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

Криптосистема Хилла

Шифр Хилла — полиграммный шифр подстановки, основанный на линейной алгебре. Лестер С. Хилл изобрел этот шифр в 1929, и это был первый шифр, который позволял на практике оперировать более чем с тремя символами за раз. Шифрование: каждой букве сперва сопоставляется число: А = 0, Б =1, ..., Я=31, но это не является существенным свойством шифра. Блок из n букв рассматривается как n-мерный вектор и умножается на n × n матрицу по модулю 31. Матрица целиком является ключом шифра. Матрица должна быть обратима, чтобы была возможна операция расшифрования.

Система шифрования омофонов

Данная система характеризуется тем, что буквы исходного сообщения имеют несколько замен. Число замен символа пропорционально вероятности его появления в открытом тексте. Данные о распределениях вероятностей букв в русском тексте приведены в следующей таблице:

Буква	Вероятность	Буква	Вероятность	Буква	Вероятность	Буква	Вероятность
Пробел	0,175	Р	0,040	Я	0,018	Х	0,009
О	0,090	В	0,038	Ы	0,016	Ж	0,007
Е	0,072	Л	0,035	З	0,016	Ю	0,006
А	0,062	К	0,028	Ъ	0,014	Ш	0,006
И	0,062	М	0,026	Б	0,014	Ц	0,004
Н	0,053	Д	0,025	Г	0,013	Щ	0,003
Т	0,053	П	0,023	Ч	0,012	Э	0,003
С	0,045	У	0,021	Й	0,010	Ф	0,002

Шифруя букву исходного сообщения, выбирают случайным образом одну из ее замен. Замены часто называемые омофонами могут быть представлены трехразрядными числами от 000 до 999. Например, букве О присваивается 90 случайных номеров, буквам Б и Ъ – по 14 номеров. Если омофоны присваиваются случайным образом различным появлениям одной и той же буквы, тогда каждый омофон появляется в шифротексте равновероятно. Система омофонов Обеспечивает простейшую защиту от криптоаналитических атак, основанных на подсчете частот появления букв в шифротекст.