Работа №4

Шифрующие таблицы 2

1. Шифрующие таблицы Трисемуса

В 1508 г. аббат из Германии Иоганн Трисемус написал печатную работу по криптологии под названием "Полиграфия". В этой книге он впервые систематически описал применение шифрующих таблиц, заполненных алфавитом в случайном порядке. Для получения такого шифра замены используется таблица для записи букв алфавита и ключевое слово (или фраза):

- в таблицу сначала вписывается по строкам ключевое слово, причем повторяющиеся буквы отбрасывались;
- таблица дополняется не вошедшими в нее буквами алфавита по порядку.

Поскольку ключевое слово или фразу легко хранить в памяти, то такой подход упрощал процессы шифрования и расшифрования.

********** *Пример* 1**********

Для русского алфавита шифрующая таблица может иметь размер 4x8. Выберем в качестве ключа слово БАНДЕРОЛЬ. Шифрующая таблица с таким ключом показана в таблице 1:

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	Ы	**Ъ**	Э	Ю	Я

*Здесь цветом выделены буквы для пояснения следующего шифра (шифра Плейфера) во 2-м разделе.

Сообщение

ВЫЛЕТАЕМ ПЯТОГО

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, тогда для шифртекста берут самую верхнюю букву из того же столбца,

получаем шифртекст

ПДКЗЫВЗЧ ШЛЫЙСЙ

Такие табличные шифры называются монограммными, так как шифрование выполняется по одной букве. Трисемус первым заметил, что шифрующие таблицы позволяют шифровать сразу по две буквы. Такие шифры называются *биграммными.*

2. Биграммный шифр Плейфейра

Шифр Плейфейра, изобретенный в 1854 г., является наиболее известным биграммным шифром замены. Он применялся Великобританией во время первой мировой войны. Основой шифра Плейфейра является шифрующая таблица со случайно расположенными буквами алфавита исходных сообщений.

Для удобства запоминания шифрующей таблицы отправителем и получателем сообщений можно использовать ключевое слово (или фразу) при заполнении начальных строк таблицы. В целом структура шифрующей таблицы системы Плейфейра полностью аналогична структуре шифрующей таблицы Трисемуса. Поэтому для пояснения процедур шифрования и

расшифрования в системе Плейфейра будем использовать шифрующую таблицу Трисемуса (таблицу 1) из первого раздела.

Процедура шифрования состоит из следующих шагов:

1. Открытый текст исходного сообщения разбивается на пары букв (биграммы). Текст должен иметь четное количество букв и в нем не должно быть биграмм, содержащих две одинаковые буквы. Если эти требования не выполнены, то текст модифицируется даже из-за незначительных орфографических ошибок.

2. Последовательность биграмм открытого текста преобразуется с помощью шифрующей таблицы в последовательность биграмм шифртекста по следующим правилам:

2а. Если обе буквы биграммы открытого текста не попадают на одну строку или столбец (как, например, буквы А и Й в табл. 1), тогда находят буквы в углах прямоугольника, определяемого данной парой букв. (В нашем примере это буквы АЙОВ. Пара букв АЙ отображается в пару 0В).

Последовательность букв в биграмме шифртекста должна быть зеркально расположенной по отношению к последовательности букв в биграмме открытого текста.

2б. Если обе буквы биграммы открытого текста принадлежат одному столбцу таблицы, то буквами шифртекста считаются буквы, которые лежат под ними. (Например, биграмма НС дает биграмму шифртекста ГЩ). Если при этом буква открытого текста находится в нижней строке, то для шифртекста берется соответствующая буква из верхней строки того же столбца. (Например, биграмма ЗЪ дает биграмму шифртекста УЕ).

2в. Если обе буквы биграммы открытого текста принадлежат одной строке таблицы, то буквами шифртекста считаются буквы, которые лежат справа от них. (Например, биграмма НО дает биграмму шифртекста ДЛ). Если при этом буква открытого текста находится в крайнем правом столбце, то для шифра берут соответствующую букву из левого столбца в той же строке. (Например, биграмма ФЦ дает биграмму шифртекста ХМ).

********** *Пример* 2**********

ВСЕ ТАЙНОЕ СТАНЕТ ЯВНЫМ

Разбиение этого текста на биграммы дает

ВС ЕТ АЙ НО ЕС ТА НЕ ТЯ ВН ЫМ

Данная последовательность биграмм открытого текста преобразуется с помощью шифрующей таблицы 1 в следующую последовательность биграмм шифртекста:

ГП ДУ 0В ДЛ НУ ПД ДР ЦЫ ГА ЧТ

При расшифровании применяется обратный порядок действий.

Следует отметить, что шифрование биграммами резко повышает стойкость шифров к вскрытию. Хотя книга И. Трисемуса "Полиграфия" была относительно доступной, описанные в ней идеи получили признание лишь спустя три столетия. По всей вероятности, это было обусловлено плохой осведомленностью криптографов о работах богослова и библиофила Трисемуса в области криптографии.

Задания

1. *Работа в паре.* Зашифровать сообщение длиной 6-11 слов, используя шифрующие таблицы Трисемуса. Расшифровать сообщение напарника

2 *Работа в паре.* Зашифровать сообщение длиной 6-11 слов, используя биграммный шифр Плейфейра. Расшифровать сообщение напарника.