Практическое занятие №2.
Маршрутные и подстановочные шифры

Примеры шифрования и дешифрования, вскрытие ключа.

Шифры маршрутной перестановки используют некоторую геометрическую фигуру (плоскую или объемную). Преобразования состоят в том, что в фигуру исходный текст вписывается по ходу одного маршрута, а выписывается по-другому.

Шифр табличной маршрутной перестановки основаны на таблицах. При шифровании в такую таблицу вписывают исходное сообщение по определенному маршруту, а выписывают (получают шифрограмму) – по-другому. Для данного шифра маршруты вписывания и выписывания, а также размеры таблицы являются ключом.

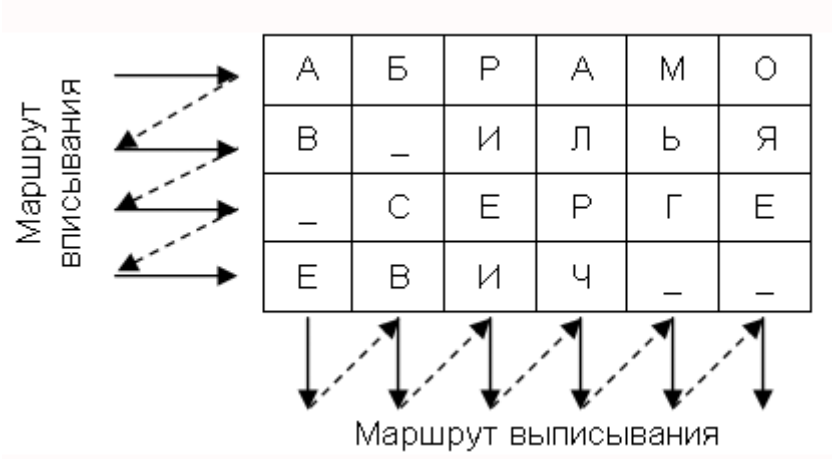

Рис.1 Пример использования шифра маршрутной перестановки

Задание.

Необходимо зашифровать свою фамилию шифром маршрутной перестановки

При дешифровании текста используют частотные характеристики открытого текста. Однако для получения устойчивой картины длина послания должна быть существенно больше ключа. Одной из наиболее устойчивых характеристик осмысленного текста является отсутствие запретных биграмм (пара соседних букв). Например, биграммы «Ъ + Ь», «гласная + Ь», «пробел + Ь». Знание и использование частотной диаграммы открытого текста значительно упростит дешифрование шифра перестановки

Шифр Плейфера

Шифр Плейфера — подстановочный шифр, реализующий замену биграмм. Для шифрования необходим ключ, представляющий собой таблицу букв размером 5*5 (без буквы J).

Процесс шифрования сводится к поиску биграммы в таблице и замене ее на пару букв, образующих с исходной биграммой прямоугольник.

Рассмотрим, в качестве примера следующую таблицу, образующую ключ шифра Плейфера:

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

Задание.

1. **Задание.**
   Открытый текст:

Please note that spaces and punctuation characters have been removed before encryption

Шифротекст:

LMBEUDOPUASIIYUNEDDUDOENSPARTEYOPODGCTEDUASTIDZBCBDPUCNPZBACBKMTDZDPGWZOYOPO

Найти ключ.

2. **Задание.**
   - Придумать ключ.
   - Написать код шифровки своих фамилии, имени, отчества
   - Написать код дешифровки своих фамилии, имени, отчества

Практические занятия:

Основная цель проведения лабораторных занятия состоит в закреплении теоретического материала курса, приобретении навыков выполнения задач по основам криптографических технологий, анализа результатов, грамотного оформления отчетов.

1. Криптоанализ классических шифров.
2. Маршрутные и подстановочные шифры.
3. Шифрование, дешифрование информации с применением криптографических алгоритмов гаммирования.
4. Исследование ассиметричных алгоритмов шифрования.
5. Исследование методов идентификация и аутентификация пользователя. Протоколы «рукопожатия» и идентификации типа «запрос-ответ».
6. Цифровые подписи DSA и ГОСТ.
7. Сертификаты инфрастуктуры открытых ключей и их структура. Функции удостоверяющего центра.
8. Примеры прикладных протоколов (протоколы заключения сделок, платежных систем, сертифицированная электронная почта, голосования и др.).