МИНИСТЕРСТВО ОБРАЗОВАНИЯ РЕСПУБЛИКИ БЕЛАРУСЬ

Учреждение образование «Белорусский государственный технологический университет»

Кафедра информационных систем и технологий

**«Исследование криптографических шифров на основе перестановки символов»**

Студент:

Агапкина Диана Сергеевна

Вариант 7

Преподаватель:

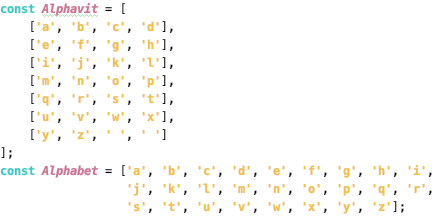
Блинова Евгения Александровна

Минск 2020

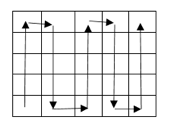
**ЗАДАНИЕ 1.** Маршрутная перестановка (маршрут: зигзагом; параметры таблицы – по указанию преподавателя)

Преобразования состоят в том, что в фигуру исходный текст вписывается по ходу одного маршрута, а выписывается по другому.

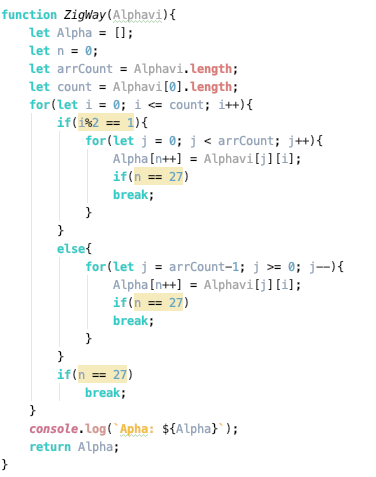
Для начала сформировала алфавит для шифрования двумя методами.

Массив Alphavit используется для шифрования маршрутной перестановка (маршрут: зигзагом). Массив Alphabet используется для шифрования множественной перестановки с ключевыми словами

Маршрутная перестановка (маршрут: зигзагом) уже упоминавшаяся маршрутная перестановка (записываем сообщение по строкам, считываем – по столбцам матрицы) можно усложнить и считывать не по столбцам, а зигзагом. Ниже показан маршрут.



Функция, реализующая данный метод шифра перестановки, продемонстрирована ниже.





Здесь мы формируем алфавит из указанного ранее массива и строим маршрут.

**ЗАДАНИЕ 2.** Множественная перестановка, ключевые слова – собственные имя и фамилия

Особенностью шифров данного подкласса является минимум двукратная перестановка символов шифруемого сообщения. В данном подклассе шифров используется идея повторного шифрования уже зашифрованного сообщения или многократной перестановки символов исходного сообщения перед попаданием в итоговую шифрограмму. 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.

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.



