**ШИФР ВИЖИНЕРА**

Шифры сложной замены называют многоалфавитными, так как для шифрования каждого символа исходного сообщения применяют свой шифр простой замены. К таким шифрам относятся система Вижинера и «двойной квадрат» Уитстона.

Рассмотрим систему Виженера на практике. Система Вижинера подобна такой системе шифрования Цезаря, у которой ключ подстановки меняется от буквы к букве. Этот шифр многоалфавитной замены описывается таблицей шифрования, называемой таблицей Вижинера.

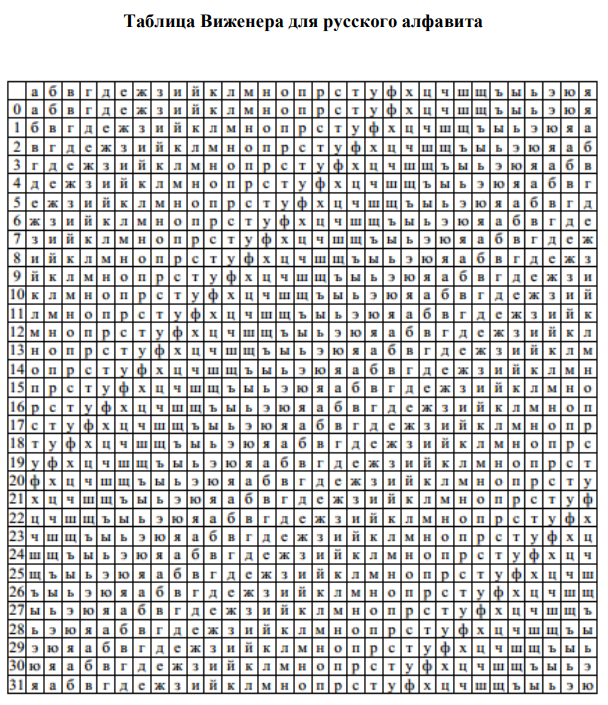


Таблица Вижинера имеет два входа:

- верхнюю строку подчеркнутых символов, используемую для считывания очередной буквы исходного открытого текста;

- крайний левый столбец ключа.

Последовательность ключей получают из порядковых номеров в алфавите букв ключевого слова (начиная с 0). При шифровании исходного сообщения его выписывают в строку, а под ним записывают ключевое слово или фразу. Если ключ оказался короче сообщения, то его циклически повторяют. В процессе шифрования находят в верхней строке таблицы очередную букву исходного текста и в левом столбце очередное значение ключа. Очередная буква шифртекста находится на пересечении столбца, определяемого шифруемой буквой, и строки, определяемой числовым значением ключа.

Задание:

1. Написать программу используя языки программирования (С++, C#, Phyton … любой по выбору) реализующая кодирование по методу Вижинера;
2. Реализовать возможность самостоятельного выбора ключа;
3. Оптимизировать код и проверить на всевозможные ошибки;
4. Использовать в алфавите знаки препинания, заглавные буквы, а также цифры;
5. Реализовать шифрование текста из файла и перезапись кодируемого сообщения в другой файл;
6. Реализовать декодирования шифрованного файла;
7. Реализовать проверку декодируемого файла с исходным (например, можно сравнивать количество затраченных байт в исходном и в раскодируемом файле, или сравнение каждого символа), вывести процент ошибки.