**Лабораторная работа 4**

**Система шифрования Вижинера**

Эта система впервые была опубликована в 1586г. и является одной из старейших и наиболее известных многоалфавитных систем. Система названа по имени французского дипломата XVI века Блеза Вижинера, который развивал и совершенствовал криптографические системы.

Система Вижинера подобна такой системе шифрования Цезаря, у которой ключ подстановки меняется от буквы к букве. Этот шифр многоалфавитной замены можно описать таблицей шифрования, называемой таблицей (квадратом) Вижинера. Для букв русского алфавита таблица Вижинера выглядит следующим образом (Таблица).

Таблица используется для шифрования и дешифрования, имея два входа:

* верхнюю строку подчёркнутых символов используют для считывания очередной буквы исходного открытого текста;
* крайний левый столбец ключа.





Последовательность ключей обычно получают из числовых значений букв ключевого слова. При шифровании исходного сообщения его выписывают в строку, а под ним записывают ключевое слово (или фразу). Если ключ короче сообщения, то его циклически повторяют, подобно ключу шифра Гронсфельда. В процессе шифрования находят в верхней строке таблицы очередную букву исходного текста и в левом столбце очередное значение ключа. Буква шифртекста находится на пересечении столбца, определяемого шифруемой буквой, и строки, определяемой числовым значением ключа.

Рассмотрим пример. Необходимо зашифровать сообщение: ПРИЛЕТАЮ СЕДЬМОГО. Выберем ключевым слово АМБРОЗИЯ.

Согласно алгоритму, в 1-ю строку запишем сообщение, во 2-ю – ключевое слово, а в 3-ю будем выписывать буквы шифра применив, таблицу Вижинера.



**Задание – зашифровать и расшифровать сообщение с собственным ключом на языке программирования Python**