**Лабораторная работа 5**

**Биграммный шифр Плейфера**

Основой шифра Плейфейра является шифрующая таблица со случайно расположенными буквами алфавита исходного текста.

Для удобства запоминания шифрующей таблицы отправителем и получателем сообщений можно использовать ключевое слово (или фразу) при заполнении начальных строк таблицы.



Процедура шифрования включает следующие шаги:

№ 1. Открытый текст исходного сообщения разбивается на пары букв (биграммы). Текст должен иметь чётное количество букв, и в нём 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:

1. Если обе буквы биграммы открытого текста не попадают на одну строку или столбец (например, буквы А и Й), тогда находят буквы в углах прямоугольника, определяемого данной парой букв. (в нашем примере это буквы АЙОВ). Пара букв АЙ отображается в пару ОВ. Последовательность букв в биграмме шифртекста должна быть зеркально расположенной по отношению к последовательности букв в биграмме открытого текста.
2. Если буквы биграммы открытого текста принадлежат одному столбцу таблицы, то буквами шифртекста считаются буквы, которые расположены под ними. (Например, биграмма НС даёт биграмму шифртекста ГЩ). Если при этом буква открытого текста находится в нижней строке, то для шифртекста берётся соответствующая буква из верхней строки того же столбца. (Например, биграмма ВШ даёт биграмму шифртекста ПА).
3. Если обе буквы открытого текста принадлежат одной строке таблицы, то буквами шифртекста считаются буквы, которые лежат справа от них. (Например, биграмма НО даёт биграмму шифртекста ДЛ). Если при этом буква открытого текста находится в правом крайнем столбце, то для шифра берут соответствующую букву из левого столбца в той же строке. (Например, биграмма ФЦ даёт биграмму шифртекста ХМ).

**Задание – Создать таблицу шифрования Плейфера, зашифровать и расшифровать сообщение по ней на языке программирования Python**