Фестиваль исследовательских и творческих работ учащихся «Портфолио»

Биграммный шифр

- Шифр Плейфейра, изобретенный в 1854г., является наиболее известным биграммным шифром замены.

- Основой шифра Плейфейра является шифрующая таблица со случайно расположенными буквами алфавита исходных сообщений.

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

Б	А	Н	Д	Е	Р	О	Л
Ь	В	Г	Ж	З	И	Й	К
М	П	С	Т	У	Ф	Х	Ц
Ч	Ш	Щ	Ы	Ъ	Э	Ю	Я

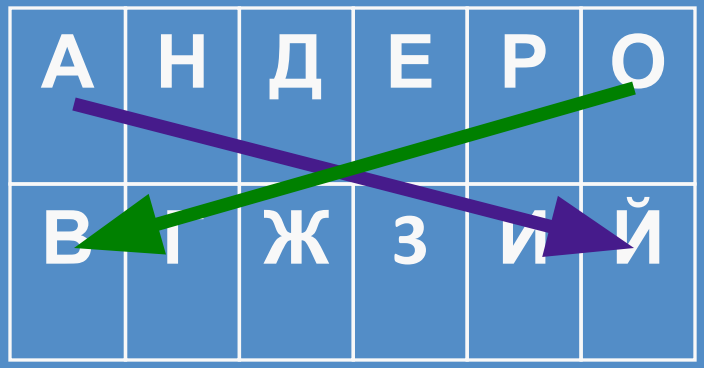
- Открытый текст исходного сообщения разбивается на пары букв (биграммы).

- Текст должен иметь четное количество букв и в нем не должно быть биграмм, содержащих две одинаковые буквы.

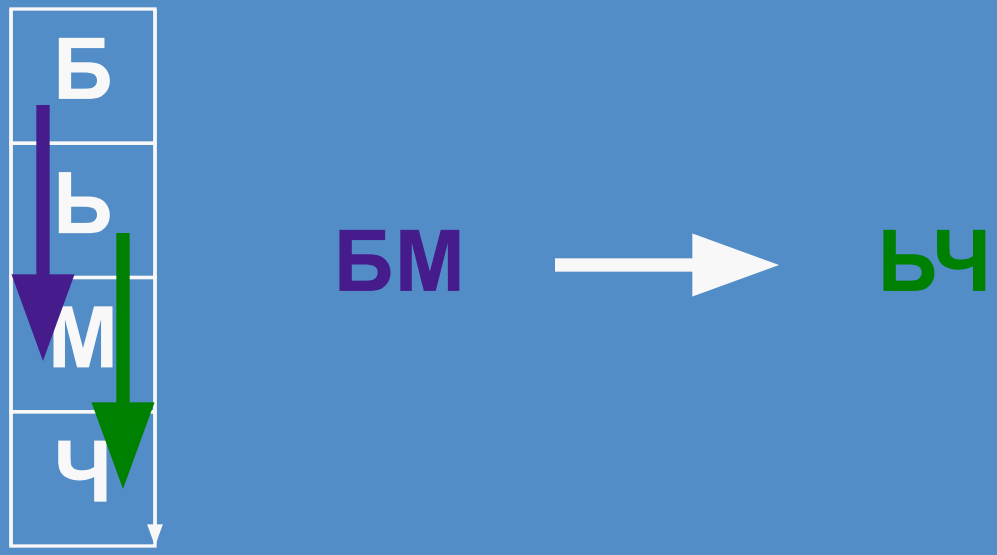
- Если эти требования не выполнены, то текст модифицируется даже из-за незначительных орфографических ошибок.

РЕСПУБЛИКА → РЕ СП УБ ЛИ КА

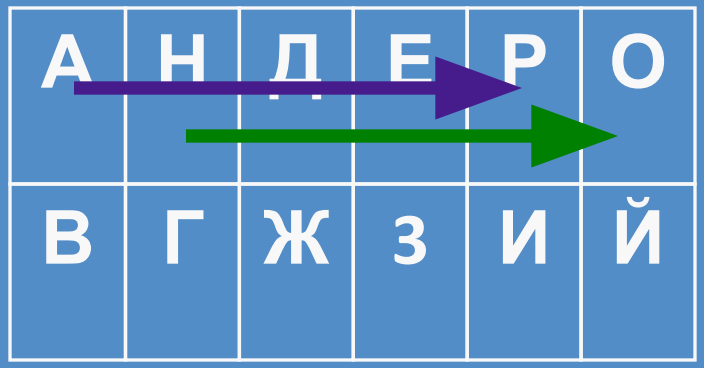
- Если обе буквы биграммы открытого текста не попадают на одну строку или столбец, тогда находят буквы в углах прямоугольника, определяемого данной парой букв.



- Если обе буквы биграммы открытого текста принадлежат одному столбцу таблицы, то буквами шифртекста считаются буквы, которые лежат под ними.
- Если при этом буква открытого текста находится в нижней строке, то для шифртекста берется соответствующая буква из верхней строки того же столбца.



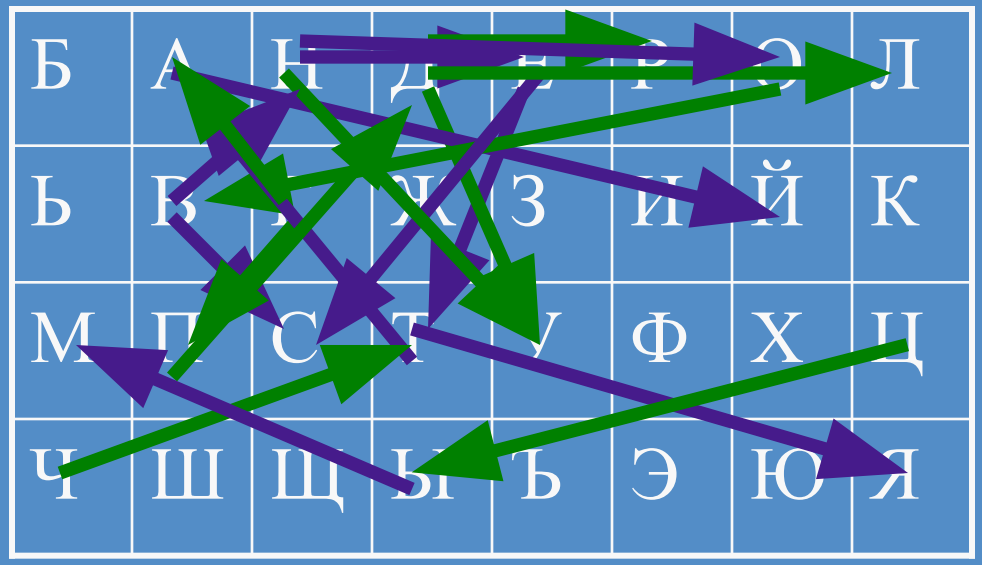
- Если обе буквы биграммы открытого текста принадлежат одной строке таблицы, то буквами шифртекста считаются буквы, которые лежат справа от них.
- Если при этом буква открытого текста находится в крайнем правом столбце, то для шифра берут соответствующую букву из левого столбца в той же строке.



АР → НО

- Например, нужно зашифровать фразу: ВСЕ ТАЙНОЕ СТАНЕТ ЯВНЫМ, используя шифртаблицу с ключевым словом: БАНДЕРОЛЬ

ВС ЕТ АЙ НО ЕС ТА НЕ ТЯ ВН ЫМ



ГП ДУ ОВ ДЛ НУ ПД ДР ЦЫ ГА ЧТ

назад