


*Фестиваль исследовательских и творческих работ учащихся
«Портфолио»*

Шифр «Двойной квадрат»





Шифр «двойной квадрат»
придуман
Чарльзом Уитсоном
в 1854 году



Шифр «двойной квадрат» - шифр замены

Алгоритм шифрования

- При шифровании открытый текст разбивается на биграммы: **ПРИЕЗЖАЮ В ДВА**

П Р И Е З Ж А Ю _ В _ Д В А

- Буквы биграммы разносятся в разные квадраты случайным образом.
- Пустые клетки заполняются символами.

О			Л		Т
	Ь	К	Г		Э
Ч	У	С		Б	

	Ф	Ы		И	
Ц	Й		Н	Щ	
	Х	Ш	Ъ		К

Алгоритм шифрования

Если буквы входной биграммы
оказываются в одинаковых строках таблиц

Да

То буквы выходной
биграммы выбираются
в той же строке, но с
противоположными номерами

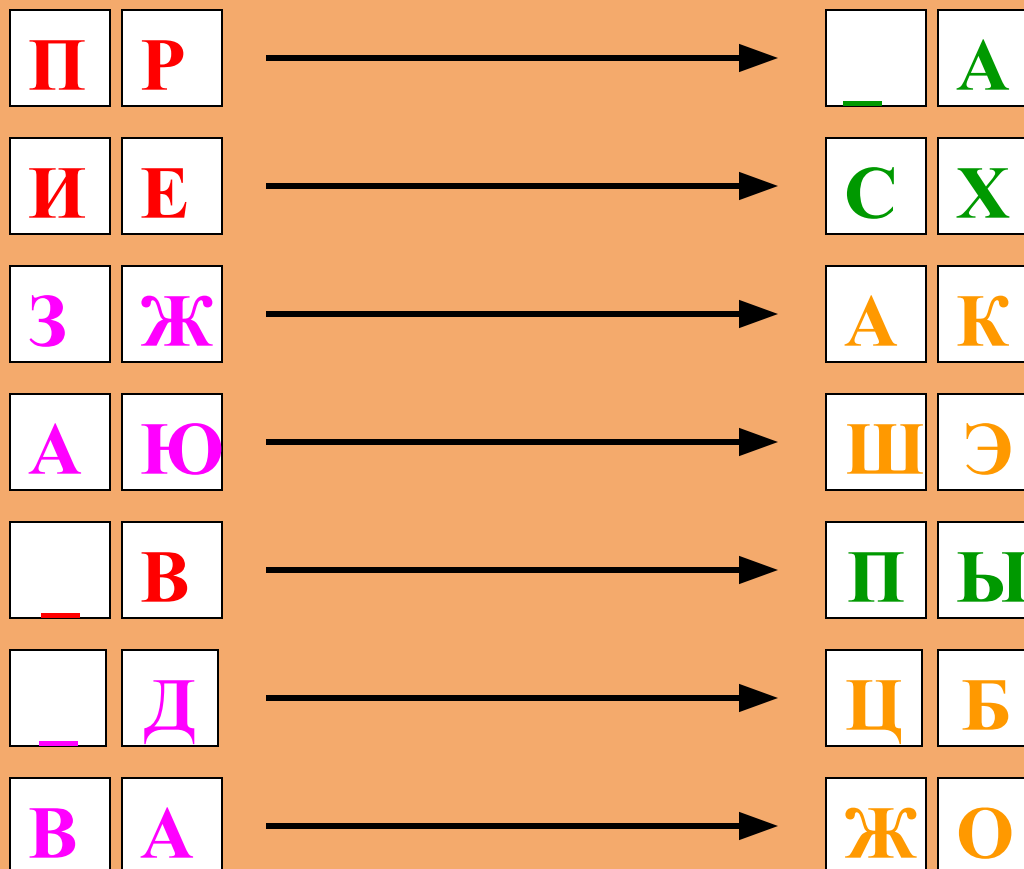
Нет

То рисуется воображаемый
прямоугольник, а выходная
биграмма берется как его
альтернативные вершины

О	П	З	Л	Т	
В	Ь	К	Г	Э	
Ч	У	С	И	Б	А

Р	Ф	Ы	В	И	А
Ц	Й	Ю	Н	Щ	Ж
Д	Х	Ш	С	Е	К

В результате:



Попробуй отгадай слово:

ЕП ВА ВВ



Получилось слово:

УИТСОН

