



## Тема 2.3 Шифр Плейфера. Полибианский квадрат

# Шифр Плейфера

Шифр предусматривает шифрование пар символов (биграмм) вместо одиночных символов, как в шифре подстановки .

*Шифрование английского текста*

A	B	C	D	E
F	G	H	I	K
L	M	N	O	P
Q	R	S	T	U
V	W	X	Y	Z

Буквы «I» и «J» объединяются в одну ячейку.

Получили простую матрицу с английским алфавитом.

Чтобы составить *ключевую матрицу*, сначала записываются в ячейки матрицы буквы ключевого слова (не записывая повторяющиеся символы), а потом заполняются оставшиеся ячейки матрицы символами алфавита, не встречающимися в ключевом слове. Ключевое слово может быть записано, начиная с верхней строки матрицы слева направо, либо по спирали из левого верхнего угла к центру. Ключевое слово, дополненное алфавитом, составляет матрицу 5x5 и является *ключом шифра*.

Рассмотрим пример заполнения матрицы с ключевой фразой *GOOD DAY.*

<b>G</b>	<b>O</b>	<b>D</b>	<b>A</b>	<b>Y</b>
<b>B</b>	<b>C</b>	<b>E</b>	<b>F</b>	<b>H</b>
<b>I</b>	<b>K</b>	<b>L</b>	<b>M</b>	<b>N</b>
<b>P</b>	<b>Q</b>	<b>R</b>	<b>S</b>	<b>T</b>
<b>U</b>	<b>V</b>	<b>W</b>	<b>X</b>	<b>Z</b>

Для того чтобы зашифровать сообщение, необходимо разбить его на биграммы (группы из двух символов). Возьмем, например, сообщение – HELLOW MOSCOW. Разобьём его на биграммы:

**HE LL OW MO SC OW**

Если два символа биграммы совпадают (или если остался один символ), то после первого символа добавляется буква «X» (в некоторых вариантах шифра Плейфера вместо «X» используется «Q»). В примере есть такая биграмма, поэтому преобразовываем последовательность биграмм:

**HE LX LO WM OS CO WX**

## Правила зашифрования

Если символы биграммы исходного текста встречаются в одной строке, то эти символы замещаются на символы, расположенные от них справа. Если символ является последним в строке, то он заменяется на первый символ этой же строки.

Например, для биграммы NO:

```
* * * * *  
* N A O S  
* * * * *  
* * * * *  
* * * * *
```

NO заменяется на AS

```
* * * * *  
* * * * *  
F N I * O  
* * * * *  
* * * * *
```

NO заменяется на IF

2. Если символы биграмм исходного текста встречаются в одном столбце, то они преобразуются в символы того же столбца, находящиеся непосредственно под ними. Если символ является нижним в столбце, то он заменяется на первый символ этого же столбца. Например, для биграммы NO:

```
* * N * *  
* * B * *  
* * * * *  
* * O * *  
* * Y * *
```

NO заменяется на BY

3. Если символы биграмм исходного текста находятся в разных столбцах и разных строках, то они заменяются на буквы, находящиеся в тех же строках под (над) второй буквой биграммы (в углах прямоугольника). Например, для биграммы NO:

```
E * * N *  
* * * * *  
* * * * *  
O * * S *  
* * * * *
```

NO заменяется на ES

## Шифрование биграмм. Пример

Полученные биграммы сообщения: HE LX LO WM OS CO WX.

Символы биграммы HE находится в одной строке, зашифрованная биграмма – BF.

Символы биграммы LX находятся в разных строках, зашифрованная биграмма – MW.

3) Символы биграммы LO находятся в разных строках, зашифрованная биграмма – KD.

4) Символы биграммы WM находятся в разных строках, зашифрованная биграмма – XL.

5) Символы биграммы OS находятся в разных строках, зашифрованная биграмма – AQ.

6) Символы биграммы CO находятся в одном столбце, заменяются символами непосредственно находящимися под ними – KC.

7) Символы биграммы WX находится в одной строке, зашифрованная биграмма – XZ.

Полученное зашифрованное сообщение: **BFMWKDXLAQKCXZ.**

G	O	D	A	Y
B	C	E	F	H
I	K	L	M	N
P	Q	R	S	T
U	V	W	X	Z

Расшифрование сообщения производится способом наоборот относительно правил зашифрования. Например, буквы биграммы **BF** находятся в одно строке и для расшифрования следует брать соседку слева для каждой буквы. Получаем **HE**. Однако, если буквы биграммы образуют прямоугольник, то исходное правило сохраняется без изменения. Например, биграмма **KD** расшифровывается как **LO**.

После расшифрования из текста выбрасываются все лишние буквы X.

Самостоятельно: Зашифровать методом Плейфера сообщение

**IDIOCY OFTEN LOOKS LIKE INTELLIGENCE**



## *Шифрование текста на русском языке*

При шифровании текста на русском языке способом Плейфера все правила, естественно, остаются прежними. Изменяется только матрица. Она имеет размер 4 x 8.

Если два символа биграммы совпадают (или если остался один символ), то после первого символа добавляется буква «Ъ».

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

Самостоятельно: Зашифровать методом Плейфера сообщение

**ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ**