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.

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

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**

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

HE LX LO WM OS CO WX

Правила зашифрования

1. 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 биграммы 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 биграммы 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.

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

Полученное зашифрованное сообщение: **BFMWKDXLAQKCXZ**.

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».

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

Самостоятельно: Зашифровать методом Плейфера сообщение

ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ