**100**

**ЧЕСТНАЯ ИГРА (PLAYFAIR)**

Шифр Плейфеир использовался в тактических целях британскими вооруженными силами во Второй Англо-Бурской войне и в Первой мировой войне, а также австралийцами и немцами во время Второй Мировой Войны . Причиной использования шифра Плейфера было то, что он достаточно быстр в применении и не требует никакого специального оборудования. Основной целью использования этой системы шифрования была защита важной, но не секретной информации во время ведения боя. К тому времени, когда вражеские криптоаналитики взламывали сообщение, информация уже была бесполезна для них. Использование шифра Плейфера в настоящее время является нецелесообразным, потому что современные переносные компьютеры могут легко взломать шифр в течение нескольких секунд.

Для шифрования сообщения необходимо разбить его на биграммы (группы из двух символов), при этом, если в биграмме встретятся два одинаковых символа, то между ними добавляется заранее оговоренный вспомогательный символ (в оригинале – **X**, для русского алфавита - **Я**). Например, «зашифрованное сообщение» становится «за ши фр ов ан но ес о**Я** об ще ни е**Я**».



Затем, руководствуясь следующими правилами, выполняется зашифровывание пар символов исходного текста:

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

2. Если символы биграммы исходного текста встречаются в одном столбце, то они преобразуются в символы того же столбца, находящимися непосредственно под ними. Если символ является нижним в столбце, то он заменяется на первый символ этого же столбца.

3. Если символы биграммы исходного текста находятся в разных столбцах и разных строках, то они заменяются на символы, находящиеся в тех же строках, но соответствующие другим углам прямоугольника.

Для расшифровки необходимо выполнить действия, противоположные описанным.

Пример шифрования.

- биграмма «за» формирует прямоугольник – заменяется на «жб»;

- биграмма «ши» находятся в одном столбце – заменяется на «юе»;

- биграмма «фр» находятся в одной строке – заменяется на «хс»;

**ЗАДАНИЕ**

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| а | л | г | е | б | р |
| в | д | ё | ж | з | и |
| й | к | м | н | о | п |
| с | т | у | ф | х | ц |
| ч | ш | щ | ъ | ы | ь |
| э | ю | я | \_ | , | . |

Используя шифр Playfair, расшифруй следующий шифртекст:

**ЙВ НО АЪ БЕ ХЗ М, ЦШ УЭ АФ РД ЙВ НО АЪ БЕ ЙХ ПЛ ЧЗ ЛС Щ.**