**Лабораторная работа № 3.1**

**Реализация алгоритма шифрования Плейфера**

**1 Цель работы: изучить и закрепить умение шифровать информацию алгоритмом Плейфера.**

**2 Порядок выполнения работы:**

**2.1 Выбрать язык программирования.**

**2.2 Изучить материал.**

**2.3 Выполнить задания.**

**2.4 Ответьте на контрольные вопросы.**

**2.4.1 Как зашифровывается сообщение в шифре Плейфера?**

**2.5 Оформить отчет.**

**Теоретические сведенья:**

Шифр Плейфера использует матрицу 5х5 (для латинского алфавита, для кириллического алфавита необходимо увеличить размер матрицы до 4х8), содержащую ключевое слово или фразу. Для создания матрицы и использования шифра достаточно запомнить ключевое слово и четыре простых правила. Чтобы составить ключевую матрицу, в первую очередь нужно заполнить пустые ячейки матрицы буквами ключевого слова (не записывая повторяющиеся символы), потом заполнить оставшиеся ячейки матрицы символами алфавита, не встречающимися в ключевом слове, по порядку (в английских текстах обычно опускается символ «Q», чтобы уменьшить алфавит, в других версиях «I» и «J» объединяются в одну ячейку). Ключевое слово может быть записано в верхней строке матрицы слева направо, либо по спирали из левого верхнего угла к центру. Ключевое слово, дополненное алфавитом, составляет матрицу 5х5 и является ключом шифра.

Для того чтобы зашифровать сообщение, необходимо разбить его на биграммы (группы из двух символов), например «Hello World» становится «HE LL OW OR LD», и отыскать эти биграммы в таблице. Два символа биграммы соответствуют углам прямоугольника в ключевой матрице. Определяем положения углов этого прямоугольника относительно друг друга. Затем, руководствуясь следующими 4 правилами, зашифровываем пары символов исходного текста:

1. Если два символа биграммы совпадают (или если остался один символ), добавляем после первого символа «Х», зашифровываем новую пару символов и продолжаем. В некоторых вариантах шифра Плейфера вместо «Х» используется «Q».

2. 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.

3. 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.

4. 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 использовать инверсию этих четырёх правил, откидывая символы «Х» (или «Q»), если они не несут смысла в исходном сообщении.

Пример:

Используем ключ «playfair example», тогда матрица примет вид:

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

Зашифруем сообщение «Hide the gold in the tree stump»  
HI DE TH EG OL DI NT HE TR EX ES TU MP  
1. Биграмма HI формирует прямоугольник, заменяем её на BM.  
2. Биграмма DE расположена в одном столбце, заменяем её на ND.  
3. Биграмма TH формирует прямоугольник, заменяем её на ZB.  
4. Биграмма EG формирует прямоугольник, заменяем её на XD.  
5. Биграмма OL формирует прямоугольник, заменяем её на KY.  
6. Биграмма DI формирует прямоугольник, заменяем её на BE.  
7. Биграмма NT формирует прямоугольник, заменяем её на JV.  
8. Биграмма HE формирует прямоугольник, заменяем её на DM.  
9. Биграмма TR формирует прямоугольник, заменяем её на UI.  
10. Биграмма EX находится в одной строке, заменяем её на XM.  
11. Биграмма ES формирует прямоугольник, заменяем её на MN.  
12. Биграмма TU находится в одной строке, заменяем её на UV.  
13. Биграмма MP формирует прямоугольник, заменяем её на IF.

Получаем зашифрованный текст «BM ND ZB XD KY BE JV DM UI XM MN UV IF»

Таким образом сообщение «Hide the gold in the tree stump» преобразуется в «BMNDZBXDKYBEJVDMUIXMMNUVIF»

**Практическая часть**

**Задание №1**

Зашифровать системой Плейфера индивидуальную фразу.

В качестве индивидуальной фразы зашифровать «Название любимой книги и ее автора».

В качестве ключа использовать слово из таблицы.

|  |  |
| --- | --- |
| № | Ключ |
| 1 | буйвол |
| 2 | мальта |
| 3 | портрет |
| 4 | архив |
| 5 | совершенство |
| 6 | удар |
| 7 | знакомство |
| 8 | советник |
| 9 | мгновенье |
| 10 | гвардейцы |