ЛАБОРАТОРНАЯ РАБОТА № 9

ШИФР ПЛЕЙФЕРА

Цель работы: изучение принципа шифрования информации с помощью биграммного шифра Плейфера.

Описание лабораторной работы. Шифр Плейфера, или квадрат Плейфера — ручная симметричная техника шифрования, в которой впервые использована замена биграмм. Изобретена в 1854 г. Чарльзом Уитстоном, но названа именем лорда Лайона Плейфера, который внедрил данный шифр в государственные службы Великобритании. Шифр предусматривает шифрование пар символов (биграмм) вместо одиночных символов, как в шифре подстановки и в более сложных системах шифрования Виженера. Таким образом, шифр Плейфера более устойчив к взлому по сравнению с шифром простой замены, так как затрудняется частотный анализ, который может быть проведен, но не для 26 возможных символов (латинский алфавит), а для $26 \times 26 = 676$ возможных биграмм. Анализ частоты биграмм возможен, но является значительно более трудоемким и требует намного большего объема зашифрованного текста.

Шифр Плейфера использует матрицу 5×5 для латинского алфавита (для кириллического алфавита необходимо увеличить размер матрицы до 6×6), 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 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 5×5 и является ключом шифра.

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 ниже сформулированными четырьмя правилами, зашифровываем пары символов исходного текста.

1. Если два символа биграммы совпадают, добавляем после первого символа «X», зашифровываем новую пару символов и продолжаем процесс шифрования. В некоторых вариантах шифра Плейфера вместо вставки «X» 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 замещаются на 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 замещаются на символы, находящиеся в тех же строках, но соответствующие другим углам прямоугольника.

Для расшифрования необходимо использовать инверсию этих четырех правил, откидывая символы «X» (или «Q»), если они не несут смысла в исходном сообщении.

Пример работы с программой

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 ее на BM.
2. Биграмма DE расположена в одном столбце, заменяем ее на ND.
3. Биграмма TH формирует прямоугольник, заменяем ее на ZB.
4. Биграмма EG формирует прямоугольник, заменяем ее на XD.
5. Биграмма OL формирует прямоугольник, заменяем ее на KY.
6. Биграмма DI формирует прямоугольник, заменяем ее на BE.
7. Биграмма NT формирует прямоугольник, заменяем ее на JV.

8. Биграмма HE формирует прямоугольник, заменяем ее на DM.
9. Биграмма TR формирует прямоугольник, заменяем ее на UI.
10. Биграмма EX находится в одной строке, заменяем ее на XM.
11. Биграмма ES формирует прямоугольник, заменяем ее на MN.
12. Биграмма TU расположена в одной строке, заменяем ее на UV.
13. Биграмма MP формирует прямоугольник, заменяем ее на IF.

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

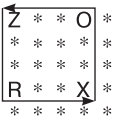
Таким образом, сообщение «Hide the gold in the tree stump» преобразуется в «BMNDZBXDKYBEJVDMUIXMMNUVIF».

Пример работы с программой

Предположим, что необходимо зашифровать биграмму **OR**. Рассмотрим четыре случая:

OR заменяется на **YZ**.

OR заменяется на **BY**.



OR заменяется на **ZX**.

OR заменяется на **ZY**.

Главное окно программы ШИФР ПЛЕЙФЕРА (The Playfair cipher) имеет вид, представленный на рис. 3.1.

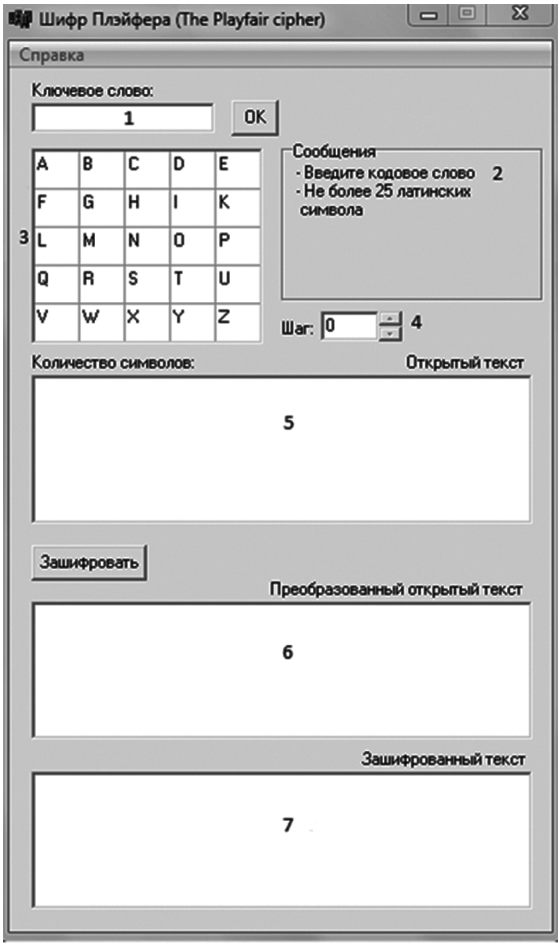


Рис. 3.1. Главное окно программы

Интерфейс программы включает несколько полей.

1. Поле ввода ключевого слова.
2. Форма вывода текстовых сообщений.
3. Ключевая матрица.
4. Кнопка просмотра результатов шифрования в пошаговом режиме.
5. Поле для ввода исходного текста.
6. Поле для вывода преобразованного открытого текста.
7. Поле для вывода зашифрованного текста.

Задание

Для выполнения лабораторной работы на компьютере необходимо установить программу *Playfair. exe*, используемую для демонстрации метода шифрования Плейфера.

1. Для того чтобы начать работу с программой, необходимо ввести ключевое слово в соответствующее поле и нажать кнопку OK. При этом первые ячейки ключевой матрицы займут символы ключевого слова (без повторяющихся символов).

***Внимание*!** Ключевое слово может состоять только из букв латинского алфавита (кроме буквы *J*), длина ключевого слова не более 25 символов.

2. В поле **«Открытый текст»** ввести (или же вставить комбинацией **Ctrl-V**) текст, который необходимо зашифровать. Вводить можно любые символы (буква J, при шифровании, заменится символом I). Нажать на кнопку **«Зашифровать»**.

3. В поле **«Преобразованный открытый текст»** отобразится обработанный текст, а в поле **«Зашифрованный текст»** — результат шифрования.

4. С помощью переключателя **«Шаг»** можно последовательно наблюдать, каким образом шифруется каждая биграмма.

5. Сохранить в отчете экранные формы, демонстрирующие процесс шифрования исходного текста. Сделать выводы по проделанной работе.

6. Включить в отчет о лабораторной работе ответы на контрольные вопросы, выбранные в соответствии с номером варианта из табл. 3.1.

Таблица 3.1

Номер варианта	Контрольные вопросы
1, 5, 7, 3, 9, 18, 28	К какому классу шифров относится шифр Плейфера? Укажите особенности подобных шифров
2, 4, 6, 8, 20, 22, 24, 26, 30	Опишите процедуры шифрования и расшифрования по методу Плейфера
11, 13, 15, 10, 17, 19, 27	Оцените криптостойкость изученного метода шифрования и возможности использования подобных методов в современных криптосистемах
12, 14, 16, 21, 23, 25, 29	Зашифруйте свою фамилию шифром Плейфера вручную. Сравните результаты ручного шифрования и полученные с помощью программы *Playfair.exe*