Лабораторная работа №1
«Классические шифры»

1. Цель работы:

Изучение классических методов шифрования.

2. Основные теоретические сведения:

Все классические алгоритмы шифрования основываются на использовании двух операций: *замены*, означающей замещение каждого элемента открытого текста (бита, буквы, группы битов или группы букв) некоторым другим элементом, и *перестановки*, означающей изменение порядка следования элементов открытого текста. При этом главным требованием оказывается отсутствие потерь информации (т.е. обратимость всех операций). В большинстве реальных систем шифрования применяют не одну, а комбинацию нескольких операций замены и перестановки. Соответствующие шифры называются продукционными.

2.1. Шифр Цезаря.

В шифре Цезаря каждая буква алфавита заменяется буквой, которая находится на три позиции дальше в этом же алфавите.

```
Открытый текст:     АБВГДЕЁЖЗИЙКЛМНОПРСТУФХЦЧШЩЪЫЬЭЮЯ
Шифрованный текст: ГДЕЁЖЗИЙКЛМНОПРСТУФХЦЧШЩЪЫЬЭЮЯАБВ
```

Необходимо обратить внимание на то, что алфавит считается "циклическим", поэтому после «Я» идет «А».

Например:

```
Открытый    текст: ИСТРОФИЛОВ КОНСТАНТИН ГЕННАДЬЕВИЧ
Шифрованный текст: ЛФХУСЧЛОСЕ НСРФХГРХЛР ЁЗРРГЖЯЗЕЛЪ
```

Алгоритм дешифрования аналогичен: каждая буква алфавита заменяется буквой, которая находится на три левей в этом же алфавите

2.2. Шифр Плейфера (Playfair).

Данный шифр базируется на методе многобуквенного шифрования, в котором биграммы открытого текста рассматриваются как самостоятельные единицы, преобразуемые в заданные биграммы шифрованного текста. Алгоритм основан на использовании матрицы букв размерности 5x6 (для английского языка 5x5), созданной на основе некоторого ключевого слова.

Матрица создается путем размещения букв, использованных в ключевом слове, слева направо и сверху вниз (повторяющиеся буквы отбрасываются). Затем оставшиеся буквы алфавита размещаются в естественном порядке в оставшихся строках и столбцах матрицы. Буквы «Ё», «Й», «Ъ» заменяются соответственно на буквы «Е», «И», «Ь», и считаются одной и той же буквой (для английского языка буквы «I», «J»).

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

Открытый текст шифруется порциями по две буквы в соответствии со следующими правилами.

1. Если оказывается, что повторяющиеся буквы открытого текста образуют одну пару для шифрования, то между этими буквами вставляется специальная буква-заполнитель, например «Я». В частности, такое слово как «ПАССИВНЫЙ» будет преобразовано к виду «ПА СЯ СИ ВН ЫИ».
2. Если буквы открытого текста попадают в одну и ту же строку матрицы, каждая из них заменяется буквой, следующей за ней в той же строке справа – с тем условием, что для замены последнего элемента строки матрицы служит первый элемент той же строки. Например, «ДА» шифруется как «ЛБ».
3. Если буквы открытого текста попадают в один и тот же столбец матрицы, каждая из них заменяется буквой, стоящей в том же столбце сразу под ней, с тем условием, что для замены самого нижнего элемента столбца матрицы берется самый верхний элемент того же столбца. Например, «ТЫ» шифруется как «АТ».
4. Если не выполняется ни одно из приведенных выше условий, каждая буква из пары букв открытого текста заменяется буквой, находящейся на пересечении содержащей эту букву строки матрицы и столбца, в котором находится вторая буква открытого текста. Например, «ЦВ» шифруется как «УБ», а «ПР» – как «ЦИ».

Например:

```
Открытый    текст: ко нс та нт ин ге ня на дь ев ич
Шифрованный текст: мр жф аз зф фе лм шф зд вя жл оп
```

Алгоритм дешифрования немного отличается: во втором правиле буквы заменяются на предыдущие, причем первый элемент строки заменяется на последний; в третьем правиле буквы заменяются на буквы расположенные выше, причем верхняя буква заменяется нижней; а буквы заполнители из первого правила удаляются исходя из интуиции.

2.3. Шифр Виженера (Vigenere).

Этот шифр базируется на наборе правил моноалфавитной подстановки. Используется матрица, называемая «табло Виженера».

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

Процесс шифрования прост – необходимо по ключевой букве «К» и букве открытого текста «Л» найти букву шифрованного текста, которая находится на пересечении строки «К» и столбца «Л». В данном случае такой буквой является буква «Ц».

Чтобы зашифровать сообщение, нужен ключ, имеющий ту же длину, что и само сообщение. Обычно ключ представляет собой повторяющееся нужное число раз ключевое слово, чтобы получить строку подходящей длины. Например, если ключевым словом является «ИСТРОФИЛОВ», то сообщение «КОНСТАНТИН ГЕННАДЬЕВИЧ» шифруется следующим образом.

```
ключ:                ИСТРОФИЛОВИСТРОФИЛОВИ
открытый текст:      КОНСТАНТИНГЕННАДЬЕВИЧ
шифрованный текст:   УААВБФЦЮЧПЛЦАЮОШЕРРКА
```

Расшифровать текст также просто – буква ключа определяет строку, буква шифрованного текста, находящаяся в этой строке, определяет столбец, и в этом столбце в первой строке таблицы будет находиться соответствующая буква открытого текста.

2.4. Шифр Виженера с автоматическим выбором ключа.

В связи с тем, что в шифре Виженера шифрованный текст состоит из $n = длина(ключевое\ слово)$ моноалфавитных подстановок, вскрыть открытый текст можно атакой на моноалфавитный шифр узнав (или подобрав) n. Периодичности в ключевой строке можно избежать, используя для ключевой строки непериодическую последовательность той же длины, что и само сообщение. Виженер предложил подход, получивший название системы с автоматическим выбором ключа, когда последовательность ключевой строки получается в результате конкатенации ключевого слова с самим открытым текстом.

Например:

```
ключ:                ИСТРОФИЛОВКОНСТАНТИНГ
открытый текст:      КОНСТАНТИНГЕННАДЬЕВИЧ
шифрованный текст:   УААВБФЦЮЧПНУЫЯТДЙЧКЦЪ
```

При дешифровании каждая полученная буква открытого текста подписывается к ключу.

2.5. Шифр Хилла (Lester Hill).

Лежащий в его основе алгоритм заменяет каждые m последовательных букв открытого текста m буквами шифрованного текста. Подстановка определяется m линейными уравнениями, в которых каждому символу присваивается числовое значение (А = 0, Б = 1, … Я = 32). Например, при m = 3, получаем следующую систему уравнений:

$$Y_1 = (k_{11}X_1 + k_{12}X_2 + k_{13}X_3) \bmod 33,$$
$$Y_2 = (k_{21}X_1 + k_{22}X_2 + k_{23}X_3) \bmod 33,$$
$$Y_3 = (k_{31}X_1 + k_{32}X_2 + k_{33}X_3) \bmod 33.$$

Эту систему уравнений можно записать в виде произведения вектора и матрицы в следующем виде:

$$\begin{pmatrix} Y_1 \\ Y_2 \\ Y_3 \end{pmatrix} = \begin{pmatrix} k_{11} & k_{12} & k_{13} \\ k_{21} & k_{22} & k_{23} \\ k_{31} & k_{32} & k_{33} \end{pmatrix} \begin{pmatrix} X_1 \\ X_2 \\ X_3 \end{pmatrix}$$

где X и Y представляют соответственно открытый и шифрованный текст, а K – это матрица, представляющая ключ шифрования. Операции выполняются по модулю 33.

Рассмотрим, например, как будет зашифрован текст "ИСТРОФИЛОВКОНСТАНТИНГЕННАДЬЕВИ" при использовании ключа

$$K = \begin{pmatrix} 4 & 18 & 15 \\ 10 & 11 & 19 \\ 32 & 5 & 23 \end{pmatrix}$$

Первые три буквы открытого текста представлены вектором (9 18 19). Таким образом, $\begin{pmatrix} 4 & 18 & 15 \\ 10 & 11 & 19 \\ 32 & 5 & 23 \end{pmatrix} \begin{pmatrix} 9 \\ 18 \\ 19 \end{pmatrix} = \begin{pmatrix} 18 \\ 22 \\ 23 \end{pmatrix} = СХЦ$. Продолжая вычисления, получим для данного примера шифрованный текст вида

СХЦЩЗМОЛАВЭВЕЁСИУЛГДЮУЗЧЛБЪЩЛН.

Для расшифровки нужно воспользоваться матрицей, обратной K.

$$K^{-1} = \begin{pmatrix} 13 & 12 & 6 \\ 24 & 4 & 4 \\ 14 & 14 & 31 \end{pmatrix}$$

2.6. Шифр перестановки «Лесенка».

Открытый текст записывается вдоль наклонных строк определенной длины ("ступенек"), а затем считывается построчно по горизонтали. Например, чтобы зашифровать сообщение "ИСТРОФИЛОВКОНСТАНТИНГЕННАДЬЕВИЧ" методом «Лесенка» со ступеньками длиной 2, запишем это сообщение в виде

```
И Т О И О К Н Т Н И Г Н А Ь В Ч
 С Р Ф Л В О С А Т Н Е Н Д Е И
```

Шифрованное сообщение будет иметь следующий вид.

ИТОИОКНТНИГНАЬВЧСРФЛВОСАТНЕНДЕИ

Дешифрование очевидно.

2.7. Шифр вертикальной перестановки.

Шифр вертикальной перестановки предполагает запись текста сообщения в горизонтальные строки одинаковой длины и последующее считывание текста столбец за столбцом, но не по порядку, а в соответствии с некоторой перестановкой столбцов. Порядок считывания столбцов при этом становится ключом алгоритма. Рассмотрим следующий пример.

```
Ключ:                5 3 4 1 7 2 6
Открытый текст:      И С Т Р О Ф И
                     Л О В К О Н С
                     Т А Н Т И Н Г
                     Е Н Н А Д Ь Е
                     В И Ч Я Я Я Я
Шифрованный текст: РКТАЯФННЬЯСОАНИТВННЧИЛТЕВИСГЕЯООИДЯ
```

Дешифрование также очевидно.

3. Задание на лабораторную работу

1. С помощью шифра Цезаря зашифровать свои «ФамилияИмяОтчество».
2. С помощью шифра Плейфера зашифровать свои «ИмяОтчество», используя свою фамилию в качестве

ключевого слова.

3. С помощью шифра Виженера зашифровать свои «ИмяОтчество», используя свою фамилию в качестве ключевого слова.
4. С помощью шифра Хилла зашифровать первые 9 букв своих «ФамилияИмяОтчество», используя ключ $K = \begin{pmatrix} 4 & 18 & 15 \\ 10 & 11 & 19 \\ 32 & 5 & 23 \end{pmatrix}$.
5. С помощью шифра Виженера с автоматическим выбором ключа, зашифровать свои «ИмяОтчество», используя свою фамилию в качестве ключевого слова.
6. С помощью шифра «Лесенка» зашифровать свои «ФамилияИмяОтчество».
7. С помощью шифра вертикальной перестановки зашифровать свои «ФамилияИмяОтчество», используя ключ 5341726.

3*. Дополнительное задание на лабораторную работу.

Составить программу на языке высокого уровне (Pascal, C++) реализующую алгоритм шифрования:

1. Плейфера.
2. Хилла.
3. Виженера.
4. Виженера с автоматическим выбором ключа.
5. Вертикальной перестановки.

4. Содержание отчета

1. Название лабораторной работы.
2. Фамилия, Имя, Отчество, выполнившего лабораторную работу.
3. Вычисления для каждого пункта задания.
4. Ответ для каждого пункта.