УНИВЕРСИТЕТ ИТМО

Отчёт по практике на тему «Шифрование и дешифрование текста высокой важности.»

Выполнил:
Студент группы № П-862б
Думбасар Максим Александрович
Руководитель: Атурина В.А, Меленчук М.А

Санкт-Петербург, 2019

Введение

Во время прохождения практики на тему «Зашифровать осмысленный текст высокой важности. Шифрование и дешифрование выполнять без ключа» были рассмотрены следующие этапы:

- Постановка цели и задач.
- Формирование шагов к созданию.
- Выбор механизма шифрования.
- Проектирование модели разработки.
- Произведение реализации продукта.
- Выполнения тестирования программы.
- Совершения отладки продукта.

Цели и задачи

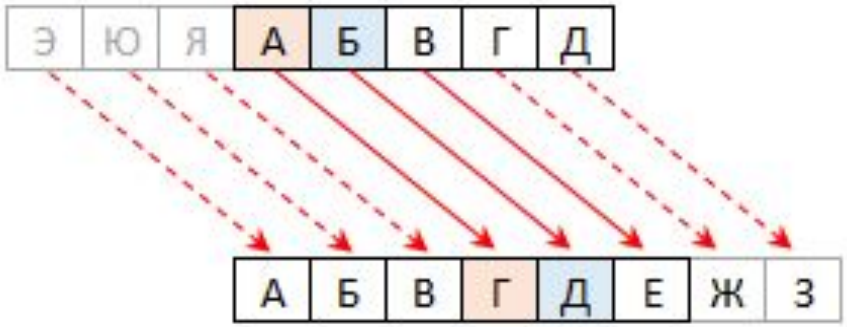
Целью практики является разработаться систему шифрование удовлетворяющею следующим требованиям:

- Шифрование и дешифрование выполнять без использования ключа.
- Задача должна быть реализована как законченное приложение со скрытыми формулами и открытыми полями ввода.
- При реализации учитывать особенности ввода данных так чтобы избежать переполнения или ошибок ввода.

Шифр Цезаря

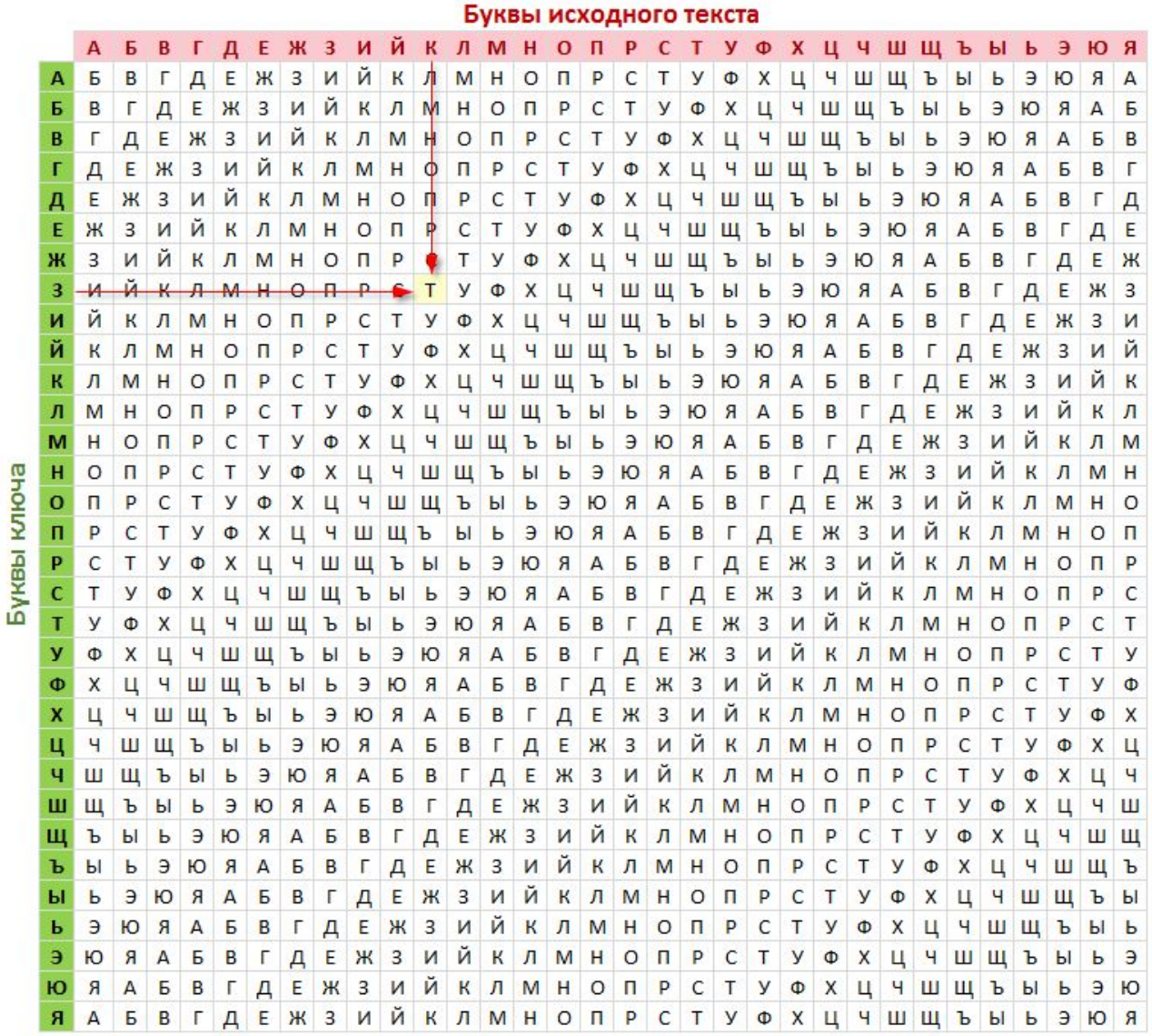
Шифр Цезаря - один из самых простых и наиболее широко известных методов шифрования.

Шифр Цезаря — это вид шифра подстановки, в котором каждый символ в открытом тексте заменяется символом, находящимся на некотором постоянном числе позиций левее или правее него в алфавите. Например, в шифре со сдвигом вправо на 3, А была бы заменена на Г, Б станет Д, и так далее.



Шифр Виженера

Шифр Виженера — это последовательность шифров Цезаря с различными значениями сдвига. То есть к первой букве текста применяется преобразование, например, ROT5, ко второй, например, ROT17, и так далее. Последовательность применяемых преобразований определяется ключевой фразой, в которой каждая буква слова обозначает требуемый сдвиг, например, фраза ГДЕ ОН задает такую последовательность шифров Цезаря: ROT3-ROT4-ROT5-ROT15-ROT14, которая повторяется, пока не будет зашифрован весь текст сообщения.



Буквы ключа \ Буквы исходного текста	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
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	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	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	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	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	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	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	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	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	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	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	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	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	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	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	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	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	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	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	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	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	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	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	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	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	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	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	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	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	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	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	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	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

Шифр Полибия

Шифр Полибия — это сдвиговый шифр, сдвигающий символ на один вверх или вниз в столбце. Например, со сдвигом вверх, А заменяется на Э, Б станет Ю, и так далее. Шифр назван в честь древнегреческого историка и полководца Полибия.

Реализация (1/4)

```
//шифрация Цезарь
var alphabet=new Array('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','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','0','1','2','3','4',
  '5','6','7','8','9',' ','.',',',';',':');
    function shifrcez(){
    var strokaishod=document.getElementById('a1').value;
    var strokarez='';
    var x;
    for (var i = 0; i < strokaishod.length; i++) {
    x=alphabet.indexOf(strokaishod[i])+3;
    if (x < 81) {strokarez += alphabet[x];} else {strokarez += alphabet[x-81];}

    }
    document.getElementById('a2').value=strokarez;
    }
```

Реализация (2/4)

```
//шифрование Виженер
var alphabet=new Array('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','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','0','1','2','3','4','5','6','7'
    ,'8','9',' ','.',',','!',':');
function shifrviz(){
var strokaishod=document.getElementById('a2').value;
var strokarez='';
var x;
var y;
var kluch='ключ';
var dlina=strokaishod.length/kluch.length;
kluch=kluch.repeat(Math.ceil(dlina));
for (var i = 0; i < strokaishod.length; i++) {
x=alphabet.indexOf(strokaishod[i]);
y=alphabet.indexOf(kluch[i]);
if (x + y < 81) {strokarez += alphabet[x+y];} else {strokarez += alphabet[x+y-81];}

}
document.getElementById('a2').value=strokarez;
}
```

Реализация (3/4)

```
var tablica=[
      ['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','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','0','1','2','3','4','5'],
      ['6','7','8','9',' ','.',',','-',';',':'],
      ];

  //шифрация Полибий
    function shifrpolib(){
    var strokanach=document.getElementById('a2').value;
    var strokaitog='';
    var z;
    var k;

    for (var n = 0; n < strokanach.length; n++) {
        for (var i = 0; i < 9; i++) {
            for (var j = 0; j < 9; j++) {
                if (tablica[i][j]==strokanach[n]) {
                z=j;
            if (i == 8) {k=0;} else {k=i+1;}
                }
            }
        }
      strokaitog += tablica[k][z];
    }


    document.getElementById('a2').value=strokaitog;
  }
```

Реализация (4/4)

Исходный текст: Зашифрованный текст: Расшифрованный текст: шифровать расшифровать

Допустимые символы:

АБВГДЕЁЖЗИЙКЛМНОПРСТУФХЦЧШЩЪЫЬЭЮЯ

абвгдеёжзийклмнопрстуфхцчшщъыьэюя

0123456789.,:!

УНИВЕРСИТЕТ ИТМО

Спасибо за внимание

Санкт-Петербург, 2019