Разработка программной платформы для шифрования и дешифрования с помощью ключа размер которого может быть меньше, чем шифруемый текст.

КОЖЕВНИКОВА П.В.

РУКОВОДИТЕЛЬ: АТУРИНА В.А,МЕЛЕНЧУК М.А.

Введение

Во время прохождения практики на тему «Шифрование и дешифрование текста высокой важности с использованием ключа размер которого может быть меньше, чем шифруемый текст..» 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

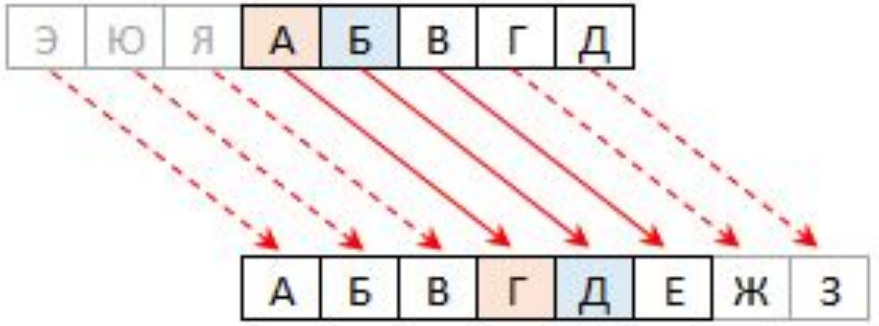
Целью практики является разработать систему шифрования удовлетворяющею следующим требованиям:

- Шифрование и дешифрование выполнять с использованием 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

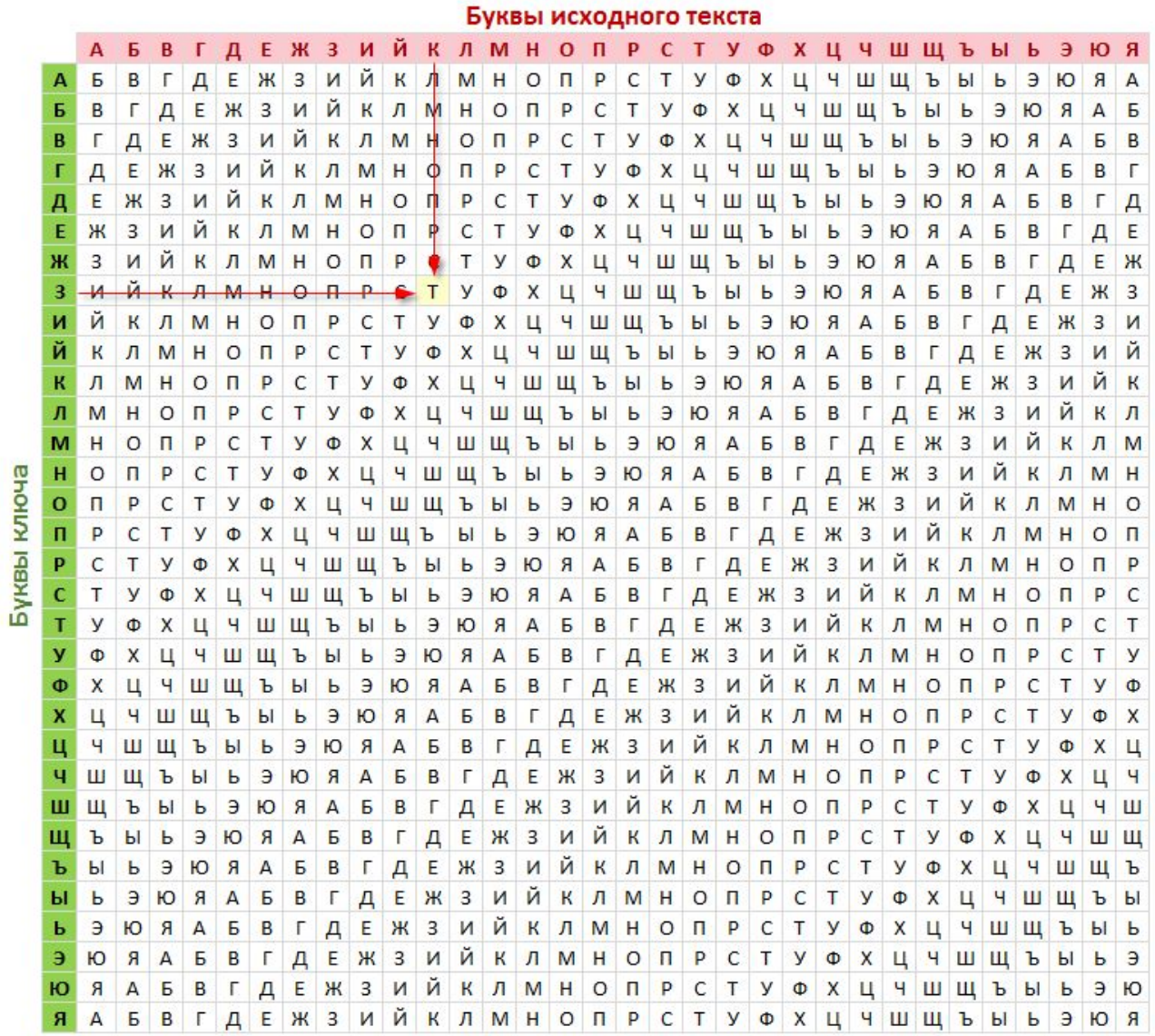
Шифр Цезаря - один из самых простых и наиболее широко известных методов шифрования.

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.



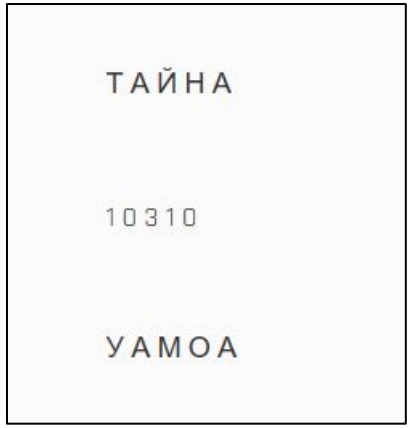
Шифр Виженера

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 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
Буквы ключа
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
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
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
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
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
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
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
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
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
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
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
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
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
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
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
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
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
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
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
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
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
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
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
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
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
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
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
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
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
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
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
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

Шифр Гронсфельда

Шифр Гронсфельда представляет собой модификацию шифра Цезаря числовым ключом. Для этого под буквами исходного сообщения записывают цифры числового ключа. Если ключ короче сообщения, то его запись циклически повторяют. Шифртекст получают примерно, как в шифре Цезаря, но отсчитывают по алфавиту не третью букву, а выбирают ту букву, которая смещена по алфавиту на соответствующую цифру ключа.



Реализация (1/4) Шифр Цезаря

```
<script>
        document.getElementById('a1').oninput=function()  {/
        let offset=document.getElementById("keyCAES").value;
        let str=this.value;
        console.log(str.charCodeAt(0));
        let out="";
        for(let i=0;i<str.length;i++){
            let code=str.charCodeAt(i);

            code=code+parseInt(offset);
            out+=String.fromCharCode(code);

        };
        document.getElementById("out").innerHTML=out;
    }
```

```
<script>
        document.getElementById('a1').oninput=function()  {//u
        let offset=document.getElementById("keyCAES").value;
        let str=this.value;
        console.log(str.charCodeAt(0));
        let out="";
        for(let i=0;i<str.length;i++){
            let code=str.charCodeAt(i);

            code=code+parseInt(offset);
            out+=String.fromCharCode(code);

        };
        document.getElementById("out").innerHTML=out;
    }




         document.getElementById('a4').oninput=function (){//p
        let offset1=document.getElementById("keyCAES").value;
        let str=this.value;
        console.log(str.charCodeAt(0));
        let out="";
        for(let i=0;i<str.length;i++){
            let code=str.charCodeAt(i);
            code=code-parseInt(offset1);
            out+=String.fromCharCode(code);

    }

    document.getElementById("out12").innerHTML=out;
}
```

Реализация(2/4)Шифр Гронсфельда

```
document.getElementById('out3').oninput=function () {//шифровка гронсфельдом

var key = document.getElementById("keyG").value;
var keyArr = key.split('');
var text = this.value;
var result = "";
var counter = 0;

for (var i = 0; i < text.length; ++i) {
var c = text.charCodeAt(i);

if (c === 32) {
counter = -1;
result += String.fromCharCode(c)
} else if (c < 1040 || c > 1103) {
result += String.fromCharCode(c)
} else if (c > 1071 && c < 1072) {
result += String.fromCharCode(c)
} else if (c >= 1072 && (parseInt(c) + parseInt(keyArr[counter])) > 1103) {
result += String.fromCharCode(parseInt(1071) + parseInt((parseInt(c) + parseInt(keyArr[counter]) -
     parseInt(1103))));
} else if (c <= 1071 && (parseInt(c) + parseInt(keyArr[counter])) > 1071) {
result += String.fromCharCode(parseInt(1039) + parseInt((parseInt(c) + parseInt(keyArr[counter]) -
     parseInt(1071))));
} else {
result += String.fromCharCode(parseInt(c) + parseInt(keyArr[counter]));
}

++counter;

if (counter === keyArr.length) {
counter = 0;
}
}

document.getElementById("out33").value = result;
}
```

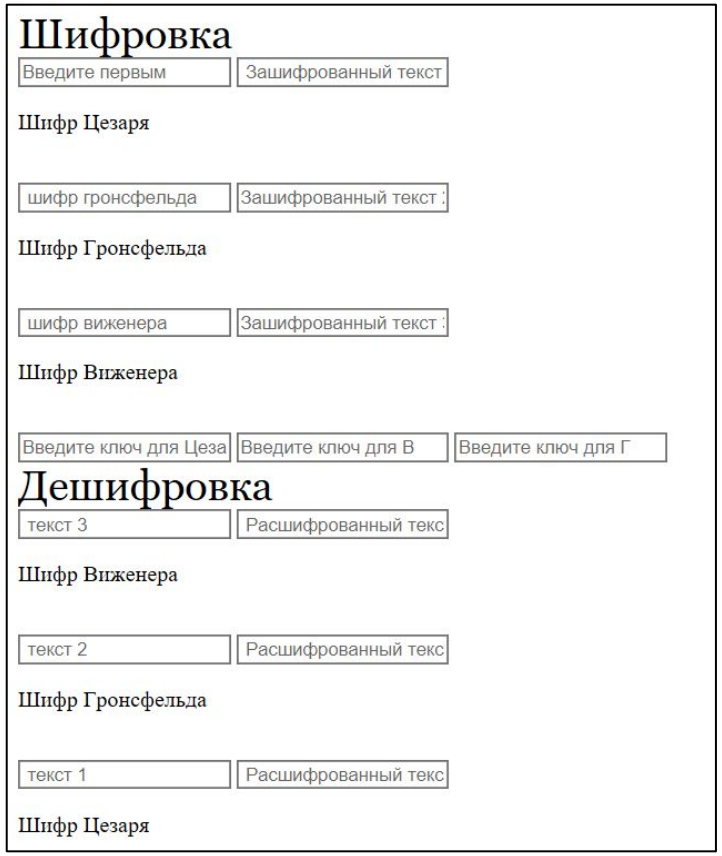

```
document.getElementById('out3').oninput=function () {//шифровка гронсфельдом

var key = document.getElementById("keyG").value;
var keyArr = key.split('');
var text = this.value;
var result = "";
var counter = 0;

for (var i = 0; i < text.length; ++i) {
var c = text.charCodeAt(i);

if (c === 32) {
counter = -1;
result += String.fromCharCode(c)
} else if (c < 1040 || c > 1103) {
result += String.fromCharCode(c)
} else if (c > 1071 && c < 1072) {
result += String.fromCharCode(c)
} else if (c >= 1072 && (parseInt(c) + parseInt(keyArr[counter])) > 1103) {
result += String.fromCharCode(parseInt(1071) + parseInt((parseInt(c) + parseInt(keyArr[counter]) -
     parseInt(1103))));
} else if (c <= 1071 && (parseInt(c) + parseInt(keyArr[counter])) > 1071) {
result += String.fromCharCode(parseInt(1039) + parseInt((parseInt(c) + parseInt(keyArr[counter]) -
     parseInt(1071))));
} else {
result += String.fromCharCode(parseInt(c) + parseInt(keyArr[counter]));
}

++counter;

if (counter === keyArr.length) {
counter = 0;
}
}

document.getElementById("out33").value = result;
}
```

Реализация(3/4)Шифр Виженера

```
document.getElementById('out4').oninput=function (){//шифровка виженром
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',' ','.',',','!',':');

var strokaishod=this.value;
var strokarez='';
var x;
var y;
var kluch=document.getElementById("keyVal").value;
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+1];} else {strokarez += alphabet[x+y-81];}

}
document.getElementById('out44').value=strokarez;
}
```

```
 document.getElementById('a2').oninput=function (){

    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',' ','.',',','!',':');
 var strokaishod=this.value;
var strokarez='';
var y;
var x;
var kluch=document.getElementById("keyVal").value;
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 < 0) {strokarez += alphabet[x-y+81];} else {strokarez += alphabet[x-y-1];}
}
document.getElementById('out2').value=strokarez;
}
```

Реализация (4/4) Интерфейс



Спасибо за внимание