

Разработка программы для шифрования и дешифрования текста особой важности

Выполнил:

Студент группы.№ П-862б

Игнатъев Леонид Сергеевич

Руководитель: Атурина В.А, Меленчук М.А

Введение

Во время прохождения практики на тему «Шифрование и дешифрование матрицы с использованием ключа» были рассмотрены следующие этапы:

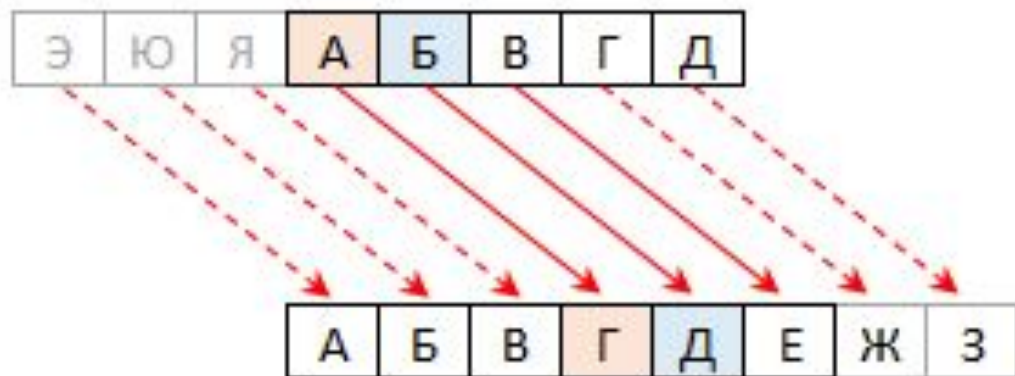
- 1) Постановка цели и задач.
- 2) Формирование шагов к созданию.
- 3) Выбор механизма шифрования.
- 4) Проектирование модели разработки.
- 5) Производство реализации продукта.
- 6) Выполнения тестирования программы.
- 7) Совершения отладки продукта.

Цели и задачи

Целью практики является разработать систему шифрования удовлетворяющую следующим требованиям:

- 1) Шифрование и дешифрование выполнять с использованием ключа.
- 2) Задача должна быть реализована как законченное приложение со скрытыми формулами и открытыми полями ввода.
- 3) 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.

Шифр Гронсфельд

Этот шифр сложной замены, называемый шифром 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 (как это делается в шифре Цезаря), а выбирают ту букву, которая смещена по алфавиту на соответствующую цифру ключа. Например, применяя в качестве ключа группу из четырех начальных цифр числа e (основания натуральных логарифмов), а именно 2718, получаем для исходного сообщения ВОСТОЧНЫЙ ЭКСПРЕСС следующий шифртекст:

| | A | B | C | D | E | F | G | H | I | J | K | L | M | N | O | P | Q | R | S | T | U | V | W | X | Y | Z |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| 0 | A | B | C | D | E | F | G | H | I | J | K | L | M | N | O | P | Q | R | S | T | U | V | W | X | Y | Z |
| 1 | B | C | D | E | F | G | H | I | J | K | L | M | N | O | P | Q | R | S | T | U | V | W | X | Y | Z | A |
| 2 | C | D | E | F | G | H | I | J | K | L | M | N | O | P | Q | R | S | T | U | V | W | X | Y | Z | A | B |
| 3 | D | E | F | G | H | I | J | K | L | M | N | O | P | Q | R | S | T | U | V | W | X | Y | Z | A | B | C |
| 4 | E | F | G | H | I | J | K | L | M | N | O | P | Q | R | S | T | U | V | W | X | Y | Z | A | B | C | D |
| 5 | F | G | H | I | J | K | L | M | N | O | P | Q | R | S | T | U | V | W | X | Y | Z | A | B | C | D | E |
| 6 | G | H | I | J | K | L | M | N | O | P | Q | R | S | T | U | V | W | X | Y | Z | A | B | C | D | E | F |
| 7 | H | I | J | K | L | M | N | O | P | Q | R | S | T | U | V | W | X | Y | Z | A | B | C | D | E | F | G |
| 8 | I | J | K | L | M | N | O | P | Q | R | S | T | U | V | W | X | Y | Z | A | B | C | D | E | F | G | H |
| 9 | J | K | L | M | N | O | P | Q | R | S | T | U | V | W | X | Y | Z | A | B | C | D | E | F | G | H | I |

Реализация Шифра Цезаря

```
function zezar(){
var alphabet=['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 sfsh ;
var shs=[];
sfsh=document.getElementById('vvod').value;
var x;
var n=document.getElementById('key_1').value;
sfsh=sfsh.split('');
for (var i = 0; i < sfsh.length; i++) {
x=alphabet.indexOf(sfsh[i])+n*1;
while(x>alphabet.length){
x=x-alphabet.length;
}
shs.push(alphabet[x]);
}
return shs;
}
```


Реализация Шифра Виженера

```
function vizener(){
var alphabet=['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 lol=zezar();
var shs_1=[];
var c;
var x;
var s;
lol=lol.split('');
var n=document.getElementById('key_2').value;
n=n.split('');
var key=[];
key.join(n);

for(var i=key.length;i<lol.length;i++){
n.push(n[i+key.length]);
}
for(var i=0;i<lol.length;i++){
c=alphabet.indexOf(n[i]);
x=alphabet.indexOf(lol[i]);
s=x+(c+1);
console.log(c);
console.log(x);
console.log(s);

while(s>alphabet.length-1){
s=s-alphabet.length;
}

shs_1.push(alphabet[s]);
var strokainend
}

strokainend=shs_1.join('');
return strokainend;
```

Реализация Шифра Гронсфелда

```
function first(){
var alphabet=['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 kluch=['0','1','2','3','4','5','6','7','8','9'];
var lol_1=vizener();
var shs=[];
var c;
var x;
var s;
lol_1=lol_1.split('');
var n=document.getElementById('key_3').value;
n=n.split('');
var key=[];
key.join(n);

for(var i=key.length;i<lol_1.length;i++){
n.push(n[i+key.length]);
}
for(var i=0;i<lol_1.length;i++){
c=kluch.indexOf(n[i]);
x=alphabet.indexOf(lol_1[i]);
s=x+c;
console.log(c);
console.log(x);
console.log(s);
while(s>alphabet.length-1){
s=s-alphabet.length;
}

shs.push(alphabet[s]);
}
document.getElementById('itog').value=shs.join('');
}
```

Исходный текст:

Ключ для Цезаря:

Ключ для Виженера:

Ключ для Гронсфельда:

Зашифрованный/Дешифрованный текст:

Шифровка

Дешифровка

Инструкция по использованию:

I. Шифровка:

- 1) В поле "Исходный текст" вы вводите текст который хотите зашифровать.
- 2) В поле "Ключ для Цезаря" вы вводите ключ для Цезаря(цифры).
- 3) В поле "Ключ для Виженера" вы вводите ключ для Виженера(цифры и буквы русского алфавита).
- 4) В поле "Ключ для Гронсфельда" вы вводите ключ для Гронсфельда(цифры).
- 5) В поле "Зашифрованный текст" выводится зашифрованный текст.

II. Дешифровка:

- 1) В поле "Исходный текст" вы вводите текст который хотите дешифровать.
- 2) В поле "Ключ для Цезаря" вы вводите ключ для Цезаря(цифры).
- 3) В поле "Ключ для Виженера" вы вводите ключ для Виженера(цифры и буквы русского алфавита).
- 4) В поле "Ключ для Гронсфельда" вы вводите ключ для Гронсфельда(цифры).
- 5) В поле "Зашифрованный текст" выводится дешифрованный текст.

Спасибо за внимание