**Міністерство освіти та науки України**

**НТУУ «КПІ ім. І.Сікорського»**

**Кафедра АПЕПС**

Звіт до лабораторної роботи №6

з предмету: «Безпека програм і даних»

на тему: *«Метод шифрування даних «шифр Тритеміуса»*

12 варіант

Виконав: студент 4 курсу  
 ТЕФ, ТІ-31  
 Ніколаєв В.В.

Перевірив: Тарнавський Ю.А.

Київ-2016

Цілі роботи:

Ознайомитись з методом шифрування даних «Щифр Тритеміуса» і надати його програмну реалізацію

Алгоритм шифрування:

1. Визначаємо код букви в алфавіті.

2. Обчислюємо крок зміщення k.

3. Знаходимо код зашифрованою літери, користуючись наступним рівнянням: L = (m + k) mod N, де L - код зашифрованої букви; m - код букви, яка шифрується; k - крок зміщення; N - число букв алфавіту.

4. За кодом L відновлюємо букву криптограми.

5. Повторюємо пункти 1-5 до закінчення тексту шифрограми.

Алгоритм розшифрування:

1. Визначаємо код букви в алфавіті.

2. Обчислюємо крок зміщення k.

3. Знаходимо код розшифрованої літери, користуючись наступним рівнянням: m =(L – k) mod N, де L - код зашифрованої букви; m - код розшифрованої букви; k - крок зміщення; N - число букв алфавіту.

4. За кодом m відновлюємо чергову букву криптограми.

5. Повторюємо пункти 1-5 до закінчення тексту криптограми.

В алгоритмах шифрування і розшифрування крок зміщення k може задаватись різними способами:

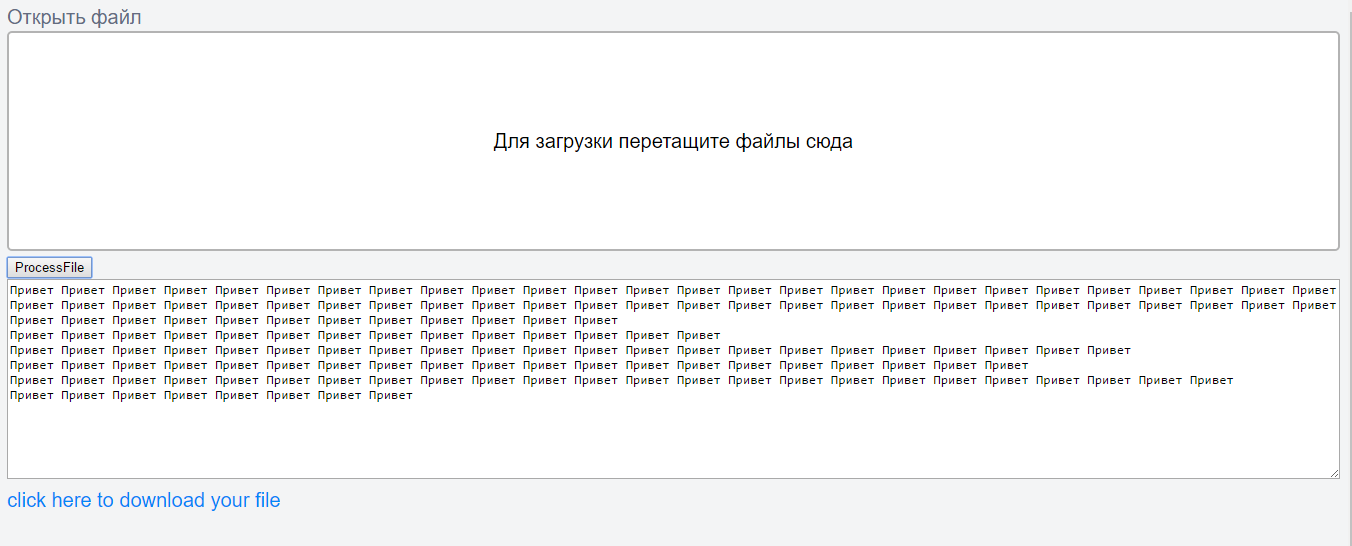
 За допомогою лінійного рівняння, наприклад, k=3t+1.

 За допомогою нелінійного рівняння, наприклад, k=8t2+4t +9.

 За допомогою використання гасла – текстового рядка, який багаторазово записується під текстом повідомлення (криптограми); крок зміщення в цьому випадку визначається номером в алфавіті відповідної букви гасла.

Тут t позначає порядковий номер букви в повідомленні (криптограмі).

В розробленому програмному продукті реалізоаний інтерфейс Драг-Н-Дроп, для можливості перетягування файлів будь-якого формату на активну зону, для пришвидшення вибору необхідного файлу.



Після кодування чи декодування файлу користувач має змогу його скачати, для подальшого використання.

Код программи

function Encoder(alph,encType){

alphabet=[];//алфавіт

t=0;//допоміжна змінна

key=0;//допоміжна змінна

size=0;//розмір алфавіту

/\*\*

функція кодування/ декодування

str - вхідні дані (текст)

decode - флаг декодування

\*/

this.encode=function(str,decode){

var result="";

if(encType=="linear"||encType=="nonlinear"){

for(var i=0;i<str.length;i++){

var t=i+1;//порядковий номер в повідомленні

if(encType=="linear")

var key=3\*t+1;

else if(encType=="nonlinear")

var key=-11\*t\*t+121\*t-117;

var index=alphabet.indexOf(str[i]);

if(index==-1){

throw new Error('Unknown symmbol! '+ str[i])

}

//перевірка шифратор чи дешифратор

//методи відрізняються лише знаком в формулі

//(index+key)%size чи (index-key)%size

if(decode){

key=-key;

}

var resultInd=(index+key)%size;

if(resultInd>=size){

resultInd=resultInd%size;

}

else if(resultInd<0){

while(resultInd<0){

resultInd+=size;

}

}

result+=alphabet[resultInd];

}

}

else if(encType=="string"){

var slogan;

if(alph=="english")

slogan="super private string";

else if(alph=="russian"){

slogan="супер приватная строка";

}

for(var i=0;i<str.length;i++){

var t=i+1;//порядковий номер в повідомленні

if(t>=slogan.size){

t=t%slogan.size

}

var key=alphabet.indexOf(slogan[t]);

var index=alphabet.indexOf(str[i]);

var resultInd=(index+key)%size;

if(resultInd>=size){

resultInd=resultInd%size;

}

else if(resultInd<0){

while(resultInd<0){

resultInd+=size;

}

}

result+=alphabet[resultInd];

}

}

else{

throw new Error(1);

}

//console.log(result)

return result;

}

//ЗАПОВНЕННЯ АЛФАВІТУ

if(alph=="english"){

for(var i='A';;i=nextChar(i)){

alphabet.push(i);

if(i=='z')

break;

}

}else if(alph=="russian"){

for(var i='А';;i=nextChar(i)){

alphabet.push(i);

if(i=='я')

break;

}

}

else{

throw new Error('Unimplemented alphabet '+alph);

}

for(var i=0;i<10;i++){

alphabet.push(i+'');

}

alphabet.push(' ','\n','=','-','\_','+','\*','/','!');

size=alphabet.length;

//console.log(this.alphabet);

/\*\*

Отримуємо символ з кодом більшим на 1

\*/

function nextChar(c) {

return String.fromCharCode(c.charCodeAt(0) + 1);

}

}

Висновки:

Було вивчено алгоритм вищевказаного шифру та реалізовано його з відповідністю до його специфікації. Був розроблений дружній інтерфейс користувача для спрощення роботи з програмою.