Міністерство освіти і науки України  
НТУУ «КПІ ім. І. Сікорського»

Кафедра цифрових технологій в енергетиці

Безпека інформаційних систем

Лабораторна робота № 2

«Шифрування методом гамування»

Варіант №1

Виконав:  
студент 2-го курсу НН ІАТЕ  
групи ТР-15  
Руденко Владислав Ігорович

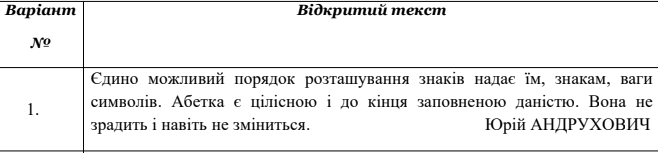
Перевірив:

доц. Онисько А. І.

Київ – 2022

**Завдання**

Завдання виконується індивідуально кожним студентом. Усі необхідні обчислення зі скріншотами описуються у звіті. Створити програму на будь-якій мові програмування для шифрування повідомлення із лабораторної роботи No1 (таблиця нижче) із використанням шифругамування. Додати скріншот зашифровування до звіту. Порівняти час на шифрування методом заміни (Цезаря) та методом гамування, якщо час не сильно відрязняється додайте де-кілька речень за власним бажанням (або обрати свій текст).



ПРИМІТКА! Текст було змінено на англомовний варіант через проблеми з компілятором.

**Теоретичні відомості**

Для зашифровування вхідної послідовності за цим методом відправник виконує побітове додавання по модулю 2 ключа k (відомий й одержувачу й відправнику) і m- розрядної двійкової послідовності, що відповідає повідомленню, яке пересилається:

ci=mi+ki, i=1,m, де mi, ki, ci – черговий i-й біт відповідно вихідного повідомлення m, ключа k і зашифрованого повідомлення с. Процес розшифровування зводиться до повторної генерації ключової послідовності й накладенню її на зашифровані дані. Рівняння розшифрування має вигляд:

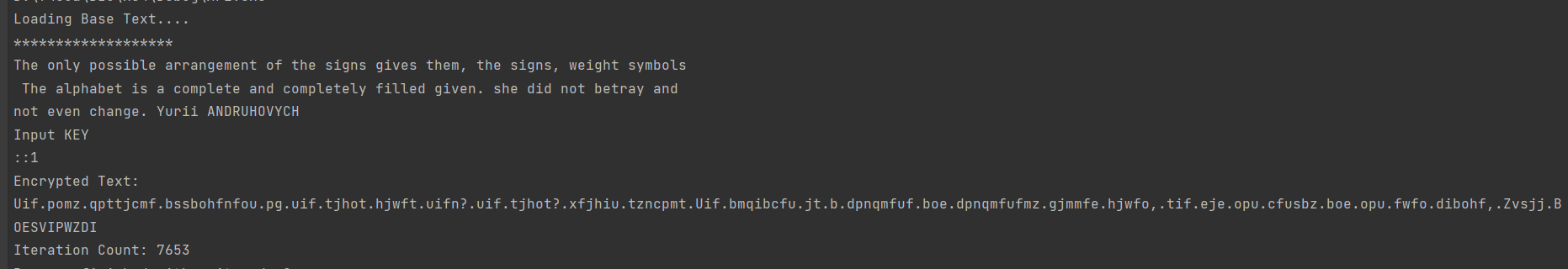
mi=ci–ki, i=1,m

Розрізняють гамування з кінцевою й нескінченною гамами. У якості кінцевої гами може використовуватися фраза, в якості нескінченної – послідовність, яка генерується генератором псевдовипадкових чисел. У тому випадку, коли безліччю використовуваних для шифрування знаків повідомлення є текст, відмінний від двійкового коду, то його символи й символи гами замінюються цифровими еквівалентами, які потім підсумовуються по модулю N. Процес зашифровування в цьому випадку визначається співвідношенням

ci=(mi+ri) mod N, i=1, m, де mi, ri, ci – черговий i-й знак вихідного повідомлення, гами й шифротексту відповідно;

N – кількість символів в алфавіті повідомлення; m – кількість знаків відкритого тексту. 2. Завдання до лабораторної роботи

**Результати виконання**

****

|  |  |  |
| --- | --- | --- |
| **Результати методів** | **Метод Цезаря** | **Метод Гамування** |
| **Кількість ітерацій** | **7946** | **7653** |

**Висновок**

В результаті виконання Лабораторної роботи №2 ознайомлено з методом шифрування «Гамування», що є поліпшеним варіантом методу Цезаря. В якості індивідуального завдання було переведено деякий текст в Шифро-Текст, за допомогою абетки та спеціального ключа. В ході виконання перевірено бистродію методу, за допомогою його порівняння з методом Цезаря. В результаті виявлено що метод гамування є швидшим за рахунок своєї математичної формули.

**Лістинг програми**

#include <iostream>  
#include <ostream>  
#include <vector>  
  
using namespace std;  
int INTER=0;  
  
int GetValue(char Word, vector<char> ABC)  
{  
 for(int i=0;i<ABC.size();i++)  
 {  
 INTER++;  
 if(Word == ABC[i])  
 return i;  
 }  
  
 return -1;  
   
}  
  
string Encryption(string& Text, int Key, vector<char> ABC)  
{  
 for(int i=0;i<Text.length();i++)  
 {  
 int TempWordValue = GetValue(Text[i],ABC);  
 if(TempWordValue == -1)  
 {  
 cout << "Error...Incorrect ABC\n"<< Text[i];  
 exit(-1);  
 }  
 Text[i] = ABC[(TempWordValue+Key)%ABC.size()];  
 INTER+=2;  
 }  
 return Text;  
}  
  
int main()  
{  
 vector<char> ABC = { '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','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', ' ', '.', ',', '?', '!'};  
 string Text = "The only possible arrangement of the signs gives them, the signs, weight symbols The alphabet is a complete and completely filled given. she did not betray and not even change. Yurii ANDRUHOVYCH";  
  
 cout << "Loading Base Text...." << endl << "\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*" << endl << Text << endl;  
 cout << "Input KEY\n::";  
 int KEY;  
 cin >> KEY;  
 cout << "Encrypted Text:\n" << Encryption(Text,KEY,ABC) << endl << "Iteration Count: " << INTER;  
   
}