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

Кафедра цифрових технологій в енергетиці

Безпека інформаційних систем

Лабораторна робота № 3

«Шифрування методом блокноту»

Варіант №1

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

Перевірив:

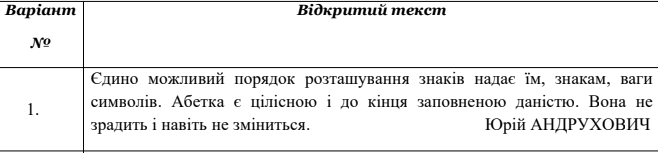
доц. Онисько А. І.

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 попередньої лабораторної роботи (таблиця нижче), використавши шифр одноразового блокноту з ключем

110000 011110 010100 110010 010110 011110

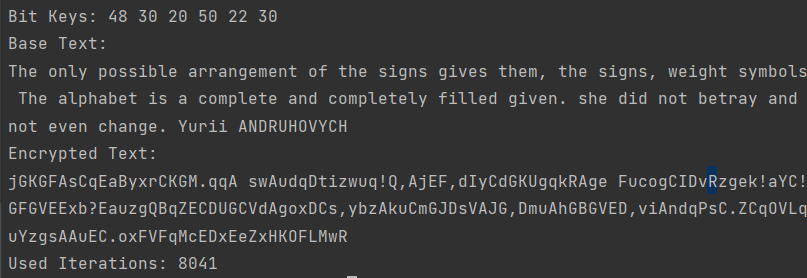


ПРИМІТКА! Текст було змінено на англомовний варіант через проблеми з компілятором.

**Теоретичні відомості**

У період класичної криптографії як правило не виникали потреби записувативідкритий текст та криптотекст якось інакше, ніж у звичайній абетці. Завдяки цьому криптограф-практик не потребував для роботи нічого, крім письмового приладдя свого часу, чого було достатньо і для шифрування, і для пересилання повідомлення. Але як тільки ми забажаємо скористатися модерними засобами зв’язку для передачі повідомлення, або доручити шифрування комп’ютерові, то виявимо, що у технічному відношенні традиційний текст не є найзручнішою формою для перетворення та передачі інформації. З цього погляду вигіднішим є подання інформації у цифровій формі. Ідея є зовсім простою – кожен символ тексту заміняємо його номером у алфавіті. Нагадаємо, що нумерацію починаємо з 0. Для прикладу, слово банан буде подане як 01 00 17 00 17. Кожна літерапредставлена своїм номером, записаним двома цифрами, перша з яких може бути нулем. При потребі в алфавіт можна включити окрім букв також знаки пунктуації, пропуск, цифри тощо. Номери букв ми можемо записувати не в десятковій системі числення, а у двійковій. Для того ж слова банан матимемо запис 000001 000000 010001 000000 010001, де кожний блок із шести цифр є номером відповідної букви у двійковому записі. Таку форму подання тексту називатимемо двійковою. Ми потребуємо не менше шести цифр, бо п’ятьма можна Записати щонайбільше 32 числа, в той час як українська абетка налічує 33 літери. Таким чином, довільний текст можна записати у двійковій формі, використовуючи всього лише два символи – 0 та 1 (один біт). Будь-яку послідовність бітів називають двійковим словом. Шифр одноразового блокноту був винайдений у 1917 році Гілбертом Вернамом. Він використовує операцію поступового додавання бітів за модулем 2, яку ми розглядаємо перед тим як описати сам шифр. Операція позначається символом ⨁ і задається виразами по модулю 2

**Результати виконання**

****

|  |  |  |
| --- | --- | --- |
| **Результати методів** | **Метод Блокноту** | **Метод Гамування** |
| **Кількість ітерацій** | **8048** | **7653** |

**Висновок**

В ході виконання лабораторної роботи №3 було ознайомлено з принципами шифрування методом блокноту, який відомий як шифр Вермана. На його основі розроблено програму яка шифрує деякий текст. Порівняно два типи шифрування: метод блокноту та метод гомування в результаті чого було виявлено що попри те, що метод блокноту займає більшу частину операцій, він є більш надійним способом шифрування данних.

**Лістинг програми**

#include <iostream>  
#include <string>  
#include <vector>  
  
using namespace std;  
  
int GetValue(char Word, vector<char> ABC)  
{  
 for(int i=0;i<ABC.size();i++)  
 {  
 if(Word == ABC[i])  
 return i;  
 }  
 return -1;  
   
}  
  
void Encryption(string &Text, int Key[6])  
{  
 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', ' ', '.', ',', '?', '!'};  
   
 int counter = 0;  
 for(char &word : Text)  
 {  
 int temp = GetValue(word, ABC);  
 temp = temp ^ Key[(counter < 7 ? counter : counter = 0)];  
 word = ABC[(temp < ABC.size() ? temp : temp%ABC.size())];  
 counter++;  
 }  
}  
  
int main(int argc, char\* argv[])  
{  
 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";  
 int key[6] = {0b110000, 0b011110, 0b010100, 0b110010, 0b010110, 0b011110};  
  
 cout << "Bit Keys: ";  
 for(int i=0;i<6;i++)  
 cout << key[i] << " ";  
 cout << endl;  
 cout<< "Base Text:" << endl << Text << endl;  
 Encryption(Text,key);  
 cout<< "Encrypted Text:" << endl << Text << endl;  
}