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

Кафедра цифрових технологій в енергетиці

Безпека інформаційних систем

Лабораторна робота № 1

«КЛАСИЧНИЙ ШИФР ПРОСТОЇ

ЗАМІНИ ТА ЙОГО КРИПТОАНАЛІЗ»

Варіант №1

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

Перевірив:

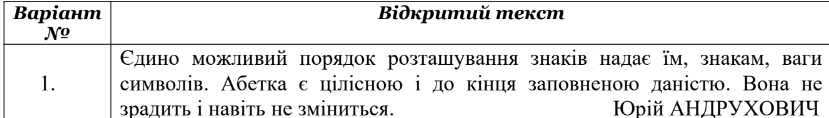
доц. Онисько А. І.

Київ – 2022

**Завдання**

1)Створити програму на будь-якій мові програмування для шифрування повідомлень із використанням шифру Цезаря (англійській алфавіт). Значення ключа шифрування визначається номером за алфавітним списком студента у журналі. Зашифрувати своє прізвище та дешифрувати отриманий шифротекст.

2)За допомогою програми CrypTool Online – <https://www.cryptool.org/en/cto/> з використанням шаблону Caesar виконати шифрування тексту шифром Цезарязгідно варіанту.



3) Завдання 3. Підрахувати частоти зустрічальності літер у шифротексті, використовуючи шаблон N-Gram Analysis в розділі криптоаналізу на сайті https://www.cryptool.org/en/cto

**Теоретичні відомості**

Розглянемо один з найдавніших та найбільш поширених шифрівпростої(моноалфавітної) заміни – шифр Цезаря, названий на честь римського імператораГаяЮліяЦезаря. У цьому шифрі кожна літера повідомлення зсувається в алфавіті на �–позиційвперед від символу, що замінюється. При досягненні кінця алфавіту виконуєтьсяциклічнийперехід до його початку. При необхідності розділові знаки та пробіли ігноруються.

Таким чином, наприклад, літерам алфавіту відповідатимуть числові позиції (табл. 1.1,табл. 1.2):

**Таблиця. 1.1. Нумерація позицій літер англійського алфавіту**

****

**Таблиця. 1.2. Нумерація позицій літер українського алфавіту**

****

Ключем шифрування є деяке фіксоване секретне число � – від 1 до 25 для англійського(латинського) алфавіту та � – від 1 до 32 для українського.

При дешифруванні літера зашифрованого тексту замінюється на літеру розташованувалфавіті на � позицій назад.

**Приклад 1.1:**

Відомо, що Цезар для шифрування використовував ключ K=3, тобто відбувавсязсувсимволів повідомлення на **три** позиції вперед у латинському алфавіті (рис. 1.1). Отже,повідомлення римського імператора ALEA JACTA EST (Жереб кинутий) післязашифрування буде мати вигляд DOHDMDFWDHVW.

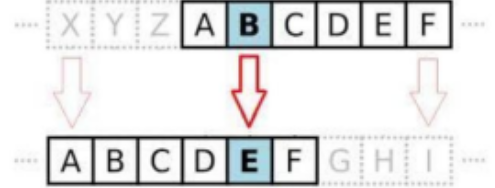
****

Рис. 1.1. Заміна символів повідомлення у шифрі Цезаря з ключемK=3

Зазначимо, що цей алгоритм шифрування, на сьогоднішній день, являється нестійкимдозламу і не використовується на практиці, проте є важливим для вивчення. Оскількивідомо,що навіть дуже складні сучасні криптосистеми в якості типових складових використовуютьпрості шифри заміни.

**Результати виконання**

**Завдання 1**

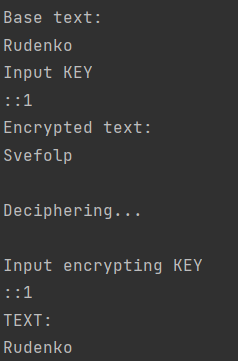
****

Рисунок 1 Виконання завдання

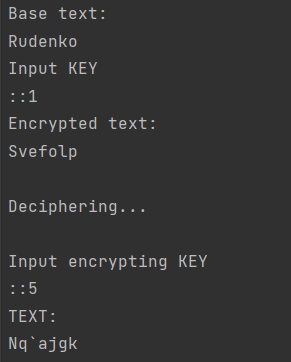
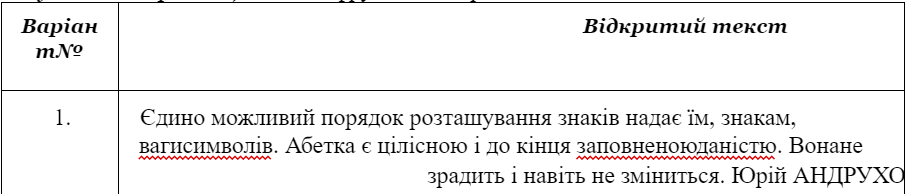


Рисунок 2 Результат використання хибного ключа

**Завдання 2**

****

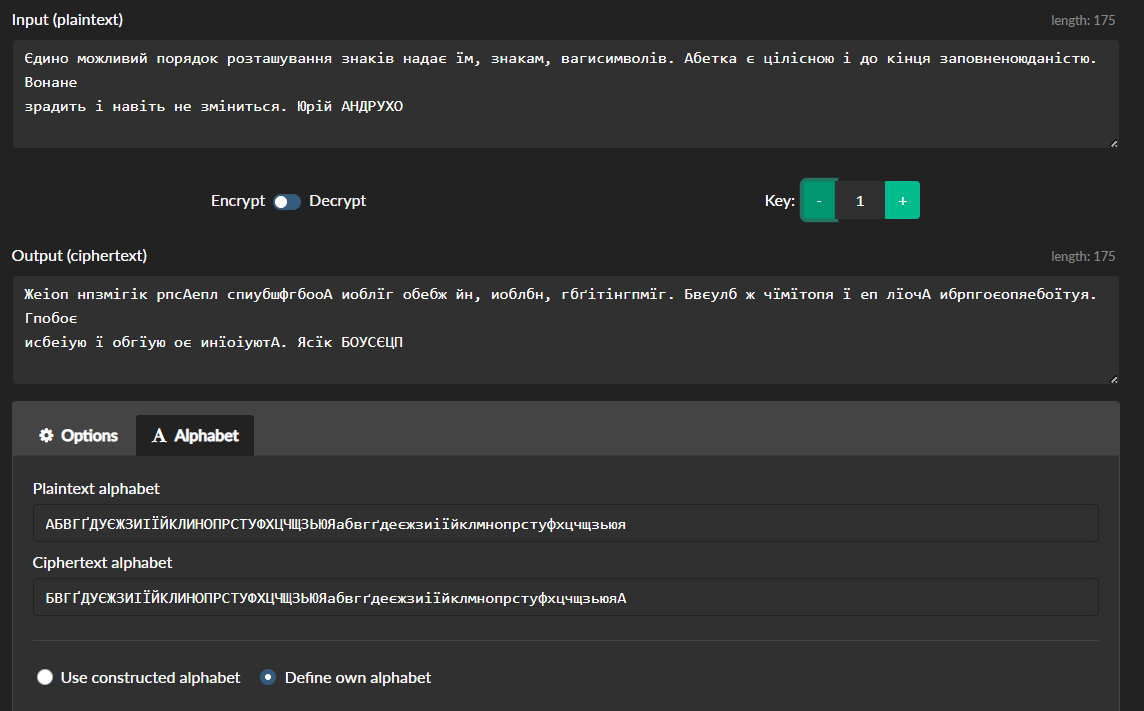
****

Рисунок 3 Шифрування деякого тексту наплатформі CrypTool

**Завдання 3**

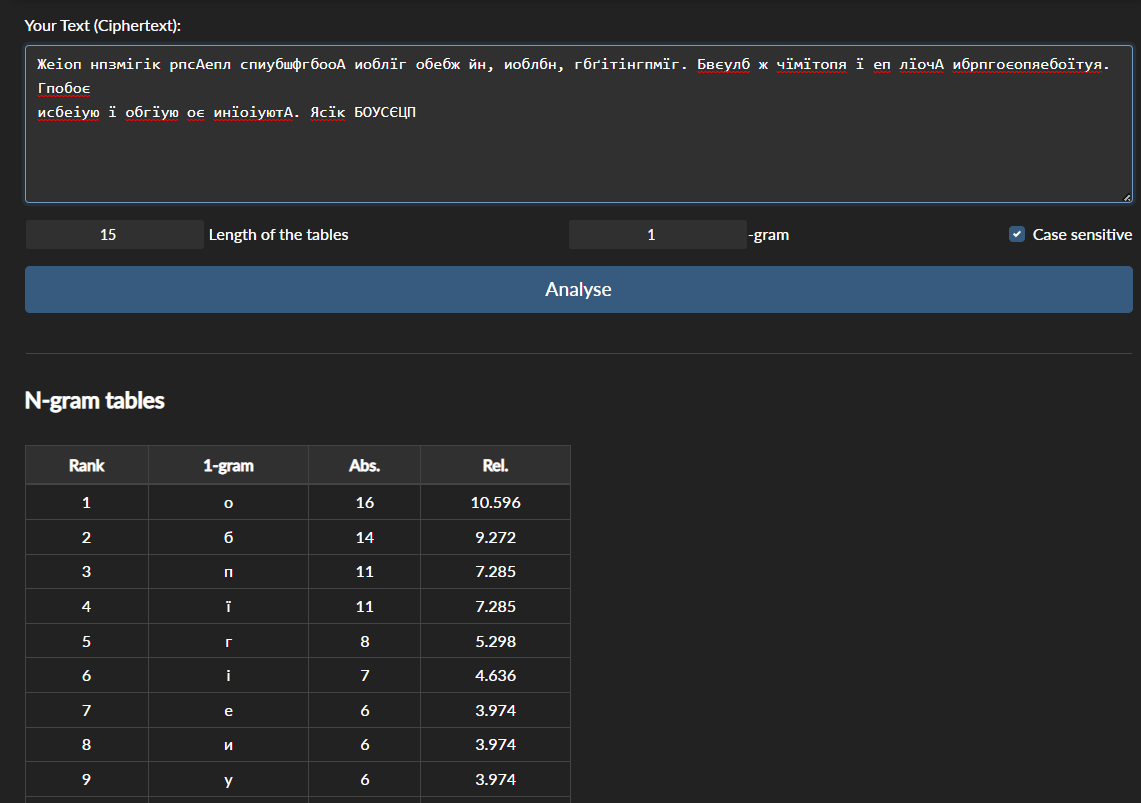
****

Рисунок 4 Підрахунок N-Gram Аналізу

Аналізуючи отримані дані було отримано ключ: 1. Підбір відбувався методом підбору на основі знаннях про найчастішою букви в абетці «п» та прирівняння її до перших 3х результатів. Таким чином ключ міг бути один із: «1» «14» «0»

**Висновок**

Під час виконання лабораторної роботи №1 було ознайомлено з базовими принципами шифрування та дешифрування. В якості першого методу було використано метод Цезаря. В ході виконання було проведено деяку кількість дослідів за для отримання навичок шифрування та дешифрування данним методом. В результаті виконання створенно програму, яка здатна шифрувати та дешифрувати деякий текст за домогою заданого ключа.

**Лістинг програми**

Посилання на онлайн-компілятор:

<https://replit.com/join/zsmaoqwzvu-hetik>

#include <iostream>  
#include <string>  
  
using namespace std;  
  
  
int main(int argc, char\* argv[])  
{  
 string BasicTEXT = "Rudenko";  
 int KEY;  
 cout << "Base text: " << endl << BasicTEXT << endl << endl << "Input KEY\n::";  
 cin >> KEY;  
 for (auto &word : BasicTEXT)  
 {  
 word = ((int)word + KEY);  
 }  
 cout << "Encrypted text: " << endl << BasicTEXT << endl << endl << "Deciphering...\n\nInput encrypting KEY\n::";  
 cin >> KEY;  
 for (auto &word : BasicTEXT)  
 {  
 word = ((int)word - KEY);  
 }  
 cout << "TEXT: " << endl << BasicTEXT;  
 return 0;  
}