**Міністерство освіти і науки України**

**Національний університет «Львівська політехніка»**

**Кафедра СКС**

****

# Звіт

до лабораторної роботи №1

# з дисципліни: «Захист інформації в комп’ютерних системах»

На тему: «Шифр моноалфавітної зміни (шифр Цезаря)»

# Варіант №3

Виконав:

ст.гр. КІ-307

Ващишин І.І.

Прийняв:

Морозов Ю.В.

Львів 2025

**Мета:** ознайомитись з основами класичної техніки шифрування – шифрами моноалфавітної заміни та типовим прикладом шифрів даного виду - шифром Цезаря.

**Теоретичні відомості**

При використанні моноалфавітної заміни окремі букви відкритого тексту заміняються іншими буквами або числами або якимись іншими символами. Якщо відкритий текст розглядається як послідовність бітів, то підстановка зводиться до заміни заданих послідовностей бітів відкритого тексту заданими послідовностями бітів шифрованого тексту.

Найдавнішим і найпростішим з відомих підстановочних шифрів є шифр, що використовувався Юлієм Цезарем. У шифрі Цезаря кожна буква алфавіту замінюється буквою, що перебуває на три позиції далі в цьому ж алфавіті. Найпростіше побачити це на прикладі.

Відкритий текст: meet me after the toga party

Шифрований текст: PHHW PH DIWHU WKH WRJD SDUMB

Зверніть увагу на те, що алфавіт вважається "циклічним", тому після Z іде А. Визначити перетворення можна, перелічивши всі варіанти, як показано нижче.

Якщо відомо, що певний текст був шифрований за допомогою шифру Цезаря, то за допомогою простого перебору всіх варіантів розкрити шифр дуже просто - для цього досить перевірити 25 можливих варіантів ключів.

Застосування методу послідовного перебору всіх можливих варіантів виправдано наступними трьома важливими характеристиками даного шифру:

1. Відомі алгоритми шифрування й дешифрування.

2. Необхідно перебрати всього 25 варіантів.

3. Мова відкритого тексту відома і легко пізнавана.

**Завдання лабораторної роботи**

1.Створити програму, що реалізує шифрування вихідного повідомлення за допомогою шифру Цезаря з врахуванням того, що повідомлення, що необхідно зашифрувати, написано українською мовою.

В якості кроку шифрування обирається номер студента у списку групи.

2. Оформити і захистити звіт.

**Хід виконання роботи:**

Крок шифрування згідно списку: 3

Програма реалізована на мові C++.

**Код програми:**

#include <iostream>

#include <string>

#include <locale>

#include <windows.h>

using namespace std;

string encrypt(const string& plaintext, int shift) {

string ciphertext = "";

int n = plaintext.length();

// Повний алфавіт української мови

string alphabet\_upper = "АБВГҐДЕЄЖЗИІЇЙКЛМНОПРСТУФХЦЧШЩЬЮЯ";

string alphabet\_lower = " абвгґдеєжзиіїйклмнопрстуфхцчшщьюя";

int alphabet\_size = alphabet\_upper.length();

for (int i = 0; i < n; i++) {

char c = plaintext[i];

// Знаходимо позицію символу у відповідному алфавіті

size\_t index = alphabet\_upper.find(c);

if (index != string::npos) { // Якщо символ знайдено в верхньому регістрі

c = alphabet\_upper[(index + shift) % alphabet\_size];

}

else { // Якщо символ знайдено в нижньому регістрі

index = alphabet\_lower.find(c);

if (index != string::npos) {

c = alphabet\_lower[(index + shift) % alphabet\_size];

}

}

ciphertext += c;

}

return ciphertext;

}

string decrypt(const string& ciphertext, int shift) {

string plaintext = "";

int n = ciphertext.length();

// Повний алфавіт української мови

string alphabet\_upper = "АБВГҐДЕЄЖЗИІЇЙКЛМНОПРСТУФХЦЧШЩЬЮЯ";

string alphabet\_lower = " абвгґдеєжзиіїйклмнопрстуфхцчшщьюя";

int alphabet\_size = alphabet\_upper.length();

for (int i = 0; i < n; i++) {

char c = ciphertext[i];

// Знаходимо позицію символу у відповідному алфавіті

size\_t index = alphabet\_upper.find(c);

if (index != string::npos) { // Якщо символ знайдено в верхньому регістрі

c = alphabet\_upper[(index - shift + alphabet\_size) % alphabet\_size];

}

else { // Якщо символ знайдено в нижньому регістрі

index = alphabet\_lower.find(c);

if (index != string::npos) {

c = alphabet\_lower[(index - shift + alphabet\_size) % alphabet\_size];

}

}

plaintext += c;

}

return plaintext;

}

int main() {

setlocale(LC\_CTYPE, "ukr");

SetConsoleCP(1251);

SetConsoleOutputCP(1251);

string plaintext, ciphertext;

int shift;

cout << "Введіть текст для шифрування: ";

getline(cin, plaintext);

cout << "Введіть зсув: ";

cin >> shift;

cin.ignore(); // очистка буфера вводу

shift %= 32; // обрізання зсуву до 33 символів

ciphertext = encrypt(plaintext, shift);

cout << "Зашифрований текст: " << ciphertext << endl;

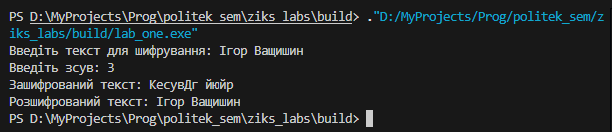
plaintext = decrypt(ciphertext, shift);

cout << "Розшифрований текст: " << plaintext << endl;

return 0;

}

**Результат виконання програми:**



**Табличні обрахунки:**

|  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **1** | **І** | **г** | **о** | **р** |  | **В** | **а** | **щ** | **и** | **ш** | **и** | **н** |
| **2** | **25** | **18** | **9** | **10** | **0** | **16** | **15** | **2** | **5** | **18** | **5** | **7** |
| **3** | **7** | **1** | **21** | **25** | **15** | **31** | **30** | **17** | **20** | **33** | **20** | **23** |
| **4** | **7** | **1** | **21** | **25** | **15** | **31** | **30** | **17** | **20** | **33** | **20** | **23** |
| **5** | **К** | **е** | **с** | **у** | **в** | **Д** | **г** |  | **й** | **ю** | **й** | **р** |

**Висновок:** на цій лабораторній роботі, я користуючись методичними вказівками навчився працювати з шифрами моноалфавітної заміни та розглянув типовий приклад шифрів даного виду, навчився виправляти помилки які можуть появитись та розібрався на практиці з шифрами Цезара. Також після перевірки встановив, що код працює правильно.