**Міністерство освіти та науки України**

**ДВНЗ «Український державний хіміко-технологічний університет»**

**Факультет комп’ютерних наук та інженерії**

**Кафедра спеціалізованих комп’ютерних систем**

**Звіт**

**з лабораторної роботи №2**

Виконав:

студент гр. 4-ІС-33

Філіпський П.В.

Керівник:

Брехов О.В.

Дніпро

2023

**Мета роботи**:  *зрозуміти, вивчити та реалізувати будь-яким відомим програмним засобом алгоритм реалізації афінного шифру*

**Код програми:**

#include <iostream>

#include <math.h>

#include <string.h>

#include <string>

#include <stdio.h>

#include <stdlib.h>

#include <algorithm>

#include <fstream>

#include <vector>

int gcd(int a, int b);

int modInverse(int a, int b);

int main() {

using namespace std;

string choice;

do {

cout << "Encrypt or Decrypt? [e/d] = ";

getline(cin, choice);

transform(choice.begin(), choice.end(), choice.begin(), tolower);

} while (choice.length() > 1 || choice != "e" && choice != "d");

cout << "\nInput string: ";

string input;

getline(cin, input);

int a, b;

do {

cout << "\na and b must be coprime\na = ";

cin >> a;

cout << "b = ";

cin >> b;

} while (cin.fail() || gcd(a, b) != 1);

cout << '\n';

if (choice == "e") {

for (int i = 0; i < input.length(); ++i) {

if (input[i] >= 'a' && input[i] <= 'z') {

cout << (char)((a \* (input[i] - 'a') + b) % 26 + 'a');

}

else if (input[i] >= 'A' && input[i] <= 'Z') {

cout << (char)((a \* (input[i] - 'A') + b) % 26 + 'A');

}

else {

cout << input[i];

}

}

}

else {

for (int i = 0; i < input.length(); ++i) {

if (input[i] >= 'a' && input[i] <= 'z') {

cout << (char)(modInverse(a, 26) \* (26 + input[i] - 'a' - b) % 26 + 'a');

}

else if (input[i] >= 'A' && input[i] <= 'Z') {

cout << (char)(modInverse(a, 26) \* (26 + input[i] - 'A' - b) % 26 + 'A');

}

else {

cout << input[i];

}

}

}

cout << '\n';

return 0;

}

int gcd(int a, int b) {

return b == 0 ? a : gcd(b, a % b);

}

int modInverse(int a, int b) {

int b0 = b, t, q;

int x0 = 0, x1 = 1;

if (b == 1) return 1;

while (a > 1) {

q = a / b;

t = b, b = a % b, a = t;

t = x0, x0 = x1 - q \* x0, x1 = t;

}

if (x1 < 0) x1 += b0;

return x1;

}

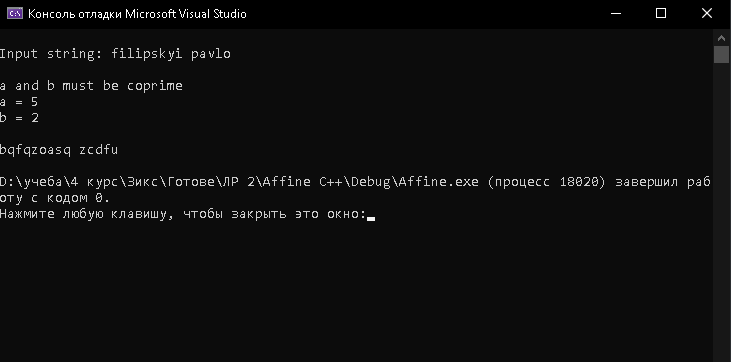


Рисунок 1 Шифрування тексту

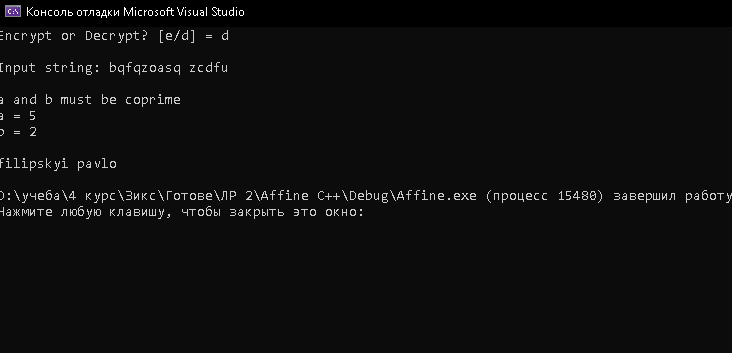


Рисунок 2 Дешифрування тексту

**Висновок**: Зрозумів, як працює афінний шифр та навчився його використовувати у практиці.