

Министерство образования Республики Беларусь
Учреждение образования
БЕЛОРУССКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ
ИНФОРМАТИКИ И РАДИОЭЛЕКТРОНИКИ

Факультет компьютерного проектирования

Кафедра ИПиЭ

Дисциплина: Криптографические технологии

Отчет
по Лабораторной работе №1
на тему «Криптоанализ классических шифров»

Студент гр. 910902

Шпак В.А.

Проверил

Давыдович К.И.

Минск 2022

Цель работы: изучить шифр Цезаря и шифр простой замены, научиться дешифровать текст.

Ход работы:

Цели лабораторной работы реализованы посредством программы на языке C++, листинг которой представлен ниже.

Задание 1.

А. Напишите программу дешифрования текста, зашифрованного с помощью шифра Цезаря.

С помощью метода подбора мы выяснили, что ключом смещения является 3.

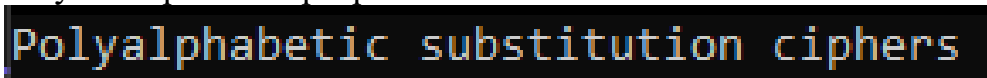
```
#include <iostream>
#include <string>

using namespace std;

string Decoder(int key, string str) {
    for (auto& c : str)
    {
        if (c == ' ')
            c = ' ';
        if (c >= 'A' && c <= 'Z') {
            c -= (key % 26);
            if (c >= 56 && c <= 64)
                c += 26;
        }
        if (c >= 'a' && c <= 'z') {
            c -= (key % 26);
            if (c >= 91 && c <= 96)
                c += 26;
        }
    }
    return str;
}

int main() {
    string code = "Srobdoskdehwlf vxevwlwxwlrq flskhuv";
    int key = 3;
    string str = Decoder(key, code);
    cout << str;
    return 0;
}
```

Результат работы программы:



Polyalphabetic substitution ciphers

Б. Найти ключ шифра простой замены, используя для дешифрования известный открытый текст.

Для решения данной задачи напишем цикл, который будет просматривать каждую букву зашифрованного и расшифрованного текстов, и заменять букву из алфавита буквой шифра. Так как в шифре представлены не все буквы алфавита, отсутствующие буквы заменим нулями.

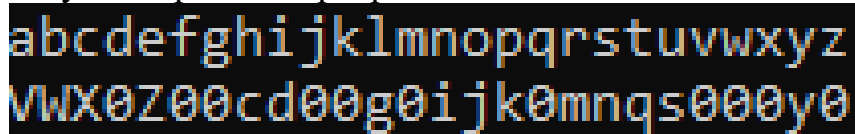
```
#include <iostream>
#include <string>
#include <cstring>
```

```

using namespace std;
void Cipher(char* str, char* shifr) {
    char alf1[] = "abcdefghijklmnopqrstuvwxyz";
    char res[26]{ '\0' };
    memset(res, '0', 26);
    for (int i = 0; i < strlen(str); i++) {
        for (int j = 0; j < strlen(alf1); j++) {
            if (alf1[j] == str[i]) {
                res[j] = shifr[i];
            }
        }
    }
    for (int i = 0; i < 26; i++) {
        cout << res[i];
    }
}
int main() {
    char alf1[] = "abcdefghijklmnopqrstuvwxyz";
    char code[] = "KjgyVgkcVWZqdX nSWnqdsqdi XdkcZmn";
    char text[] = "Polyalphabetic substitution ciphers";
    cout << alf1 << endl;
    Cipher(text, code);
    return 0;
}

```

Результат работы программы:



The screenshot shows the output of the program. The first line is the alphabet 'abcdefghijklmnopqrstuvwxyz'. The second line is the encrypted text 'VWX0Z00cd00g0ijk0mnqs000y0'. The text is displayed in a monospaced font with a black background and white characters.

Задание 2.

Написать программу, которая зашифрует и дешифрует ФИО, и сравнить результаты.

Для шифрования текста был выбран шифр Цезаря с ключом смешения 4.

```

#include <iostream>
#include <string>

using namespace std;

string Coder(int key, string str) {
    for (auto& c : str)
    {
        if (c == ' ')
            c = ' ';
        if (c >= 'A' && c <= 'Z') {
            c += (key % 26);
        }
        if (c >= 'a' && c <= 'z') {
            c += (key % 26);
        }
        if (c >= 56 && c <= 64 || c >= 91 && c <= 96) {
            c = c + 26;
        }
    }
    return str;
}

string Decoder(int key, string str) {
    for (auto& c : str)
    {
        if (c == ' ')
            c = ' ';
        if (c >= 'A' && c <= 'Z') {
            c -= (key % 26);
        }
    }
}

```

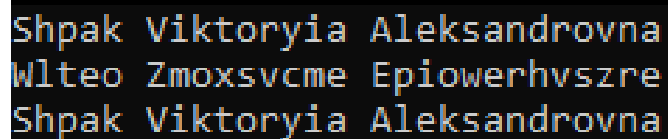
```

    }
    if (c >= 'a' && c <= 'z') {
        c -= (key % 26);
    }
    if (c >= 56 && c <= 64 || c >= 91 && c <= 96) {
        c = c + 26;
    }
}
return str;
}

int main() {
    setlocale(LC_ALL, "rus");
    string fio = "Shpak Viktoryia Aleksandrovna";
    int key = 4;
    cout << fio << endl;
    string code = Coder(key, fio);
    string text = Decoder(key, code);
    cout << code << endl << text << endl;
    return 0;
}

```

Результат работы программы:



```

Shpak Viktoryia Aleksandrovna
Wlteo Zmoxsvcmc Epiowerhvszre
Shpak Viktoryia Aleksandrovna

```

Как можем заметить программа правильно зашифровала и расшифровала исходный текст.

Вывод: таким образом, в ходе лабораторной работы были изучены шифр Цезаря и шифр простой замены, а также получены навыки написания программы шифрования и дешифрования с помощью изученных шифров.