ФГБОУ ВПО «Чувашский Государственный Университет им. И.Н.Ульянова»

Факультет информатики и вычислительной техники

Кафедра вычислительной техники

**Лабораторная работа №1  
“** **ШИФРОВАНИЕ ДАННЫХ МЕТОДОМ ПОДСТАНОВКИ”**

Выполнил: студент группы ИВТ-21-12  
 Чесноков Александр  
 Проверил: Павлов П.В.

Чебоксары, 2015

**Цель работы**

Целью работы является знакомство с классическим криптографическим алгоритмом - алгоритмом шифрования данных при помощи подстановки.

**Индивидуальное задание**

| **№ п.п.** | **V** | **m** |
| --- | --- | --- |
| **1** | **{0,1}** | **5** |

**Функция шифрования**

Параметры, заданные по своему варианту:

string V[32] = {

"00000", "00001", "00010", "00011", "00100", "00101", "00110", "00111",

"01000", "01001", "01010", "01011", "01100", "01101", "01110", "01111",

"10000", "10001", "10010", "10011", "10100", "10101", "10110", "10111",

"11000", "11001", "11010", "11011", "11100", "11101", "11110", "11111"

};

const int m = 5;

const int key = 5;

**Функция шифрования:**

В основе шифрования лежит ключ key = 5, он равен количеству сдвигов в массиве 5 символьных комбинаций в алфавите V;

string Encryption(string str, int key)

{

for (int i = 0; i < str.length(); i+=m)

for (int j = 0; j < 32; j++)

if (str.compare(i, 5, V[j]) == 0)

{

str.replace(i, 5, V[(j + key) % 32]);

break;

}

return str;

}

**Текст программы, реализующей индивидуальное задание**

#include <iostream>

#include <string>

using namespace std;

string V[32] = {

"00000", "00001", "00010", "00011", "00100", "00101", "00110", "00111",

"01000", "01001", "01010", "01011", "01100", "01101", "01110", "01111",

"10000", "10001", "10010", "10011", "10100", "10101", "10110", "10111",

"11000", "11001", "11010", "11011", "11100", "11101", "11110", "11111"

};

const int m = 5;

const int key = 5;

string Encryption(string str, int key);

string Decryption(string str, int key);

void main()

{

setlocale(LC\_ALL, "Russian");

string str;

string mess;

string encryptMess;

string decryptMess;

cout << "Введите исходный текст(длина кратная 5), используя алфавит(0,1): \n";

cin >> str;

if (str.length() % m != 0)

printf("Длина сообщения не кратна %d!", m);

else

{

mess = str;

encryptMess = Encryption(str, key);

str = encryptMess;

decryptMess = Decryption(str, key);

cout << "\nИсходное сообщение: " << mess;

cout << "\nШифрограмма: " << encryptMess;

cout << "\nДешифрованное сообщение: " << decryptMess;

}

cout << "\n\n";

system("pause");

}

string Encryption(string str, int key)

{

for (int i = 0; i < str.length(); i+=m)

for (int j = 0; j < 32; j++)

if (str.compare(i, 5, V[j]) == 0)

{

str.replace(i, 5, V[(j + key) % 32]);

break;

}

return str;

}

string Decryption(string str, int key)

{

key = 32 - key;

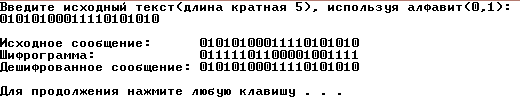
str = Encryption(str, key);

return str;

}

**Пример открытого текста и соответствующей ему шифрограммы**

Пример работы программы:



**Вывод**

Я ознакомился с классическим криптографическим алгоритмом - алгоритмом шифрование данных методом подстановки и реализовал его в среде программирования VS2013 на языке C++.