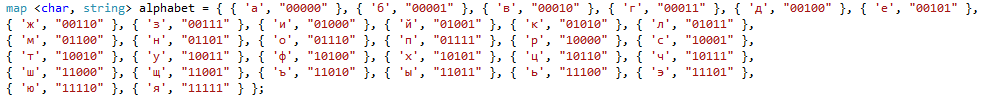
**Садов Д.В. ИВБО 7-14.**

**Лабораторная работа №2** В данной лабораторной работе нужно было реализовать шифр Виженера.

Реализована программа следующим образом:

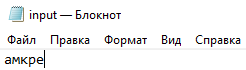
1. Каждой букве русского алфавита ставится в соответствие число в двоичном виде.

получается ассоциативный массив, в программе это реализовано с помощью контейнера map:



1. Далее из файла input.txt считывается посимвольно строка, которую нужно зашифровать. Каждый символ ищется в контейнере и в строку dvoichniy (изначально пустая) дописывается соответсвующее представение этого символа в двоичном виде.

Т.е. при введенной в файле следующей строке :



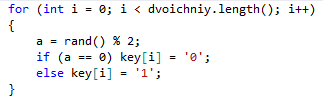
Строка dvoichniy будет иметь вид



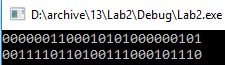
Для наглядности данная строка выводится пользователю



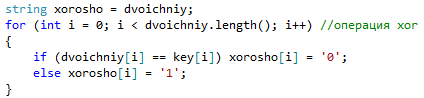
1. Далее генерируется рандомный двоичный ключ (строка такого же размера как dvoichniy)

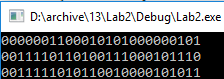


Для наглядности он выводится под выведенной исходной строкой



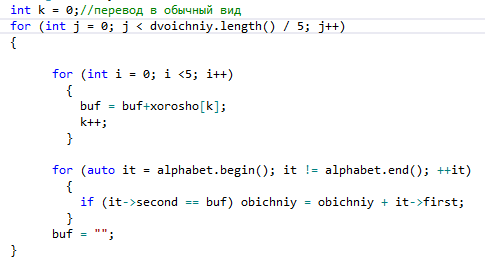
1. Формируется новая строка используя операцию xor для каждой пары символов (строка-ключ). Если символы равны в ключе и в исходной строке, то в новой строке записывается 0, если различны – 1.





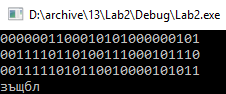
5 Сформированная новая строка переводится из двоичного вида в символьный

следующим образом:



Создается подстрока из 5 символов и это строка ищется в контейнере по полю значения, и возвращает ключ. Т.е в данном случае берутся 00111 и находится соответствие – символ ‘з’

Новая сформированная строка выводится пользователю



**Листинг программы (файл input.txt есть на гитхабе)**

#include <iostream>

#include <fstream>

#include <string>

#include <map>

#include <time.h>

#include <stdlib.h>

#include <math.h>

using namespace std;

int main(int args, const char \* argv[])

{

setlocale(LC\_ALL, "rus");

srand(time(NULL));

map <char, string> alphabet = { { 'а', "00000" }, { 'б', "00001" }, { 'в', "00010" }, { 'г', "00011" }, { 'д', "00100" }, { 'е', "00101" },

{ 'ж', "00110" }, { 'з', "00111" }, { 'и', "01000" }, { 'й', "01001" }, { 'к', "01010" }, { 'л', "01011" },

{ 'м', "01100" }, { 'н', "01101" }, { 'о', "01110" }, { 'п', "01111" }, { 'р', "10000" }, { 'с', "10001" },

{ 'т', "10010" }, { 'у', "10011" }, { 'ф', "10100" }, { 'х', "10101" }, { 'ц', "10110" }, { 'ч', "10111" },

{ 'ш', "11000" }, { 'щ', "11001" }, { 'ъ', "11010" }, { 'ы', "11011" }, { 'ь', "11100" }, { 'э', "11101" },

{ 'ю', "11110" }, { 'я', "11111" } };

string input\_text; //ввод данных из входного файла

ifstream inputFile;

inputFile.open("input.txt");

getline(inputFile, input\_text, '\0');

inputFile.close();

string dvoichniy; //перевод считанной строки в двоичный вид

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

{

auto in = alphabet.find(input\_text[i]);

dvoichniy = dvoichniy + in->second;

}

int a = 0;

string key = dvoichniy; //формирование ключа

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

{

a = rand() % 2;

if (a == 0) key[i] = '0';

else key[i] = '1';

}

cout << dvoichniy << endl;

cout << key << endl;

string xorosho = dvoichniy;

for (int i = 0; i < dvoichniy.length(); i++) //операция xor

{

if (dvoichniy[i] == key[i]) xorosho[i] = '0';

else xorosho[i] = '1';

}

cout << xorosho << endl;

string buf;

string obichniy;

int k = 0;//перевод в обычный вид

for (int j = 0; j < dvoichniy.length() / 5; j++)

{

for (int i = 0; i <5; i++)

{

buf = buf+xorosho[k];

k++;

}

for (auto it = alphabet.begin(); it != alphabet.end(); ++it)

{

if (it->second == buf) obichniy = obichniy + it->first;

}

buf = "";

}

cout << obichniy<<endl;

cin.get();

return 0;

};