Федеральное государственное автономное

образовательное учреждение

высшего образования

«СИБИРСКИЙ ФЕДЕРАЛЬНЫЙ УНИВЕРСИТЕТ»

Институт космических и информационных технологий

Кафедра вычислительной техники

**ОТЧЕТ ПО ЛАБОРАТОРНОЙ РАБОТЕ**

Симметричные шифры. Шифр Трисемуса (вариант 7)

Руководитель от университета \_\_\_\_\_\_\_\_\_\_ Сидарас А.А.

подпись, дата

Студент КИ19-06б, 031940417 \_\_\_\_\_\_\_\_\_\_ Шнайдер А.В.

подпись, дата

Красноярск 2020

**СОДЕРЖАНИЕ**

[ВВЕДЕНИЕ 3](#_Toc69410691)

[Ход выполнения работы 4](#_Toc69410692)

[1. Подробное описание алгоритма шифрования 4](#_Toc69410693)

[2. Листинг составленной программы 4](#_Toc69410694)

[3. Контрольные примеры работы программы 9](#_Toc69410695)

[ЗАКЛЮЧЕНИЕ 12](#_Toc69410696)

ВВЕДЕНИЕ

Задание к работе: согласно варианту разработать программу шифрования и дешифрования текста. На ряде контрольных примеров открытого текста, состоящего из различного количества символов, проверить правильность работы алгоритмов шифрования и дешифрования.

Ход выполнения работы

1. Подробное описание алгоритма шифрования

Для шифрование методом Трисемуса составляют таблицу с алфавитом. Сначала записываю поочерёдно буквы ключевого слова без повторений, а затем записывают весь оставшийся алфавит. Пример такой таблицы с ключевым словом defense приведён в таблице 1.

Таблица 1 – Пример таблицы Трисемуса

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| d | e | f | n | s | a | b |
| c | g | h | i | j | k | l |
| m | o | p | q | r | t | u |
| v | w | x | y | z | - | - |

Само шифрование происходит следующим образом – берут букву из заданного для шифрования слова (строки) и заменяют её на букву на строку ниже в том же столбце. Буквы из нижней строки заменяются на буквы первой строки. Если алфавит не позволяет заполнить таблицу полностью (т.е. остаются прочерки в последней строке), то по такому же правилу заменяются и буквы, находящиеся на строку выше прочерков. Таким образом по составленной выше таблице фраза «hello neighbor» будет заменена на «pguuw igqoplwz». Расшифровка происходит аналогично, но со сдвигом строки вверх.

2. Листинг составленной программы

#include <iostream>

#include <fstream>

#include <string>

using namespace std;

int search(string alph[26], string n)

{

for (size\_t i = 0; i < 26; i++)

{

if (alph[i] == n)

{

return i;

}

}

return -1;

}

string cryption(string alph[26], string f)

{

string s, n;

int j;

for (size\_t i = 0; i < f.length(); i++)

{

if (f[i] == ' ')

{

s.push\_back(' ');

}

else

{

n.clear();

n.push\_back(f[i]);

j = search(alph, n);

if (j < 0)

{

cout << "В фразе был встречен необрабатываемый символ. Шифрование не удалось." << endl;

return f;

}

else if ((j > 0) && (j < 19))

{

s.append(alph[j + 7]);

}

else if ((j > 18) && (j < 21))

{

s.append(alph[j - 14]);

}

else

{

s.append(alph[j - 21]);

}

}

}

return s;

}

string decryption(string alph[26], string f)

{

string s, n;

int j;

for (size\_t i = 0; i < f.length(); i++)

{

if (f[i] == ' ')

{

s.push\_back(' ');

}

else

{

n.clear();

n.push\_back(f[i]);

j = search(alph, n);

if (j < 0)

{

cout << "В фразе был встречен необрабатываемый символ. Расшифровка не удалась." << endl;

return f;

}

else if ((j > 0) && (j < 5))

{

s.append(alph[j + 21]);

}

else if ((j > 4) && (j < 7))

{

s.append(alph[j + 14]);

}

else

{

s.append(alph[j - 7]);

}

}

}

return s;

}

int main()

{

setlocale(LC\_ALL, "");

string alph[26] = { "d", "e", "f", "n", "s", "a", "b",

"c", "g", "h", "i", "j", "k", "l",

"m", "o", "p", "q", "r", "t", "u",

"v", "w", "x", "y", "z" };

string s;

cout << "Пожалуйста, помните - алфавит шифровки включает в себя только латиницу нижнего регистра" << endl;

cout << "Выберите режим. Зашифровать - 0, расшифровать - 1" << endl;

int i;

cin >> i;

while ((i != 1) && (i != 0))

{

cout << "Выбран неверный режим работы программы." << endl;

cout << "Выберите режим. Зашифровать - 0, расшифровать - 1" << endl;

cin >> i;

}

ifstream ist;

ist.open("ist.txt");

getline(ist, s);

ofstream ost;

ost.open("ost.txt");

if (i == 0)

{

cout << "Исходный текст: " << s << endl;

s = cryption(alph, s);

cout << "Зашифрованный текст: " << s << endl;

ost << s;

}

else

{

cout << "Зашифрованный текст: " << s << endl;

s = decryption(alph, s);

cout << "Расшифрованный текст: " << s << endl;

ost << s;

}

return 0;

}

**3. Контрольные примеры работы программы**

Примеры работы представлены на рисунках 1 – 10.

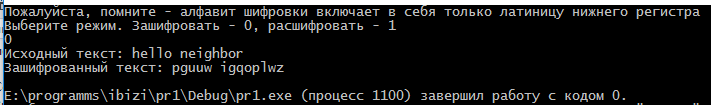


Рисунок 1 – Зашифровка фразы “hello neighbor”

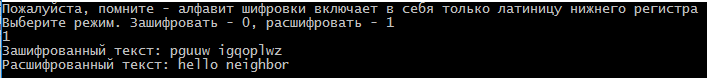


Рисунок 2 – Расшифровка фразы “pguuw igqoplwz”

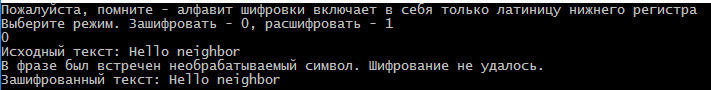


Рисунок 3 – Зашифровка фразы “Hello neighbor”

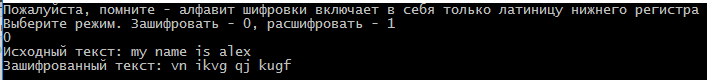


Рисунок 4 – Зашифровка фразы “my name is alex”

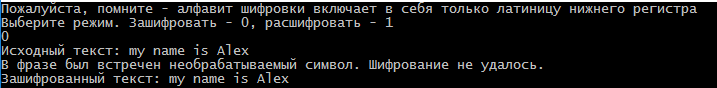


Рисунок 5 - Зашифровка фразы “my name is Аlex”

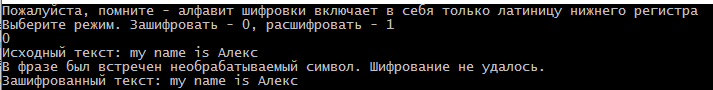


Рисунок 6 – Зашифровка фразы “my name is Алекс”

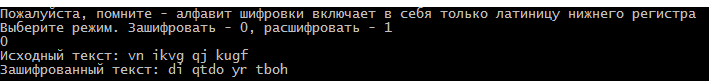


Рисунок 7 – Расшифровка фразы “ di qtdo yr tboh”

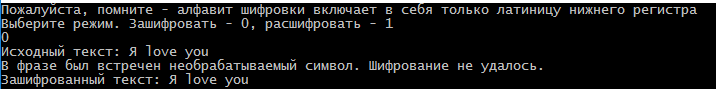


Рисунок 8 – Зашифровка фразы “Я love you”

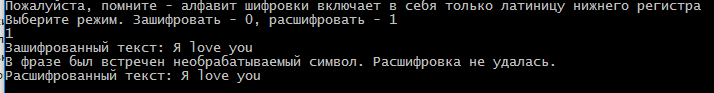


Рисунок 9 – Расшифровка фразы “Я love you”

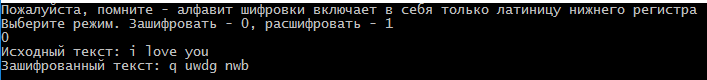


Рисунок 10 – Зашифровка фразы “I love you”

ЗАКЛЮЧЕНИЕ

В процессе выполнения данной лабораторной работы я познакомился с различными способами шифрования, а также научился их использовать для составления программ шифраторов-дешифраторов. Особое внимание было уделено методу шифрования Трисемуса.