Федеральное агентство связи

Федеральное государственное бюджетное образовательное учреждение высшего образования

«Сибирский государственный университет телекоммуникаций и информатики»

(СибГУТИ)

**Расчетно-графическая работа**

**по дисциплине**

**«Программирования»**

**Тема: «Шифрование текста шифром Виженера на языке C»**

Выполнил:

студент группы: ИА-331

Кулаков Кирилл Алексеевич

Проверил преподователь:

Лебеденко Людмила Федоровна

Новосибирск 2024

Задание

Шифрование текста шифром Виженера.

Разработать программу Vigenera, выполняющую шифрование в заданном тексте и DeVigenera – дешифровку текста. Текст до шифрования, после шифрования и после дешифровки должен выводиться на экран.

Критерии оценки «удовлетворительно»: реализована проверка того, что исходный текст и полученные после дешифровки совпадают. Не предусмотрено динамическое выделение памяти под входные данные. Функции записаны в статическую библиотеку.

Оценка «хорошо»: на вход программы подается 2 файла. Первый файл содержит текст на русском языке. Второй файл будет содержать зашифрованный текст. Обязательно динамическое выделение памяти под входные данные. Функции записаны в статическую библиотеку.

Оценка «отлично»: оценить криптостойкость шифра. Обязательно динамическое выделение памяти под входные данные. Функции записаны в динамическую библиотеку.

Анализ задачи

Для решения задачи, нам нужно посчитать нужное количество символов для кодирования. Чтобы закодировать сообщение, состоящее из русских и английских букв, можно ограничиться набором из 66 символов для русских букв в нижнем и верхнем регистре, 52 символов для латинских букв, 10 символов для арабских цифр и 1 символа для пробела. В итоге получается 129-символьный набор. Каждый такой символ будет занимать 8 бит или 1 байт. Но в таком случае возникает проблема со знаками, такими как запятые, точки, тире. Для устранения данной проблемы, стоит ограничить набор до 256 символов. Этот способ также усложнит ручное дешифрование, так как помимо обычных читаемых человеком символов, добавятся иные символы. В итоге общий алгоритм шифрования и дешифрования показан на рисунках 1 и 2.



Рисунок 1 – Шифрование текста

В алгоритме шифрования переменные lengthMessage и lengthKey отвечают за хранение длин кодируемого сообщения и ключа соответственно, переменные i и k за счетчики цикла по сообщению и ключу соответственно, переменная result за итоговую зашифрованную строку символов.

В итоговую строку записывается сумма кодов символа сообщения и соответствующего ему символа ключа, который подбирается остатком от деления от его длины. Для ограничения по набору символов выбран стандартный размер 256 символов, что соответствует пределу диапазона значений одного символа char.



Рисунок 2 – Дешифрование текста

Алгоритм дешифрования происходит аналогично шифрованию, за исключением того, что в итоговую строку записывается разность кодов символа сообщения и соответствующего ему символа ключа.

Тестовые данные

В качестве тестовых данных были выбраны несколько строк на русском и английском языках, в верхнем и нижнем регистре, с цифрами и другими символами, и без них. Некорректных данных быть не может, так как все символы исходного и кодируемого текста лежат в диапазоне 256.

Листинг программы

vigenera.h

#pragma once

#include <stdlib.h>

#include <string.h>

// Функция для шифрования текста с ключом методом Вижинера

char\* crypt(const char\* message, const char\* key);

// Функция для дешифрования текста с ключом методом Вижинера

char\* decrypt(const char\* message, const char\* key);

vigenera.c

#include "vigenera.h"

char\* crypt(const char\* message, const char\* key)

{

size\_t lengthMessage = strlen(message);

size\_t lengthKey = strlen(key);

char\* result = malloc(sizeof(char) \* (lengthMessage + 1));

result[lengthMessage] = '\0';

for (size\_t i = 0, k = 0; i < lengthMessage; i++, k++)

result[i] = message[i] + key[k % lengthKey] % 256;

return result;

}

char\* decrypt(const char\* message, const char\* key)

{

size\_t lengthMessage = strlen(message);

size\_t lengthKey = strlen(key);

char\* result = malloc(sizeof(char) \* (lengthMessage + 1));

result[lengthMessage] = '\0';

for (size\_t i = 0, k = 0; i < lengthMessage; i++, k++)

result[i] = message[i] - key[k % lengthKey] % 256;

return result;

}

main.c

#define \_CRT\_SECURE\_NO\_WARNINGS

// Макрос максимальной длинны текста при его считывании из файла

#define SIZE\_FILE 1024 \* 128

#include <stdio.h>

#include <stdlib.h>

#include "vigenera.h"

// Функция для считывания текста из файла. Возвращает нулевой указатель в случае ошибки

char\* readFromFile(const char\* filename);

// Функция для записи текста в файл. Возвращает нулевой указатель в случае ошибки

char\* writeToFile(const char\* filename, const char\* message);

// Главная функция

int main()

{

// Включение русской кодировки в консоли

system("chcp 1251");

// Имя входного файла

char filenameIn[256];

// Имя выходного файла

char filenameOut[256];

// Текст до шифрования

char\* message = 0;

// Текст после шифрования

char\* result = 0;

// Ключ

char key[256];

printf("Введите название файла, с которого взять текст: ");

scanf("%s", filenameIn);

// Считывание текста из файла

message = readFromFile(filenameIn);

if (message == 0)

{

printf("Ошибка считывания текста из файла!\n");

system("pause");

return -1;

}

printf("Введите название файла, в который нужно записать результат операции: ");

scanf("%s", filenameOut);

printf("Введите ключ: ");

scanf("%s", key);

int operation = 0;

printf("Выберите операцию: \n");

printf("0. Выход\n");

printf("1. Зашифровать текст\n");

printf("2. Расшифровать текст\n");

scanf("%d", &operation);

// Выбор операции

switch (operation)

{

case 0:

// Очистка занятой памяти перед выходом

free(message);

return 0;

case 1:

// Шифрование считанного текста

result = crypt(message, key);

break;

case 2:

// Дешифрование считанного текста

result = decrypt(message, key);

break;

default:

printf("Была выбрана некорректная операция");

system("pause");

break;

}

// Если запись результатов была с ошибкой

if (writeToFile(filenameOut, result) == 0)

{

printf("Ошибка записи результата в файл!");

system("pause");

return -1;

}

// Очистка занятой памяти

free(message);

free(result);

system("pause");

return 0;

}

char\* readFromFile(const char\* filename)

{

// Открываем файл для чтения

FILE\* file = fopen(filename, "r");

// Проверяем успешность открытия файла

if (file == NULL)

return 0;

// Выделяем память для буфера данных

char\* result = malloc(sizeof(char) \* SIZE\_FILE);

// Читаем данные из файла в буфер

while (fgets(result, SIZE\_FILE, file) != NULL);

// Закрываем файл

fclose(file);

return result;

}

char\* writeToFile(const char\* filename, const char\* message)

{

// Открываем файл для записи

FILE\* file = fopen(filename, "w");

// Проверяем успешность открытия файла

if (file == NULL)

{

printf("Ошибка открытия файла\n");

return 0;

}

// Записываем сообщение в файл

fprintf(file, "%s", message);

// Закрываем файл

fclose(file);

return message;

}

Скрины с результатами



Рисунок 3 – Исходные данные



Рисунок 4 – Шифрование исходных данных



Рисунок 5 – Дешифрование шифрованных данных

Заключение

В программе явно отделены функции readFromFile и writeInFile от статической библиотеки vigenera.h, так как они выполняют независимые друг от друга задачи.

По непонятным причинам, в расшифрованном файле появились символы, которых не было в сообщении изначально. Это явно не связано с алгоритмом шифрования, так как он просто заменяет одни символы на другие без добавление новых.

По непонятным причинам, в алгоритме считывания данных из файла, функция ftell возвращает неверный размер файла, из-за чего при каждом считывании возможно добавление новых символов. Это никак не препятствует кодированию и декодированию текста.

Список литературы

1. Царев, Р.Ю. Программирование на языке Си [Текст]: учеб. пособ. / Царев, Р.Ю. 2019. - 108 с.

2. Шифрование методом Виженера [Электронный ресурс]. – Режим доступа: [https://ru.wikipedia.org/wiki/Шифр\_ HYPERLINK "https://ru.wikipedia.org/wiki/Шифр\_Виженера"В HYPERLINK "https://ru.wikipedia.org/wiki/Шифр\_Виженера"иженера](https://ru.wikipedia.org/wiki/Шифр_Виженера)