Федеральное агентство по образованию

Пензенский государственный университет

Кафедра «Информационной безопасности систем и технологий»

ПОЯСНИТЕЛЬНАЯ ЗАПИСКА

к курсовому проекту на тему

“ Программная реализация криптографического алгоритма шифрования с использованием открытого текста в качестве ключа ”

ПГУ 3.090105.001 ПЗ

Дисциплина: КМЗИ

Группа:

Разработал студент:

Работа принята с оценкой:

Руководитель проекта:

Пенза 2006г.

**Реферат**

Пояснительная записка содержит 24 страниц, 4 источника, 4 приложения.

ТАБЛИЦА ВИЖЕНЕРА, АЛФАВИТ, ОТКРЫТЫЙ ТЕКСТ, ШИФРОТЕКСТ, ШИФРОВАНИЕ, РАСШИФРОВАНИЕ.

Объектом исследования является шифр по таблице Виженера.

Целью работы является реализация криптографического алгоритма шифрования с использованием открытого текста в качестве ключа по таблице Виженера.

В процессе работы был рассмотрен шифр замены и разработана программа, реализующая данный шифр.

В результате работы был реализован криптографический алгоритм ручного шифра по таблице Виженера, осуществляющий шифрование.

**Содержание**

Реферат

Задание

Введение

1 Разработка алгоритма программы ручного шифра по таблице Виженера

1.1 Функция шифрования

1.2 Функция расшифрования

2 Разработка программы, выполняющей шифрование и расшифрование по таблице Виженера

3 Экспериментальная проверка работы программы

Заключение

Список использованных источников

Приложение А. Обязательное. Алгоритм программы шифрования и расшифрования

Приложение Б. Обязательное. Алгоритм функции шифрования

Приложение В. Обязательное. Алгоритм функции расшифрования

Приложение Г. Обязательное. Листинг программы шифрования и расшифрования

**Введение**

В настоящее время широкое распространение получили персональные компьютеры. Они, без преувеличения, вошли во все сферы человеческой деятельности. Это максимально облегчило человеческий труд. Сейчас трудно представить, чтобы делал человек без компьютера. Предприятия, фирмы, офисы, банки - это ещё далеко не все области применения персонального компьютера.

Без использования криптографии сегодня немыслимо решение задач по обеспечению безопасности информации, связанных с конфиденциальностью и целостностью. Если до 1990г. криптография обеспечивала закрытие государственных линий связи, то в наши дни использование криптографических методов получило широкое распространение благодаря развитию компьютерных сетей и электронного обмена данными в различных областях[2].

Владение языками программирования позволяет значительно расширить круг выполняемых задач специалистом по защите информации и более полно использовать возможности компьютера.

Данная курсовая работа написана на языке С.

Разработанная программа обладает интерактивным интерфейсом. Методы и средства взаимодействия с аппаратными и программными средствами называют пользовательским интерфейсом [4].

С – это универсальный язык программирования с компактным способом записи выражений, современными механизмами управления структурами данных и богатым набором операторов[1].

Целью курсовой работы является реализация криптографического алгоритма шифрования с использованием открытого текста в качестве ключа по таблице Виженера.

Многие недостатки и неудобства схем шифрованной связи с традиционным применением ключей удаётся преодолеть, используя идею так называемого «открытого» ключа. Принципиальная основа этой идеи состоит в использовании свойства некоторых математических операций, имеющих разную сложность выполнения в «прямом» и «обратном» направлениях. На основе этого свойства можно разработать такую систему шифрования, для которой процесс зашифрования выполняется с помощью «открытого» («общедоступного») ключа, а процесс расшифрования выполняется с помощью секретного ключа, который имеется только у адресата. Определение секретного ключа на основе знания «открытого» ключа - то есть решить для ключа «обратную» задачу представляет весьма сложную проблему, что и определяет стойкость шифросистемы.

Разумеется, «сложность» выполнения математической операции зависит от применяемого алгоритма и, в конечном счёте, сводится к оценке числа так называемых «элементарных» операций, составляющих алгоритм вычисления. Если иметь в виду, что алгоритм математической операции реализуется на ЭВМ, то при данных параметрах ЭВМ (скорость вычисления, объём долговременной и оперативной памяти) «сложность» математической операции может быть оценена временем её выполнения на ЭВМ. Существует тривиальные алгоритмы, основанные на последовательном переборе всех возможных вариантов решения и выделении среди них истинного варианта. Однако такой «силовой» метод требует больших временных затрат и на практике невыполним, если параметры задачи ( в примерах – это величена чисел, разлагаемого на простые множители; свойство многочлена и величина степени, в которую он возводится) достаточно велики.

Поиск и разработка эффективных алгоритмов для выполнения некоторых математических операций или доказательство невозможности их построения представляют сложную математическую проблему, над решением которой упорно работают математики всего мира. В последние годы получены некоторые успехи в этой области, что, конечно, заставило переоценить стойкость некоторых шифросистем, построенных на основе применения «открытого» ключа. Однако существуют проблемы, где продвижения в поисках эффективных алгоритмов оказались недостаточными для их практической реализации или требуют чрезвычайно больших материальных и временных затрат. ТО, что над этими проблемами работают самые квалифицированные математики всего мира, пытаясь улучшить алгоритмы решения «обратных» задач, даёт основание полагать, что на определённый период времени такого рода «сложные» математические операции могут обеспечивать криптографическую стойкость шифросистем, построенных с их использованием. Именно к таким проблемам относится « дискретное логарифмирование»[3].

**1. Разработка алгоритма программы ручного шифра по таблице Виженера**

Алгоритм программы шифрования и расшифрования приведен в приложении А.

Программа должна реализовывать алгоритм шифрования и расшифрования по квадрату Виженера.

**1.1 Функция шифрования**

Алгоритм функции шифрования приведен в приложении Б.

Виженер высказывает идею использования в качестве ключа самого открытого текста. При шифровании применяется таблица Тритемия, слегка модифицированную Виженером (см. таблицу 1). Заранее оговаривается одна ключевая буква алфавита, обозначим ее через *t*0. Она используется как ключ при шифровании первой буквы текста *t*1. Последовательность букв открытого текста *t*1 *t*2 … подписывается под ключевой последовательностью *t*0 *t*1 *t*2 …:



Пара букв, стоящих друг под другом в ключевой последовательности и в открытом тексте, указывает, соответственно, номера строк *ti*–1 и столбцов *ti* таблицы Тритемия, на пересечении которых находится буква *si* шифрованного текста.

**1.2 Функция расшифрования**

Алгоритм функции расшифрования приведён в приложении В.

При расшифровании открытый текст, являющийся частью ключевой последовательности, нам изначально неизвестен. Но если расшифровывающий знает букву ключа *t*0, он может расшифровать первую букву шифрованного текста *s*1: для этого находим в строке таблицы Виженера (см. таблицу 1) с номером *t*0 букву *s*1, *t*1 есть номер столбца, в котором она находится (буква того же столбца в первой строке). Вписываем эту букву над *s*2 и расшифровываем вторую букву. И т.д.



Таблица 1. Таблица Виженера

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

**2. Разработка программы, выполняющей шифрование и расшифрование по таблице Виженера**

Текст программы шифрования и расшифрования приведен в приложении Г.

Данная программа написана с использованием языка программирования С.

В главной функции объявляется таблица Виженера при помощи двумерного массива alfavit[27][27].

В этой функции осуществляется вызов функции шифрования.

Для вывода сообщений на экран используются функции printf() и puts(). А для ввода данных используются функции scanf() и cin().

Для организации циклов в этих функциях используются операторы с предусловием while и с параметрическим циклом for.

**3. Экспериментальная проверка работы программы**

Для проверки работы программы, выполняющей шифрование по таблице Виженера возьмем, например слово «welcome», а ключевым символом будет являться, например символ «a».

После шифрования был получен следующий шифротекст:«wapnqaq»

Для проверки работы программы расшифрования по таблице Виженера возьмём этот же шифротекст «wapnqaq» при этом ключевым символом должен являться символ «a». При расшифровки получим первоначальный текст «welcome».

**Заключение**

В результате выполнения курсового проекта была разработана программа, реализующая криптографический алгоритм шифрования и расшифрования с использованием открытого текста в качестве ключа по таблице Виженера. Разработанная программа написана на языке Си.

Также была выполнена экспериментальная проверка работы данной программы, подтверждающая правильность шифрования.

В завершении работы была оформлена пояснительная записка, содержащая описание разработки программы, осуществляющей по таблице Виженера.

Таким образом, задание на курсовую работу выполнено в полном объеме.

**Список использованных источников**

1. Керниган Б., Ритчи Д. Язык программирования Си.\Пер. с англ., 3-е изд., испр – СПб.: «Невский Диалект», 2001. – 352с.:ил.

2. Алферов А.П., Зубов А.Ю., Кузьмин А.С., Черемушкин А.В. Основы криптографии: Учебное пособие. – М.: Гелиос АРВ, 2001. – 480 с.

3. Основы криптологии. Шифры замены. Методические указания к практическим занятиям по дисциплине «Основы криптологии». / Составители М.М. Грунтович, С.М. Геращенко – Пенза: Пензен. госуд. ун‑т, 2005.

4. Информатика: Базовый курс \ С.В. Симонович и др. – СПб,: Питер,2001. – 640 с.

**ПРИЛОЖЕНИЕ А**

Алгоритм программы шифрования и расшифрования

конец

шифрование или расшифрование

начало

**ПРИЛОЖЕНИЕ Б**

Алгоритм функции шифрования

начало

формирование ключевой последовательности

считывание открытого текста и ключевого символа

поиск символов открытого текста а табл. Виженера.

поиск символов ключевой последовательности табл. Виженера.

Нахождение пересечений символов открытого текста и текста ключевой последовательности и вывод на экран зашифрованного теста

конец

**ПРИЛОЖЕНИЕ В**

Алгоритм функции расшифрования

начало

по ключевому символу находится первый символ открытого текста

формирование ключевой последовательности

считывание зашифрованного текста и ключевого символа

по первому символу открытого текста находится следующий символ открытого текста следующего символа зашифрованного текста

вывод открытого текста на экран

конец

**ПРИЛОЖЕНИЕ Г**

Листинг программы шифрования и расшифрования

#include <stdio.h>

#include <string.h>

#include <iostream.h>

#include <stdlib.h>

void main()

{int b;

int f;

int z2;

int z1;

int y;

int y1;

char x1[20]={0};

char x2;

char x3[20]={0};

char x5[20]={0};

char filename[40];

FILE\*text;

int r=0;

char c;

int i;

int i1;

int j;

int j1;

char t1[20]={0};

char t2;

char t5[20];

static char alfavit[27][27]={

{' ','a','b','c','d','e','f','g','h','i','j','k','l','m','n','o','p','q','r','s','t','u','v','w','x','y','z'},

{'a','a','b','c','d','e','f','g','h','i','j','k','l','m','n','o','p','q','r','s','t','u','v','w','x','y','z'},

{'b','b','c','d','e','f','g','h','i','j','k','l','m','n','o','p','q','r','s','t','u','v','w','x','y','z','a'},

{'c','c','d','e','f','g','h','i','j','k','l','m','n','o','p','q','r','s','t','u','v','w','x','y','z','a','b'},

{'d','d','e','f','g','h','i','j','k','l','m','n','o','p','q','r','s','t','u','v','w','x','y','z','a','b','c'},

{'e','e','f','g','h','i','j','k','l','m','n','o','p','q','r','s','t','u','v','w','x','y','z','a','b','c','d'},

{'f','f','g','h','i','j','k','l','m','n','o','p','q','r','s','t','u','v','w','x','y','z','a','b','c','d','e'},

{'g','g','h','i','j','k','l','m','n','o','p','q','r','s','t','u','v','w','x','y','z','a','b','c','d','e','f'},

{'h','h','i','j','k','l','m','n','o','p','q','r','s','t','u','v','w','x','y','z','a','b','c','d','e','f','g'},

{'i','i','j','k','l','m','n','o','p','q','r','s','t','u','v','w','x','y','z','a','b','c','d','e','f','g','h'},

{'j','j','k','l','m','n','o','p','q','r','s','t','u','v','w','x','y','z','a','b','c','d','e','f','g','h','i'},

{'k','k','l','m','n','o','p','q','r','s','t','u','v','w','x','y','z','a','b','c','d','e','f','g','h','i','j'},

{'l','l','m','n','o','p','q','r','s','t','u','v','w','x','y','z','a','b','c','d','e','f','g','h','i','j','k'},

{'m','m','n','o','p','q','r','s','t','u','v','w','x','y','z','a','b','c','d','e','f','g','h','i','j','k','l'},

{'n','n','o','p','q','r','s','t','u','v','w','x','y','z','a','b','c','d','e','f','g','h','i','j','k','l','m'},

{'o','o','p','q','r','s','t','u','v','w','x','y','z','a','b','c','d','e','f','g','h','i','j','k','l','m','n'},

{'p','p','q','r','s','t','u','v','w','x','y','z','a','b','c','d','e','f','g','h','i','j','k','l','m','n','o'},

{'q','q','r','s','t','u','v','w','x','y','z','a','b','c','d','e','f','g','h','i','j','k','l','m','n','o','p'},

{'r','r','s','t','u','v','w','x','y','z','a','b','c','d','e','f','g','h','i','j','k','l','m','n','o','p','q'},

{'s','s','t','u','v','w','x','y','z','a','b','c','d','e','f','g','h','i','j','k','l','m','n','o','p','q','r'},

{'t','t','u','v','w','x','y','z','a','b','c','d','e','f','g','h','i','j','k','l','m','n','o','p','q','r','s'},

{'u','u','v','w','x','y','z','a','b','c','d','e','f','g','h','i','j','k','l','m','n','o','p','q','r','s','t'},

{'v','v','w','x','y','z','a','b','c','d','e','f','g','h','i','j','k','l','m','n','o','p','q','r','s','t','u'},

{'w','w','x','y','z','a','b','c','d','e','f','g','h','i','j','k','l','m','n','o','p','q','r','s','t','u','v'},

{'x','x','y','z','a','b','c','d','e','f','g','h','i','j','k','l','m','n','o','p','q','r','s','t','u','v','w'},

{'y','y','z','a','b','c','d','e','f','g','h','i','j','k','l','m','n','o','p','q','r','s','t','u','v','w','x'},

{'z','z','a','b','c','d','e','f','g','h','i','j','k','l','m','n','o','p','q','r','s','t','u','v','w','x','y'},};

while (1)

{printf("\nVvedite 1 dlya shifrovaniya \nVvedite 2 dlya rasshifrovaniya\nVvedite 3 dlya vihoda\n");

scanf("%d",&b);

switch (b)

{case 1: printf("%d - shifrovaniye\n",b);

printf("\nVibor regima:\n1 from klava\n2 from file\n");

scanf("%d",&f);

switch(f)

{case 1: printf("Vvedite slovo\n");

cin>>x1;

printf("\nVvedite kluchevoy simvol\n");

cin>>x2;

for ( z2=strlen(x1)-1;z2>0;z2--)

{x3[z2]=x1[z2-1];}

x3[0]=x2;

x3[strlen(x1)]='\0';

printf("\nSlovo dlya shifrovaniya: %s\n",x1);

printf("\nKluchevoy simvol: %c\n",x2);

printf("\nKluchevaiya posledovatel'nost': %s\n",x3);

int z3;

for (z3=0;z3<20;z3++)

{z1 = y1 = 0;

if((x1[z3] !='\0')||(x3[z3] !='\0'))

{for (z2=0;z2<27;z2++)

if (alfavit[0][z2]==x1[z3])

{z1=z2;

break;}

for (y=0;y<27;y++)

if (alfavit[y][0]==x3[z3])

{y1=y;

break;}

x5[z3]=alfavit[y1][z1];}

else

break;}

x5[z3] = '\0';

printf("\nShifrotekst: %s\n",x5);

break;

case 2: puts("Put name of file with open text:\n");

scanf("%s",&filename);

text=fopen(filename,"r");

while(!(feof(text)))

{c=getc(text);

r++;}

fseek(text,0,0);

i=0;

while(r!=1)

{c=getc(text);

x1[i]=c;

r--;

i++;}

printf("\nVvedite kluchevoy simvol\n");

cin>>x2;

for ( z2=strlen(x1)-1;z2>0;z2--)

{x3[z2]=x1[z2-1];}

x3[0]=x2;

x3[strlen(x1)]='\0';

printf("\nSlovo dlya shifrovaniya: %s\n",x1);

printf("\nKluchevoy simvol: %c\n",x2);

printf("\nKluchevaiya posledovatel'nost': %s\n",x3);

for (z3=0;z3<20;z3++)

{z1 = y1 = 0;

if((x1[z3] !='\0')||(x3[z3] !='\0'))

{for (z2=0;z2<27;z2++)

if (alfavit[0][z2]==x1[z3])

{z1=z2;

break;}

for (y=0;y<27;y++)

if (alfavit[y][0]==x3[z3])

{y1=y;

break;}

x5[z3]=alfavit[y1][z1];}

else

break;}

x5[z3] = '\0';

printf("\nShifrotekst: %s\n",x5);

fclose(text);

break;

default: return;}

break;

case 2: printf("%d - rasshifrovaniye\n",b);

printf("\nVibor regima:\n1 from klava\n2 from file\n");

scanf("%d",&f);

switch(f)

{case 1: printf("\nVvedite shifrotekst:\n");

cin>>t1;

printf("\nVvedite kluchevoy simvol:\n");

cin>>t2;

printf("\nShifrotekst: %s\n",t1);

printf("\nKluchevoy simvol: %c\n", t2);

int i2;

for (i2=0;t1[i2];i2++)

{i1 = j1 = 0;

{for (i=0;i<32;i++)

if (alfavit[i][0]==t2)

{i1=i;

break;}

for (j=0;j<34;j++)

if (alfavit[i1][j]==t1[i2])

{j1=j;

break;}

t5[i2]=alfavit[0][j1];}

t2=t5[i2];}

t5[i2] = '\0';

printf("\nOtkritiy tekst: %s\n",t5);

break;

case 2: puts("Put name of file with open text:\n");

scanf("%s",&filename);

text=fopen(filename,"r");

while(!(feof(text)))

{c=getc(text);

r++;}

fseek(text,0,0);

i=0;

while(r!=1)

{c=getc(text);

t1[i]=c;

r--;

i++;}

printf("\nVvedite kluchevoy simvol:\n");

cin>>t2;

printf("\nShifrotekst: %s\n",t1);

printf("\nKluchevoy simvol: %c\n", t2);

for (i2=0;t1[i2];i2++)

{i1 = j1 = 0;

{for (i=0;i<32;i++)

if (alfavit[i][0]==t2)

{i1=i;

break;}

for (j=0;j<34;j++)

if (alfavit[i1][j]==t1[i2])

{j1=j;

break;}

t5[i2]=alfavit[0][j1];}

t2=t5[i2];}

t5[i2] = '\0';

printf("\nOtkritiy tekst: %s\n",t5);

fclose(text);}

break;

case 3: return;

default: printf("%d - tolko 1 ili 2!!!\n",b);

return;}}}