СОДЕРЖАНИЕ

ВВЕДЕНИЕ....3
1. ТЕОРЕТИЧЕСКАЯ ЧАСТЬ....4
1.1 Математическое обоснование алгоритма работы шифра Гронсфельда....4
1.2 Алгоритм работы шифра с помощью квадрата Полибия....4
1.3 Алгоритм работы шифра Атбаша....4
1.4 Алгоритм работы шифра Вижинера....4
1.5 Алгоритм работы шифра “Тарабарская грамота”....4
2. ПРАКТИЧЕСКАЯ ЧАСТЬ....5
2.1. Постановка задачи....5
2.2. Характеристика задачи....6
2.3 Алгоритм решения задачи....7
2.5 Руководство системного программиста....11
2.6 Контрольный пример....12
3. ЗАКЛЮЧЕНИЕ....13
4. ПРИЛОЖЕНИЕ А....14

ВВЕДЕНИЕ

Актуальность Актуальность

Целью работы является разработка криптографического программного обеспечения «Шифровка и дешифровка текста».

Для реализации поставленной цели необходимо решить ряд задач:

- изучить методику …
- проанализировать…

(Все задачи отвечают на вопрос Что сделать? Не использовать слова рассмотреть).

Теоретическая база исследования (перечислить учебники или статьи (авторов)).

Программа реализована на … (технологии разработки).

1. ТЕОРЕТИЧЕСКАЯ ЧАСТЬ

В программе используется 5 методов шифрования: Гроснфельда, с помощью квадрата Полибия, Атбаша, Вижинераи “Тарабарская грамота”. Шифр Гронсфельда и Вижинера реализуются с помощью ключей.

1.1 Математическое обоснование алгоритма работы шифра Гронсфельда

1.2 Алгоритм работы шифра с помощью квадрата Полибия

1.3 Алгоритм работы шифра Атбаша

1.4 Алгоритм работы шифра Вижинера

1.5 Алгоритм работы шифра “Тарабарская грамота”

2. ПРАКТИЧЕСКАЯ ЧАСТЬ

2.1. Постановка задачи

Необходимо разработать программу, которая должна шифровать и дешифровать текст одним из представленных алгоритмов. Программа должна выполнять следующие основные действия:

- перед началом работы пользователь вводит пароль;
- ввод исходного текста;
- шифровка, то есть кодировка, текста и вывод её на экран; в некоторых алгоритмах шифровка происходит при использовании ключа, который пользователь вводит непосредственно перед процессом шифрования;
- дешифровка текста,а также выводимый на экран по запросу пользователя расшифрованный текст;

Методы шифрования реализовать в виде отдельных функций.

2.2. Характеристика задачи

1. Программа предназначена для автоматизации процесса шифрования текста и защиты паролем от использования алгоритмов сторонними лицами.
2. Программа используется пользователем для защиты персональной информации.
3. Решения задач производятся по запросу пользователя.
4. Связь с другими задачами отсутствует.
5. Специальных ограничений на временные характеристики решения задачи не налагается.
6. Специальных требований на уровень подготовки пользователя не налагаются. Но лицо, работающее с программой, должно иметь минимальное представление о компьютере (знание необходимых операций).

2.3 Алгоритм решения задачи

1. Запустить приложения
2. Вывод меню: "Пароль: "
3. Ввод пароля
4. Вывод меню: " Выберите шифр: "
   " Нажмите <1> для выбора шифра Гронсфельда"
   " Нажмите <2> для выбора шифра с помощью квадрата Полибия"
   " Нажмите <3> для выбора шифра Атбаша"
   " Нажмите <4> для выбора шифра Вижинера"
   " Нажмите <5> для выбора шифра 'Тарабарская грамота'"

4.1. Если выбран пункт – " Нажмите <1> для выбора шифра Гронсфельда"

4.1.1. Вывод подменю: " Введите сообщение: "

4.1.2. Ввод сообщения

4.1.3. Вывод подменю: " Введите ключ: "

4.1.4. Ввод ключа под данный шифр

4.1.5. Шифрование текста выбранным способом

4.1.6. Вывод зашифрованного сообщения

4.1.7. Дешифровка текста

4.1.8. Вывод на экран дешифрованного сообщения

4.1.9. Вывод подменю: " Нажмите Enter для выбора другого шифра"

4.1.10. Выбор другого алгоритма шифрования

4.2. Если выбран пункт – " Нажмите <2> для выбора шифра с помощью квадрата Полибия"

4.2.1. Вывод подменю: " Введите сообщение: "

4.2.2. Ввод сообщения

4.2.3. Шифрование текста выбранным способом

4.2.4. Вывод зашифрованного сообщения

4.2.5. Дешифровка текста

4.2.6. Вывод на экран дешифрованного сообщения

4.2.7. Вывод подменю: " Нажмите Enter для выбора другого шифра"

4.2.8. Выбор другого алгоритма шифрования

4.3. Если выбран пункт – " Нажмите <3> для выбора шифра Атбаша"

4.3.1. Вывод подменю: " Введите сообщение: "

4.3.2. Ввод сообщения

4.3.3. Шифрование текста выбранным способом

4.3.4. Вывод зашифрованного сообщения

4.3.5. Дешифровка текста

4.3.6. Вывод на экран дешифрованного сообщения

4.3.7. Вывод подменю: " Нажмите Enter для выбора другого шифра"

4.3.8. Выбор другого алгоритма шифрования

4.4. Если выбран пункт – " Нажмите <4> для выбора шифра Вижинера"

4.4.1. Вывод подменю: " Введите сообщение: "

4.4.2. Ввод сообщения

4.4.3. Вывод подменю: " Введите ключ: "

4.4.4. Ввод ключа под данный шифр

4.4.5. Шифрование текста выбранным способом

4.4.6. Вывод зашифрованного сообщения

4.4.7. Дешифровка текста

4.4.8. Вывод на экран дешифрованного сообщения

4.4.9. Вывод подменю: " Нажмите Enter для выбора другого шифра"

4.4.10. Выбор другого алгоритма шифрования

4.5. Если выбран пункт – " Нажмите <5> для выбора шифра 'Тарабарская грамота'"

4.5.1. Вывод подменю: " Введите сообщение: "

4.5.2. Ввод сообщения

4.5.3. Шифрование текста выбранным способом

4.5.4. Вывод зашифрованного сообщения

4.5.5. Дешифровка текста

4.5.6. Вывод на экран дешифрованного сообщения

4.5.7. Вывод подменю: " Нажмите Enter для выбора другого шифра"

4.5.8. Выбор другого алгоритма шифрования

2.4 Руководство пользователя

Для начала работы с программой первостепенно необходимо ввести правильный пароль (в данном случае «6230») (Рисунок 2.1).

Рисунок 2.1 – Запрос и ввод пароля

Далее программа предлагает пользователю на выбор 1 из 5 алгоритмов шифрования. Для выбора необходимого вводится соответствующий ему номер (Рисунок 2.2)

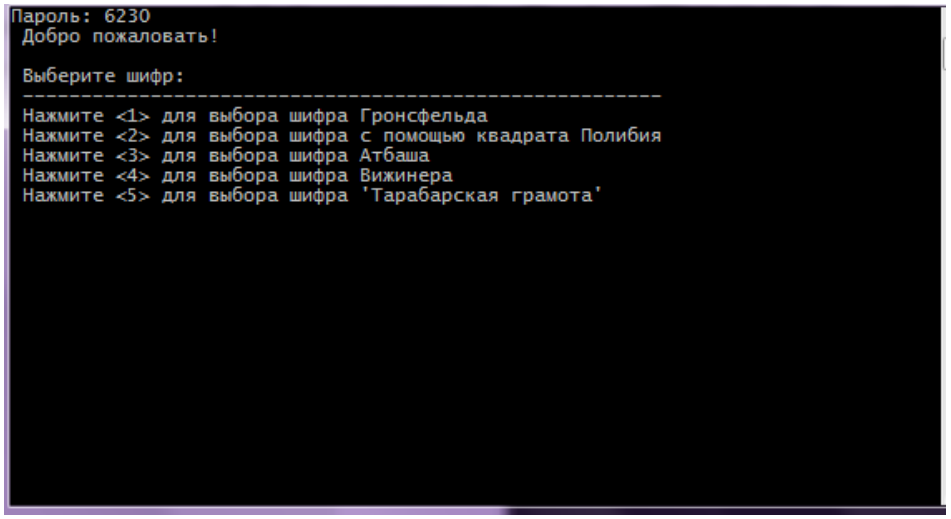

Рисунок 2.2 – Вывод меню и выбор пункта

фрагмент пропущен

2.5 Руководство системного программиста

Данная программа предназначена для шифрования и дешифрования текстового сообщения. Проект написан на языке C++ в средеCodeBlocks.

Программа состоит из трех основных модулей:

1. Заголовочный файл Header.h

Содержит объявления всех функций, использованных в данной программе.

2. Файл Source.cpp

Содержит определение функций, объявленных в заголовочном файле Header.h:

void gronsfeld(charmessage[], charkey[]); - шифрование текста алгоритмом Гронсфельда, входные данные: текст сообщения и ключ, выходные: зашифрованный и дешифрованный текст сообщения.

3. фрагмент пропущен

4. Файл main.cpp

Содержит функцию main, представляющую ввод пароля, вывод меню выбора шифров, с соответствующим вызовом функций, и вводом необходимых данных.

Программа содержит ряд сообщений, предназначенных для сигнализации ошибок:

1. «Неверный пароль» – ошибка при введении неверного пароля; программа не выдаст меню выбора алгоритмов шифрования.
2. "Повторите попытку!!!" – ошибка при вводе пункта меню; программа предложит ввести другой (существующий) номер.

2.6 Контрольный пример

Запуск программы, вводится пароль (Рисунок 2.4)

Рисунок 2.4 – Запрос и ввод пароля

фрагмент пропущен

3. ЗАКЛЮЧЕНИЕ

Текст заключения Текст заключения

4. ПРИЛОЖЕНИЕ А

Листинг программы