Министерство образования Республики Беларусь

Учреждение образования

БЕЛОРУССКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ ИНФОРМАТИКИ И РАДИОЭЛЕКТРОНИКИ

Факультет компьютерных систем и сетей

Кафедра электронных вычислительных машин

Дисциплина: Системное программное обеспечение вычислительных машин (СПОВМ)

ПОЯСНИТЕЛЬНАЯ ЗАПИСКА

к курсовому проекту

на тему:

«Защищённый диск»

Студент: гр.350501 Милько А. В.

Руководитель: Яночкин А.Л.

Минск 2015

Содержание

[ВВЕДЕНИЕ 6](#_Toc419663749)

[2. ОБЗОР ЛИТЕРАТУРЫ 7](#_Toc419663750)

[2.2. Шифрование/дешифрование 7](#_Toc419663751)

[2.1.1. RSA 7](#_Toc419663752)

[2.1.2 Имитовставка 8](#_Toc419663753)

[3. ФУНКЦИОНАЛЬНОЕ ПРОЕКТИРОВАНИЕ 8](#_Toc419663754)

[3.1. Создание хранилища 9](#_Toc419663755)

[3.2 Шифрование и дешифрование хранилища 9](#_Toc419663756)

[СПИСОК ЛИТЕРАТУРЫ 9](#_Toc419663757)

**ТЕХНИЧЕСКОЕ ЗАДАНИЕ**

Разработать систему для хранения информации в зашифрованном виде с использованием алгоритма шифрования с открытым ключом RSA. Данная программа предполагает создание и использование защищенного хранилища.

**Требования к программе или программному изделию.**

* Язык программирования – C++.
* Работа на операционной системе семейства Windows.
* Для шифрования данных использовать защищенное хранилище файлов.
* Алгоритм шифрования RSA.
* Графический пользовательский интерфейс для создания и доступа к защищенному хранилищу.

# ВВЕДЕНИЕ

Прогресс подарил человечеству великое множество достижений, но тот же прогресс породил и массу проблем. Человеческий разум, разрешая одни проблемы, непременно сталкивается при этом с другими, новыми, и этот процесс обречен на бесконечность в своей последовательности. Вечная проблема - защита информации. На различных этапах своего развития человечество решало эту проблему с присущей для данной эпохи характерностью. Изобретение компьютера и дальнейшее бурное развитие информационных технологий во второй половине 20 века сделали проблему защиты информации настолько актуальной и острой, насколько актуальна сегодня информатизация для всего общества.

Сегодня, наверное, никто не сможет с уверенностью назвать точную цифру суммарных потерь от компьютерных преступлений, связанных с несанкционированных доступом к информации. Это объясняется, прежде всего, нежеланием пострадавших компаний обнародовать информацию о своих потерях, а также тем, что не всегда потери от хищения информации можно точно оценить в денежном эквиваленте. Однако по данным, опубликованным в сети, общие потери от несанкционированного доступа к информации в компьютерных системах в 1997 году оценивались в 20 миллионов долларов, а уже в 1998 года в 53,6 миллионов долларов.

В связи с этим, было принято решение, разработать приложение, позволяющее защитить информацию на диске.

# 2. ОБЗОР ЛИТЕРАТУРЫ

## 2.1. Шифрование/дешифрование

### 2.1.1. RSA

RSA (аббревиатура от фамилий Rivest, Shamir и Adleman) — криптографический алгоритм с открытым ключом, основывающийся на вычислительной сложности задачи факторизации больших целых чисел.

Криптосистема RSA стала первой системой, пригодной и для шифрования, и для цифровой подписи. Алгоритм используется в большом числе криптографических приложений, включая PGP, S/MIME, TLS/SSL, IPSEC/IKE и других.

Криптографические системы с открытым ключом используют так называемые односторонние функции, которые обладают следующим свойством:

* если известно x, то f(x) вычислить относительно просто;
* если известно y=f(x), то для вычисления x нет простого(эффективного)

пути.

Под односторонностью понимается не теоретическая однонаправленность, а практическая невозможность вычислить обратное значение, используя современные вычислительные средства, за обозримый интервал времени.

В основу криптографической системы с открытым ключом RSA положена сложность задачи факторизации произведения двух больших простых чисел. Для шифрования используется операция возведения в степень по модулю большого числа. Для дешифрования за разумное время (обратной операции) необходимо уметь вычислять функцию Эйлера от данного большого числа, для чего необходимо знать разложения числа на простые множители.

В криптографической системе с открытым ключом каждый участник располагает как открытым ключом (англ. public key), так и закрытым ключом (англ. private key). В криптографической системе RSA каждый ключ состоит из пары целых чисел. Каждый участник создаёт свой открытый и закрытый ключ самостоятельно. Закрытый ключ каждый из них держит в секрете, а открытые ключи можно сообщать кому угодно или даже публиковать их.

Алгоритм шифрования сеансового ключа

Наиболее используемым в настоящее время является смешанный алгоритм шифрования, в котором сначала шифруется сеансовый ключ, а потом уже с его помощью участники шифруют свои сообщения симметричными системами. После завершения сеанса сеансовый ключ как правило уничтожается.

### 2.1.2 Имитовставка

Имитовставка (MAC, англ. message authentication code — код аутентификации сообщения) — средство обеспечения имитозащиты в протоколах аутентификации сообщений с доверяющими друг другу участниками — специальный набор символов, который добавляется к сообщению и предназначен для обеспечения его целостности и аутентификации источника данных. MAC обычно применяется для обеспечения целостности и защиты от фальсификации передаваемой информации.

Для проверки целостности (но не аутентичности) сообщения на отправляющей стороне к сообщению добавляется значение хеш-функции от этого сообщения, на приемной стороне также вырабатывается хеш от полученного сообщения. Выработанный на приёмной стороне и полученный хеш сравниваются, если они равны то считается, что полученное сообщение дошло без изменений.

Для защиты от фальсификации (имитации) сообщения применяется имитовставка, выработанная с использованием секретного элемента (ключа), известного только отправителю и получателю.

Окно шифрования представлено на рис.1.1.

Рис. 1.1 Окно шифрования

Рис. 1.2 Зашифрованное хранилище

Рис. 1.3 Окно дешифрования

Рис. 1.4 Расшифрованная папка

# 3. ФУНКЦИОНАЛЬНОЕ ПРОЕКТИРОВАНИЕ

## 3.1. Создание хранилища

Создание хранилища осуществляет класс Storage.

## 3.2 Шифрование и дешифрование хранилища

Шифрование дешифрование хранилища обеспечивает классы SecureDisk и cryptohandler.

# СПИСОК ЛИТЕРАТУРЫ

1. https://ru.wikipedia.org/wiki/RSA

2. https://ru.wikipedia.org/wiki/Message\_authentication\_code

3. http://www.cryptopp.com/

3.

Заключение