МИНОБРНАУКИ РОССИИ

Федеральное государственное бюджетное образовательное учреждение высшего образования

НИЖЕГОРОДСКИЙ ГОСУДАРСТВЕННЫЙ ТЕХНИЧЕСКИЙ



УНИВЕРСИТЕТ им. Р.Е.АЛЕКСЕЕВА

ОТЧЁТ

по лабораторной работе №5

по дисциплине

Защита информации

РУКОВОДИТЕЛЬ:

Капранов С.Н.

СТУДЕНТ:

Докукин Д.В.

ГРУППА:

20-ПО

Нижний Новгород 2023-2024

Задание

Лабораторная работа 5 – Ассиметричные алгоритмы шифрования

Задание №8.1

Реализовать алгоритм шифрования данных «RSA».

Описание алгоритма

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

Алгоритм создания открытого и секретного ключей

RSA-ключи генерируются следующим образом:

1) выбираются два различных [случайных простых числа](https://ru.wikipedia.org/wiki/%D0%A1%D0%BB%D1%83%D1%87%D0%B0%D0%B9%D0%BD%D0%BE%D0%B5_%D0%BF%D1%80%D0%BE%D1%81%D1%82%D0%BE%D0%B5_%D1%87%D0%B8%D1%81%D0%BB%D0%BE) p и q заданного размера (например, 1024 [бита](https://ru.wikipedia.org/wiki/%D0%91%D0%B8%D1%82) каждое);

2) вычисляется их произведение n = p ⋅ q, которое называется модулем;

3) вычисляется значение [функции Эйлера](https://ru.wikipedia.org/wiki/%D0%A4%D1%83%D0%BD%D0%BA%D1%86%D0%B8%D1%8F_%D0%AD%D0%B9%D0%BB%D0%B5%D1%80%D0%B0) от числа n :



φ ( n ) = ( p − 1 ) ⋅ ( q − 1 )

4) выбирается целое число e ( 1 < e < φ ( n ) , [взаимно простое](https://ru.wikipedia.org/wiki/%D0%92%D0%B7%D0%B0%D0%B8%D0%BC%D0%BD%D0%BE_%D0%BF%D1%80%D0%BE%D1%81%D1%82%D1%8B%D0%B5_%D1%87%D0%B8%D1%81%D0%BB%D0%B0) со значением функции φ ( n );

число e называется открытой экспонентой;

обычно в качестве e берут простые числа, содержащие небольшое количество единичных бит в [двоичной записи](https://ru.wikipedia.org/wiki/%D0%94%D0%B2%D0%BE%D0%B8%D1%87%D0%BD%D0%B0%D1%8F_%D1%81%D0%B8%D1%81%D1%82%D0%B5%D0%BC%D0%B0_%D1%81%D1%87%D0%B8%D1%81%D0%BB%D0%B5%D0%BD%D0%B8%D1%8F), например, простые из [чисел Ферма](https://ru.wikipedia.org/wiki/%D0%A7%D0%B8%D1%81%D0%BB%D0%B0_%D0%A4%D0%B5%D1%80%D0%BC%D0%B0): 17, 257 или 65537, так как в этом случае время, необходимое для шифрования с использованием   
[быстрого возведения в степень](https://ru.wikipedia.org/wiki/%D0%90%D0%BB%D0%B3%D0%BE%D1%80%D0%B8%D1%82%D0%BC_%D0%B1%D1%8B%D1%81%D1%82%D1%80%D0%BE%D0%B3%D0%BE_%D0%B2%D0%BE%D0%B7%D0%B2%D0%B5%D0%B4%D0%B5%D0%BD%D0%B8%D1%8F_%D0%B2_%D1%81%D1%82%D0%B5%D0%BF%D0%B5%D0%BD%D1%8C), будет меньше;

слишком малые значения e, например 3, потенциально могут ослабить безопасность схемы RSA.

5) вычисляется число d, [мультипликативно обратное](https://ru.wikipedia.org/wiki/%D0%9E%D0%B1%D1%80%D0%B0%D1%82%D0%BD%D0%BE%D0%B5_%D0%BF%D0%BE_%D0%BC%D0%BE%D0%B4%D1%83%D0%BB%D1%8E_%D1%87%D0%B8%D1%81%D0%BB%D0%BE) к числу e по модулю φ ( n ), то есть число, удовлетворяющее [сравнению](https://ru.wikipedia.org/wiki/%D0%A1%D1%80%D0%B0%D0%B2%D0%BD%D0%B5%D0%BD%D0%B8%D0%B5_%D0%BF%D0%BE_%D0%BC%D0%BE%D0%B4%D1%83%D0%BB%D1%8E):

d ⋅ e ≡ 1 ( mod φ ( n ) )

(число d называется секретной экспонентой; обычно оно вычисляется при помощи  [расширенного алгоритма Евклида](https://ru.wikipedia.org/wiki/%D0%A0%D0%B0%D1%81%D1%88%D0%B8%D1%80%D0%B5%D0%BD%D0%BD%D1%8B%D0%B9_%D0%B0%D0%BB%D0%B3%D0%BE%D1%80%D0%B8%D1%82%D0%BC_%D0%95%D0%B2%D0%BA%D0%BB%D0%B8%D0%B4%D0%B0));

6) пара ( e , n ) публикуется в качестве открытого ключа RSA;

7) пара ( d , n ) играет роль закрытого ключа RSA и держится в секрете.

Алгоритм шифрования:

Взять открытый ключ ( e , n )

Взять открытый текст m

Зашифровать сообщение с использованием открытого ключа:

c = E ( m ) = m^e mod n

Алгоритм расшифрования:

Принять зашифрованное сообщение c

Взять свой закрытый ключ ( d , n )

Применить закрытый ключ для расшифрования сообщения:

m = D ( c ) = c^d mod n

Демонстрация работы программы

Для демонстрации, согласно требованиям, будут зашифрованы следующие сообщения:

1. Нижегородский Государственный Технический Университет
2. Докукин Дмитрий Владимирович

Ключ будет сгенерирован автоматически, при помощи приложения. Он хранится, как текстовый документ.

Зашифрованное сообщение получается в формате бинарного файла.

Пример 1

Шифрование сообщения: Нижегородский Государственный Технический Университет

Команда

./rsa keygen

позволяет сгенерировать подходящий ключ для шифрования. Будет создано два файла с публичным и приватным ключами. Без указания названия файла ключа, по умолчанию будут созданы «key» и «key.pub». Ключ состоит из пары значений экспонента-модуль.

В файле text.txt записано сообщение. Шифртекст будет записан в файл encrypted.

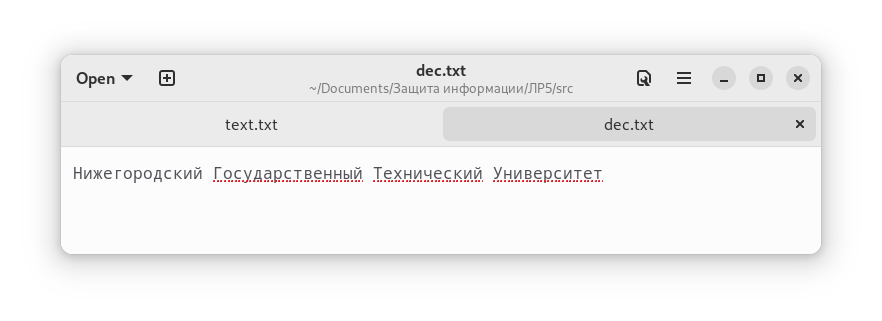
Следующая команда вызывает шифрование указанного сообщения:

./rsa encrypt text.txt encrypted key=key.pub

При расшифровке, указываю операцию расшифровки, файл с шифртекстом (encrypted),имя файла для расшифрованного сообщения (decrypted.txt) и файл с ключом (key):

./rsa decrypt encrypted dec.txt key=key

Содержимое файла dec.txt:

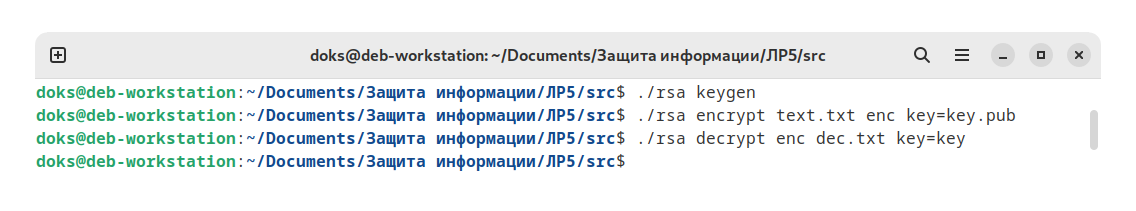


Расшифровка прошла успешно.

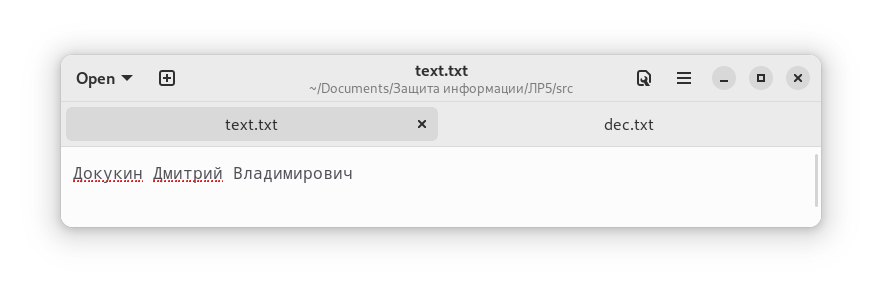
Пример 2

Шифрование и расшифровка сообщения: Докукин Дмитрий Владимирович

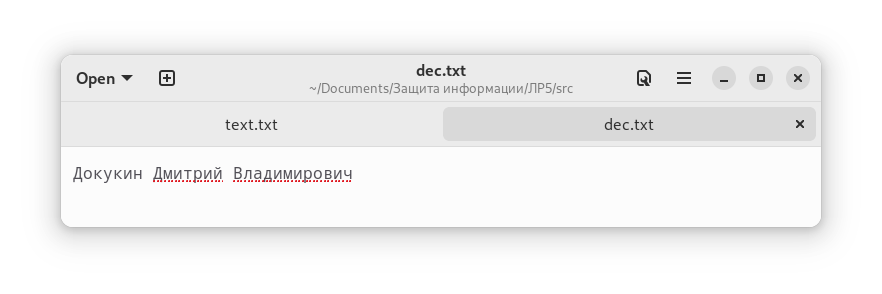
Все операции показаны на одном скриншоте:



Содержимое файла text.txt:



Содержимое файла dec.txt:



Процессы прошли успешно.

Программа

В программе представлены несколько классов и одно пространство имён:

InputHandler – отвечает за обработку ввода. Проверяет входные данные на корректность, хранит в себе имена файлов.

RSA – отвечает за шифрование и расшифровку. Хранит в себе значение ключа. Имеет методы шифрования, расшифрования и генерации ключа.

RSA::Key – вложенный класс. Содержит модуль и экспоненту ключа.

FileManager – позволяет считывать данные из файлов и сохранять результаты шифрования и расшифрования.

MPZ – класс, реализующий поддержку целых чисел динамической размерности.

Экземпляры данных классов объявляются в файле main.cpp, где происходит последовательный вызов нужных методов для выполнения требуемой операции.

KeyHandling – пространство имён, содержащее функции импорта, экспорта и обработки ключей.

Программа была написана при использовании библиотеки GMP.