Министерство образования Республики Беларусь

Учреждение образования

БЕЛОРУССКИЙ ГОССУДАРСТВЕННЫЙ УНИВЕРСИТЕТ

ИНФОРМАТИКИ И РАДИОЭЛЕКТРОННИКИ

КАФЕДРА ИНФОРМАТИКИ

Отчёт по лабораторной работе №3

По дисциплине «Методы защиты информации»

По теме «Ассиметричная криптография. RSA»

Выполнил:

студент гр. 653502

Максименко П.В.

Проверил:

Артемьев В. С.

Минск 2019

1. Постановка зада4и

Написать программу, реализующую алгоритм RSA шифрования данных.

2. Теорети4еская 4асть

**RSA** (аббревиатура от фамилий Rivest, Shamir и Adleman) — [криптографический алгоритм с открытым ключом](https://ru.wikipedia.org/wiki/%D0%9A%D1%80%D0%B8%D0%BF%D1%82%D0%BE%D1%81%D0%B8%D1%81%D1%82%D0%B5%D0%BC%D0%B0_%D1%81_%D0%BE%D1%82%D0%BA%D1%80%D1%8B%D1%82%D1%8B%D0%BC_%D0%BA%D0%BB%D1%8E%D1%87%D0%BE%D0%BC), основывающийся на [вычислительной сложности](https://ru.wikipedia.org/wiki/%D0%92%D1%8B%D1%87%D0%B8%D1%81%D0%BB%D0%B8%D1%82%D0%B5%D0%BB%D1%8C%D0%BD%D0%B0%D1%8F_%D1%81%D0%BB%D0%BE%D0%B6%D0%BD%D0%BE%D1%81%D1%82%D1%8C) [задачи факторизации](https://ru.wikipedia.org/wiki/%D0%A4%D0%B0%D0%BA%D1%82%D0%BE%D1%80%D0%B8%D0%B7%D0%B0%D1%86%D0%B8%D1%8F_%D1%86%D0%B5%D0%BB%D1%8B%D1%85_%D1%87%D0%B8%D1%81%D0%B5%D0%BB) больших целых чисел.

Криптосистема RSA стала первой системой, пригодной и для [шифрования](https://ru.wikipedia.org/wiki/%D0%A8%D0%B8%D1%84%D1%80%D0%BE%D0%B2%D0%B0%D0%BD%D0%B8%D0%B5), и для [цифровой подписи](https://ru.wikipedia.org/wiki/%D0%A6%D0%B8%D1%84%D1%80%D0%BE%D0%B2%D0%B0%D1%8F_%D0%BF%D0%BE%D0%B4%D0%BF%D0%B8%D1%81%D1%8C). Алгоритм используется в большом числе криптографических приложений, включая [PGP](https://ru.wikipedia.org/wiki/PGP), [S/MIME](https://ru.wikipedia.org/wiki/S/MIME), [TLS](https://ru.wikipedia.org/wiki/TLS)/[SSL](https://ru.wikipedia.org/wiki/SSL), [IPSEC](https://ru.wikipedia.org/wiki/IPSEC)/[IKE](https://ru.wikipedia.org/wiki/IKE) и других.

3. Блок-схема



Рис 3.1. Схема работы алгоритма.

4. Ход программы

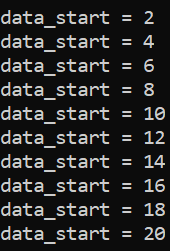


Рис 4.1. Данные, поступающие на вход

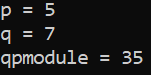


Рис 4.2. Генерирование клю4ей



Рис 4.3. Вы4исление функции Эйлера и нахождение взаимно простого 4исла

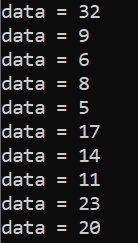


Рис 4.4. Зашифрованные данные

5. Код программы

float\* RSA()

{

// creating keys:

int p = 5;

int q = 7;

int qpmodule = p \* q;

std::cout << '\n';

std::cout << "p = " << p << std::endl;

std::cout << "q = " << q << std::endl;

std::cout << "qpmodule = " << qpmodule << std::endl;

std::cout << '\n';

int Euler\_func = (p - 1) \* (q - 1);

std::cout << "Euler's function = " << Euler\_func << std::endl;

int new\_num = 0;

int mut\_simple = 0;

for (int i = 2; i < Euler\_func; i++) {

int flag = 0;

for (int j = 2; j < Euler\_func; j++) {

if ((Euler\_func % j == 0) && (i % j == 0))

{

flag = 1;

}

}

if (flag == 0)

{

mut\_simple = i;

break;

}

}

std::cout << "Muttual simple number = " << mut\_simple << std::endl;

std::cout << '\n';

float d = 1 / mut\_simple;

int public\_key[2] = {mut\_simple, qpmodule};

float private\_key[2] = {d, qpmodule};

// data init

float data\_help[10];

for (int i = 0; i < 10; i++) {

data\_help[i] = (i + 1) \* 2;

std::cout << "data\_start = " << data\_help[i] << std::endl;

}

std::cout << '\n';

// encryption

for (int i = 0; i < 10; i++) {

data\_help[i] = pow(data\_help[i], public\_key[0]);

data\_help[i] = int(data\_help[i]) % public\_key[1];

std::cout << "data = " << data\_help[i] << std::endl;

}

return data\_help;

}

6. Вывод

В ходе выполнения лабораторной работы был успешно реализован алгоритм RSA. Были выявлены его сильные и слабые стороны, а также возможности улу4шения, например внедрением алгоритма быстрого возведения в степень. Однако, этот алгоритм всё ещё будет довольно медленным, например, на фоне AES.

Также, в 2010 году группе учёных из Швейцарии, Японии, Франции, Нидерландов, Германии и США удалось успешно вычислить данные, зашифрованные при помощи криптографического ключа стандарта RSA длиной 768 бит. Нахождение простых сомножителей осуществлялось [общим методом решета числового поля](https://ru.wikipedia.org/wiki/%D0%9E%D0%B1%D1%89%D0%B8%D0%B9_%D0%BC%D0%B5%D1%82%D0%BE%D0%B4_%D1%80%D0%B5%D1%88%D0%B5%D1%82%D0%B0_%D1%87%D0%B8%D1%81%D0%BB%D0%BE%D0%B2%D0%BE%D0%B3%D0%BE_%D0%BF%D0%BE%D0%BB%D1%8F). По словам исследователей, после их работы в качестве надежной системы шифрования можно рассматривать только RSA-ключи длиной 1024 бита и более.