МИНИСТЕРСТВО ОБРАЗОВАНИЯ И НАУКИ ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ БЮДЖЕТНОЕ ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ ВЫСШЕГО ОБРАЗОВАНИЯ «ВОРОНЕЖСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ» (ФГБОУ ВО «ВГУ»)

Факультет прикладной математики, информатики и механики

Кафедра Системного анализа и управления

Лабораторная работа №4

«Алгоритм RSA»

Выполнил: студент 4 к. 6 гр. ПМИ

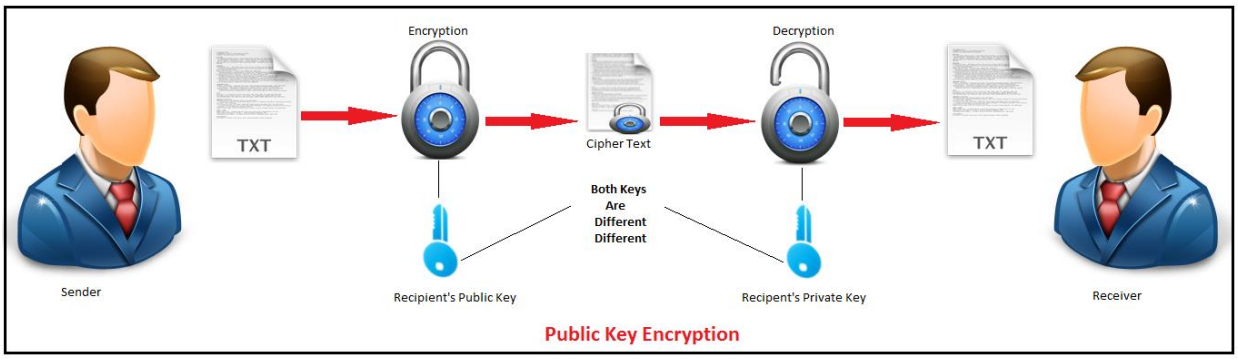
Бакаев Илья Игоревич

Воронеж – 2021

1. Цель работы:
Программно реализовать алгоритм RSA.

2. Теоретические сведения:

RSA — криптографический алгоритм с открытым ключом, основывающийся на вычислительной сложности задачи факторизации больших целых чисел.



Описание алгоритма:
1. Выбираются два простых числа p и q заданного размера.
2. Вычисляется их произведение: n = pq
3. Вычисляется значение функции Эйлера (значение функции Кармайкла):

$$\varphi(n) = (p-1)\cdot(q-1);$$

или

$$\lambda(n);$$
$$n = pq;$$
$$\lambda(n) = lcm(\lambda(p), \lambda(q)));$$
$$\lambda(p) = \varphi(p) = (p \quad 1); p \quad prime;$$
$$\lambda(q) = \varphi(q) = (q-1); q - prime;$$
$$\lambda(n) = lcm((p-1),(q-1)));$$
$$lcm(a,b) = |a\cdot b|/gcd(a,b); (Least - Common - Multiple)$$
$$\lambda(n) = |(p-1)\cdot(q-1)|/gcd((p-1),(q-1));$$
$$\varphi(n) = (p-1)\cdot(q-1); p,q - primes;$$
$$g = gcd((p-1),(q-1)); (greatest - common - divisor, Euclidean - algorithm)$$
$$\downarrow$$
$$\lambda(n) = \varphi(n)/g;$$

4. Выбирается целое число d (секретная экспонента, 1< d < φ (n))

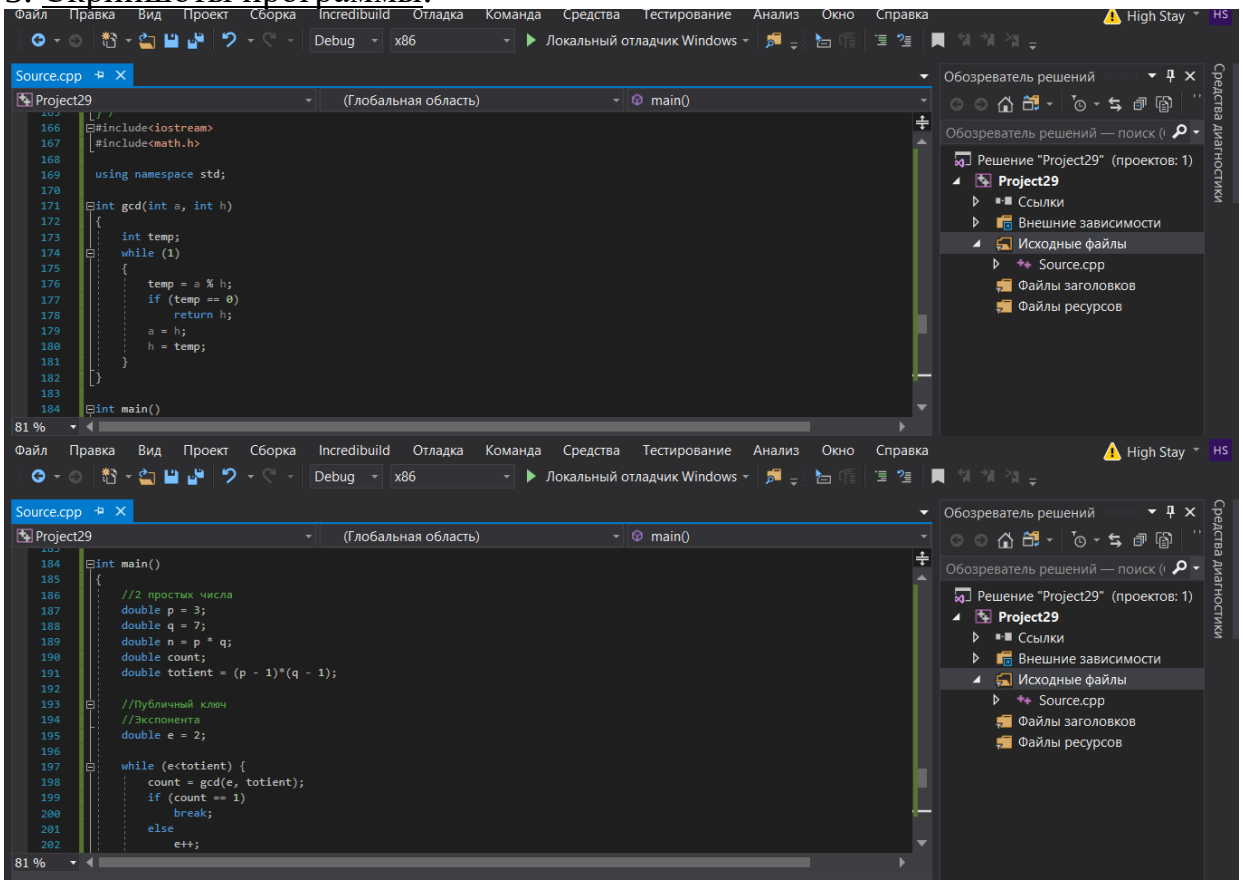
5. Вычисляется число e (открытая экспонента), мультипликативно обратное к d по модулю φ (n)

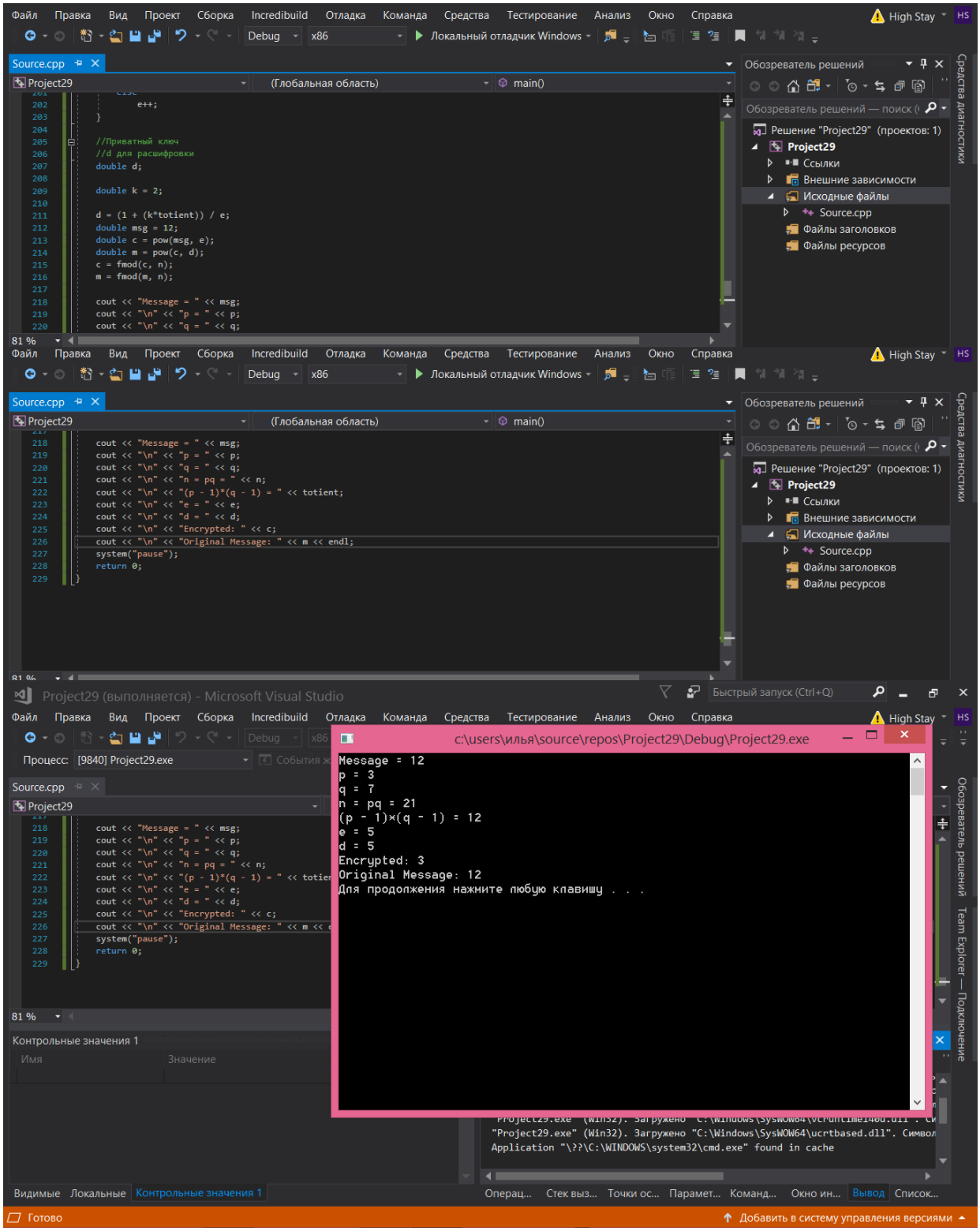
6. Пара (e, n) публикуется в качестве открытого ключа

7. Пара (d, n) играет роль закрытого ключа

Наиболее распространён в настоящее время смешанный алгоритм шифрования, в котором сначала шифруется сеансовый ключ, а потом участники с помощью данного ключа шифруют свои сообщения симметричными системами.

3. Скриншоты программы:





Программа протестирована в Visual Studio 2017.

Стандарт C++: 14882:2017(E)