Федеральное государственное автономное

образовательное учреждение

высшего профессионального образования

«СИБИРСКИЙ ФЕДЕРАЛЬНЫЙ УНИВЕРСИТЕТ»

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

институт

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

кафедра

**ОТЧЕТ ПО ЛАБОРАТОРНОЙ РАБОТЕ**

Алгоритм шифрования RSA

тема

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Преподаватель \_\_\_\_\_\_\_\_ \_\_\_\_\_\_\_\_\_\_\_\_\_\_

подпись, дата инициалы, фамилия

Студент \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ \_\_\_\_\_\_\_\_ \_\_\_\_\_\_\_\_\_\_\_\_\_\_

номер группы, зачетной книжки подпись, дата инициалы, фамилия

Красноярск 2015

Оглавление

[Задания 3](#_Toc417030214)

[Описание алгоритма 4](#_Toc417030215)

[Блок-схема алгоритма 5](#_Toc417030216)

[Листинг программы 6](#_Toc417030217)

[Примеры работы программы: 10](#_Toc417030218)

[Тестирование производительности 16](#_Toc417030219)

[Заключения и выводы: 22](#_Toc417030220)

# Задания

1. Составить в виде блок-схемы алгоритм шифрования/дешифрования RSA, со следующими особенностями:

* объём исходного текста – любой (в разумных пределах);
* исходный текст может состоять из русских и английских букв, цифр, а также знаков препинания;
* исходный текст находится в кодировке ASCII;
* N состоит из 47 десятичных знаков.
* Числа P и Q выбираются случайным образом, так, что , где P и Q – простые числа.
* исходный текст разбивается на K блоков, где K выбирается исходя из значения модуля N

1. Убедиться в правильности составления алгоритмов, а затем на языке C# составить программу, которая реализует данный алгоритм.
2. На ряде контрольных примеров (не менее 10) открытого текста проверить правильность работы алгоритмов шифрования и дешифрования (в качестве контрольного примера понимается текстовый файл в кодировке ASCII).
3. Оцените криптостойкость моего варианта алгоритма RSA, а также сделать оценку производительности, разработанной программы.

# Описание алгоритма

1. Генерация открытого и закрытого ключей
   1. Выбираются два различных случайных простых числа заданного размера.
   2. Вычисляется их произведение
   3. Вычисляется значение *функции Эйлера*
   4. Случайным образом выбирается число и взаимно простое с
   5. Вычисляется ***e***, такое что - обратный элемент в кольце целых чисел
2. Шифрование
   1. Сообщение ***M*** разбивается на на ***K***, блоков : так что размер каждого блока **.**
   2. Каждый из блоков шифруется по формуле
   3. Зашифрованное сообщениепередается.
3. Расшифровка
   1. Для каждого блока из полученного  вычисляется

* 1. Блоки объединяются в сообщение.
  2. - исходное сообщение

# Блок-схема алгоритма



# Листинг программы

using System;

using System.Collections.Generic;

using System.Numerics;

using System.Security.Cryptography;

namespace RSA\_Project

{

public class RSA

{

private static readonly Random Rnd = new Random((int) DateTime.Now.Ticks);

private static readonly RandomNumberGenerator Rng = RandomNumberGenerator.Create();

private readonly BigInteger P; //P,Q -простые числа. N - их произведение

private readonly BigInteger Q; //P,Q -простые числа. N - их произведение

private readonly int[] \_fermatNumbers = {17, 257, 65537}; //Числа ферма

private readonly byte \_lengthN; //длина числа n

private readonly BigInteger private\_key; //откртый и закрытый ключи

private readonly BigInteger public\_key; //откртый и закрытый ключи

private BigInteger N; //P,Q -простые числа. N - их произведение

public RSA(byte lengthN)

{

//Инициализация класса

\_lengthN = lengthN;

KeyValuePair<BigInteger, BigInteger> pair = GeneratePrimesPair(lengthN/2 - lengthN/10);

//Генерирует пару простых чисел

P = pair.Key;

Q = pair.Value;

N = P\*Q;

BigInteger eulierFunction = (P - 1)\*(Q - 1);

public\_key = \_fermatNumbers[Rnd.Next(0, \_fermatNumbers.Length)];

private\_key = CalcPrivateKey(eulierFunction);

}

public RSA(BigInteger P, BigInteger Q)

{

this.P = P;

this.Q = Q;

N = P\*Q;

BigInteger eulierFunction = (P - 1)\*(Q - 1);

public\_key = 11;

private\_key = CalcPrivateKey(eulierFunction);

}

public BigInteger Module

{

get { return N; }

}

public KeyValuePair<BigInteger, BigInteger> PrimePair

{

get { return new KeyValuePair<BigInteger, BigInteger>(P, Q); }

}

public BigInteger PrivateKey

{

get { return private\_key; }

}

public BigInteger PublicKey

{

get { return public\_key; }

}

public long ModuleLength

{

//Длина модуля в байтах

get

{

long l = N.ToByteArray().Length;

return l;

}

}

public byte[] Encrypt(byte[] message)

{

//Шифруем сообщение открытым ключом

var val = new BigInteger(message);

val = BigInteger.ModPow(val, public\_key, N);

return val.ToByteArray();

}

public byte[] Decrypt(byte[] message)

{

//Расшифруем cообщение открытм ключом

var val = new BigInteger(message);

val = BigInteger.ModPow(val, private\_key, N);

return val.ToByteArray();

}

private BigInteger CalcPrivateKey(BigInteger E)

{

//Вычисляем закрытый ключ, находя обратный по модулю элемент кольца

BigInteger x, y;

BigInteger g = GCD(public\_key, E, out x, out y);

return (x%E + E)%E;

}

private BigInteger GCD(BigInteger a, BigInteger b, out BigInteger x, out BigInteger y)

{

//Расширеный Алгоритм Евклида

if (a.IsZero) //Находит НОД чисел A и B, и коэфициенты x,y уравнения Ax +By = НОД(A,B)

{

x = 0;

y = 1;

return b;

}

BigInteger x1, y1;

BigInteger d = GCD(b%a, a, out x1, out y1);

x = y1 - (b/a)\*x1;

y = x1;

return d;

}

private KeyValuePair<BigInteger, BigInteger> GeneratePrimesPair(int length)

{

//Генерирует пару простых чисел, таких что их произведение имеет ровно lengthN знаков

var resList = new List<BigInteger>();

BigInteger p = BigInteger.One;

int curLength = 1;

while (curLength < length)

{

curLength++;

p \*= 10;

}

BigInteger lowLimit = p;

BigInteger upLimit = p\*10;

//Генерируем число в заданном диапазоне

var bytes = new byte[p.ToByteArray().LongLength];

while (p <= lowLimit || p > upLimit)

{

Rng.GetBytes(bytes);

p = new BigInteger(bytes);

}

//Ищем ближайшее простое

while (!IsProbablePrime(p, 40))

{

p += 1;

}

// Генерируем число в диапазоне 10^lengthN - 10^(lengthN+1)

while (curLength < \_lengthN)

{

curLength++;

lowLimit \*= 10;

}

upLimit = lowLimit\*10;

bytes = new byte[lowLimit.ToByteArray().LongLength];

BigInteger q;

do

{

Rng.GetBytes(bytes);

q = new BigInteger(bytes);

} while (q <= lowLimit || q >= upLimit);

//делим с остатком на найденное просто число

q = q/p;

while (!IsProbablePrime(q, 40))

{

q += 1;

}

//ищем ближайшее простое к нему

return new KeyValuePair<BigInteger, BigInteger>(p, q); //Возвращаем пару найденных чисел

}

private static bool IsProbablePrime(BigInteger source, int certainty)

{

//Вероятностный тест Миллера-Рабина для определения простоты числа

if (source == 2 || source == 3)

return true;

if (source < 2 || source%2 == 0)

return false;

BigInteger d = source - 1;

int s = 0;

while (d%2 == 0)

{

d /= 2;

s += 1;

}

var bytes = new byte[source.ToByteArray().LongLength];

BigInteger a;

for (int i = 0; i < certainty; i++)

{

do

{

Rng.GetBytes(bytes);

a = new BigInteger(bytes);

} while (a < 2 || a >= source - 2);

BigInteger x = BigInteger.ModPow(a, d, source);

if (x == 1 || x == source - 1)

continue;

for (int r = 1; r < s; r++)

{

x = BigInteger.ModPow(x, 2, source);

if (x == 1)

return false;

if (x == source - 1)

break;

}

if (x != source - 1)

return false;

}

return true;

}

}

}

using System;

using System.Collections.Generic;

using System.Text;

namespace RSA\_Project

{

public class MessageManager

{

//Класс работающий с кодировками и разбиением текста

public static String PartitionToString(List<byte[]> p)

{

//Переобразует разбиение в строку

String result = String.Empty;

foreach (var block in p)

{

result += GetString(block);

}

return result;

}

public static List<byte[]> partitionOfString(String s, long length)

{

//Разбиваем строку на блоки(байт-массивы)

var result = new List<byte[]>();

byte[] bytes = GetBytes(s);

var block = new List<byte>();

int count = 0;

foreach (byte x in bytes)

{

count++;

if (count < length)

{

block.Add(x);

}

else

{

result.Add(block.ToArray());

block.Clear();

block.Add(x);

count = 1;

}

}

if (block.Count > 0) result.Add(block.ToArray());

return result;

}

public static byte[] GetBytes(string str)

{

byte[] utf8bytes = Encoding.Unicode.GetBytes(str);

byte[] win1251Bytes = Encoding.Convert(

Encoding.Unicode, Encoding.GetEncoding("windows-1251"), utf8bytes);

//byte[] bytes = Encoding.ASCII.GetBytes(str);

return win1251Bytes;

}

public static string GetString(byte[] bytes)

{

byte[] unicodeBytes = Encoding.Convert(

Encoding.GetEncoding("windows-1251"), Encoding.Unicode, bytes);

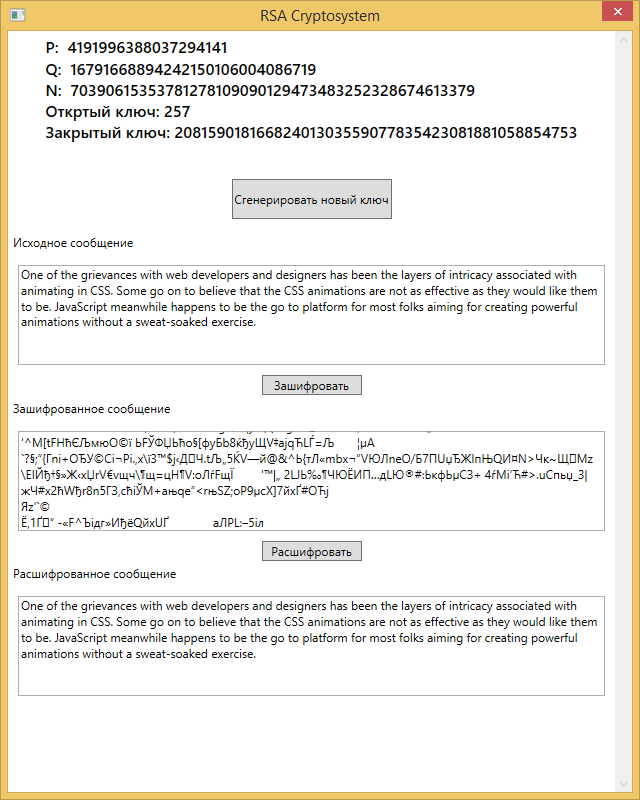
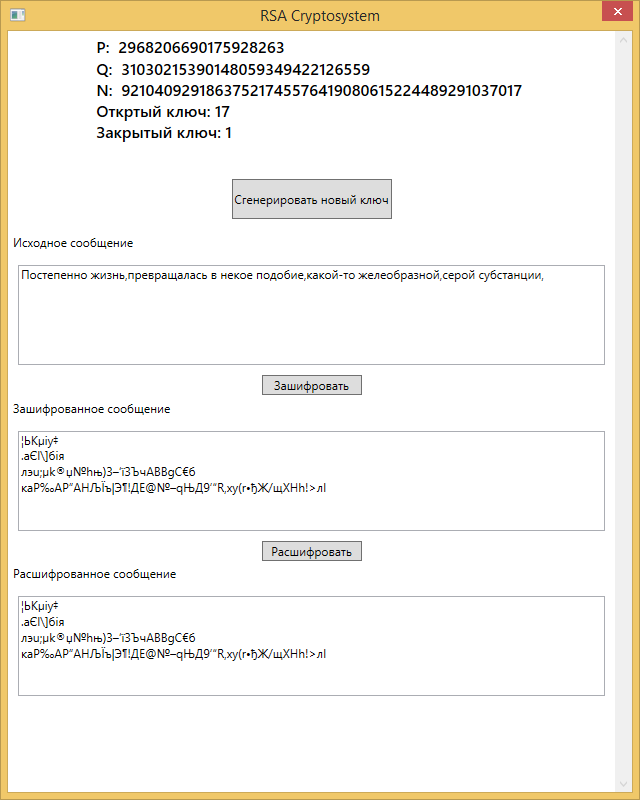
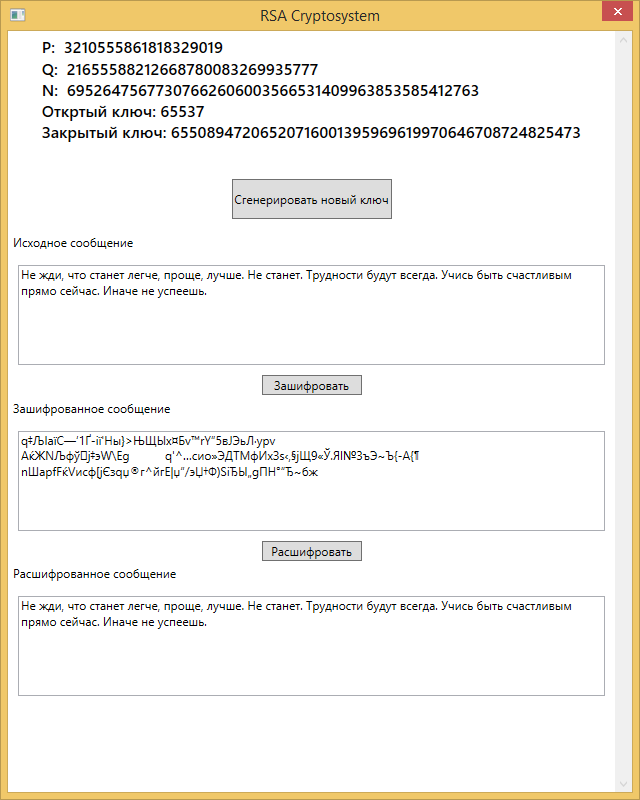
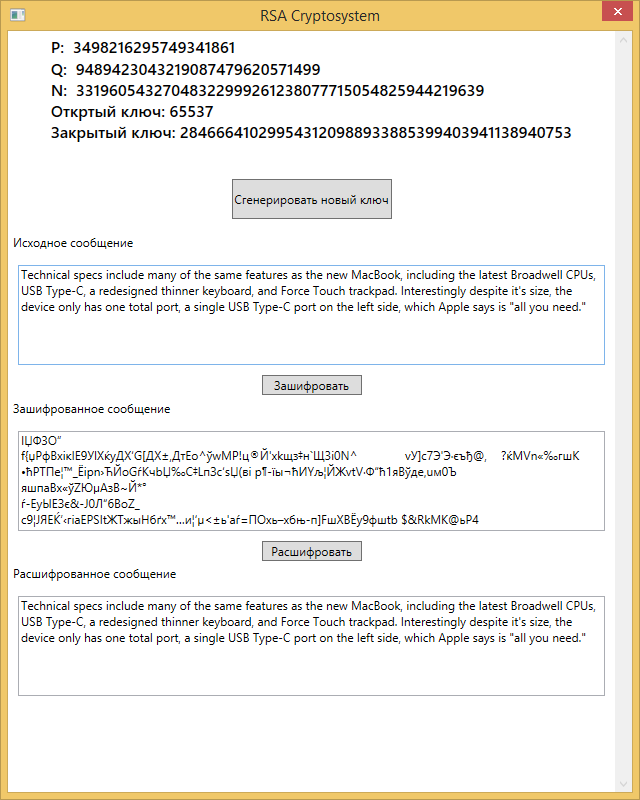
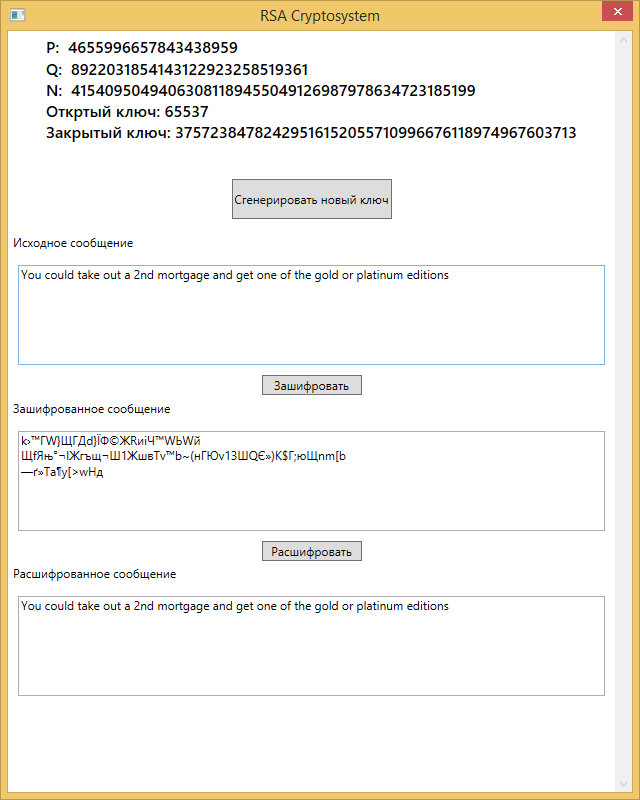
return Encoding.Unicode.GetString(unicodeBytes);

}

}

}

# Примеры работы программы:

****

# Тестирование производительности

Windows 8.1 Профессиональная

Процессор: Intel Core Duo E8600 @ 3.33GHz 2.67GHz

Установленная память: 8,00 ГБ

Тип системы: 64-разрядная операционная система, процессор x64

Время измеряется в миллисекундах (1s == 1000ms)

N – количество десятичных разрядов

TestMethod1 – измерение среднего времени генерации ключа

TestMethod2 – измерение среднего времени генерации одного простого числа

TestMethod3 – измерение среднего времени одной итерации проверки числа на простоту

using System;

using System.Numerics;

using System.Security.Cryptography;

using Microsoft.VisualStudio.TestTools.UnitTesting;

namespace RSA\_Project.UnitTest

{

[TestClass]

public class UnitTest1

{

private static readonly RandomNumberGenerator Rng = RandomNumberGenerator.Create();

[TestMethod]

public void TestMethod1()

{

const int count = 20;

Console.WriteLine(@"# N GeneratePrimesPair");

for (byte decimals = 20; decimals < 50; decimals++)

{

var rsa = new RSA(decimals);

DateTime t = DateTime.Now;

for (int i = 0; i < count; i++)

rsa.GeneratePrimesPair(decimals);

var ts = new TimeSpan(DateTime.Now.Ticks - t.Ticks);

Console.WriteLine(@"{0} {1}", decimals, ts.TotalMilliseconds/count);

}

}

[TestMethod]

public void TestMethod2()

{

const int count = 20;

Console.WriteLine(@"# N Primary");

for (int decimals = 20; decimals < 50; decimals++)

{

var bits = (int) Math.Ceiling(decimals/Math.Log10(2));

int bytes = (bits + 7)/8;

DateTime t = DateTime.Now;

for (int i = 0; i < count; i++)

{

var data = new byte[bytes];

Rng.GetBytes(data);

data[bytes - 1] = (byte) ((data[bytes - 1] & 127) | 64);

var x = new BigInteger(data);

while (!RSA.IsProbablePrime(x, RSA.NumberOfTests(x)))

{

x += 1;

}

}

var ts = new TimeSpan(DateTime.Now.Ticks - t.Ticks);

Console.WriteLine(@"{0} {1}", decimals, ts.TotalMilliseconds/count);

}

}

[TestMethod]

public void TestMethod3()

{

const int count = 20;

Console.WriteLine(@"# N IsProbablePrime");

for (int decimals = 20; decimals < 50; decimals++)

{

var bits = (int) Math.Ceiling(decimals/Math.Log10(2));

int bytes = (bits + 7)/8;

DateTime t = DateTime.Now;

int total = 0;

for (int i = 0; i < count; i++)

{

var data = new byte[bytes];

Rng.GetBytes(data);

data[bytes - 1] = (byte) ((data[bytes - 1] & 127) | 64);

BigInteger x = new BigInteger(data) | 1; // Простые являются нечётными

total += RSA.NumberOfTests(x);

RSA.IsProbablePrime(x, RSA.NumberOfTests(x));

}

var ts = new TimeSpan(DateTime.Now.Ticks - t.Ticks);

Console.WriteLine(@"{0} {1}", decimals, ts.TotalMilliseconds/count);

}

}

}

}

**# N GeneratePrimesPair**

**20 30.151785**

**21 11.550675**

**22 7.750455**

**23 15.90091**

**24 10.750615**

**25 22.7513**

**26 14.0508**

**27 11.00063**

**28 15.550895**

**29 13.25076**

**30 27.85159**

**31 23.10133**

**32 21.301225**

**33 22.501335**

**34 20.70121**

**35 31.801845**

**36 27.401595**

**37 53.203045**

**38 31.201815**

**39 27.451595**

**40 39.452295**

**41 39.602285**

**42 55.553215**

**43 48.352805**

**44 49.95287**

**45 52.853105**

**46 44.557375**

**47 56.903295**

**48 52.30303**

**49 101.90592**

**# N Primary**

**20 8.30045**

**21 9.20054**

**22 10.050565**

**23 10.350615**

**24 9.600545**

**25 11.60066**

**26 11.40067**

**27 13.70081**

**28 14.700835**

**29 19.701145**

**30 18.00109**

**31 19.751075**

**32 21.65129**

**33 21.70123**

**34 26.151505**

**35 24.75146**

**36 22.25129**

**37 28.801665**

**38 25.601475**

**39 38.152275**

**40 37.60211**

**41 37.9022**

**42 42.30244**

**43 41.75244**

**44 50.70294**

**45 46.80268**

**46 52.103025**

**47 52.503045**

**48 54.50316**

**49 67.90393**

**# N IsProbablePrime**

**20 0.700005**

**21 0.40002**

**22 0.85003**

**23 0.050015**

**24 1.00008**

**25 0.050005**

**26 0.55001**

**27 0.050035**

**28 0.09999**

**29 1.050055**

**30 0.350045**

**31 0.15001**

**32 1.35002**

**33 0.10005**

**34 0.149995**

**35 0.350015**

**36 0.09999**

**37 0.200055**

**38 1.200045**

**39 2.000135**

**40 2.100105**

**41 0.40002**

**42 0.199995**

**43 0.85006**

**44 0.300045**

**45 2.70012**

**46 2.400165**

**47 0.350035**

**48 0.19998**

**49 0.550055**

# Заключения и выводы:

1. В ходе работы были изучены следующие дополнительные навыки:

* Обобщённый алгоритм Евклида
* Вероятностный тест на простоту Миллера-Рабина
* Работ с большими числами в .NET
* Реализация оконного интерфейса с помощью технологии WPF
* Базовые знания теории чисел такие как:
  + Кольцо целых чисел
  + Функция Эйлера
  + Теорема Ферма
  + НОД
  + Сравнение по модулю

1. Алгоритм RSA является криптостойким и это свойство зависит напрямую от длины модуля N.