*Completed by student ПК-12-2 Beklenischev Vladislav*

# Program Description

## General

Program "RSA cipher" is the result of the laboratory work for the course "Methods of protection of information" and created only for educational purposes to demonstrate the encrypting / decrypting the various text messages.

To run the program you need the following software:

* Windows 7, 8, 8.1,
* Library .NET Framework version 4.5.

This program was written by means of C # on the .NET Framework in the environment Microsoft Visual Studio 2012.

## Functional purpose

Application is designed to decrypt / encrypt text messages of different lengths using an asymmetric encryption algorithm RSA.

The program allows you to encrypt text messages of different lengths.

## Description of the logical structure

As mentioned above, based on the program "RSA cipher" is the encryption algorithm RSA

RSA (theacronym of the names of Rivest, Shamir and Adleman ) - a cryptographic public key algorithm, based on computational complexity problem of factoring large integers.

RSA cryptosystem is the first system suitable for encryption and for digital signature

### Description and thealgorithm is RSA encryption

#### Search public and private keys

* Take two large prime numbers p and q.
* We define n, as a result of multiplying the p on q ( n = p \* q).
* We choose a random number that will be called d. This number must be relatively simple (not to have any common divisors except 1) with the result of the multiplication (p-1) \* (q-1) (the Eyler’s function).
* We define a number e, for which is true following relationship (e \* d) mod ((p-1) \* (q-1)) = 1.
* We call a public key numbers e and n, and a secret - d and n.

#### The encryption process

For encrypting data by the public key {e, n} must include an:

* encrypted text is divided into blocks, each of which may be in the form of M (i) = 0,1,2 ..., n-1 (i.e., only up to n-1).
* encrypt text considered as a sequence of numbers M (i) by the formula C (i) = (M (I) ^ e) mod n.

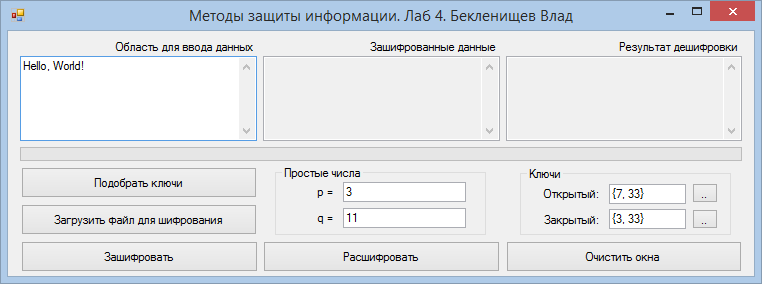
#### The process of decryption

To decrypt the data using the private key {d, n}, perform the following calculation: M(i) = (C(i) ^ d) mod n. As a result, will receive a set of numbers M (i), which are the source code.

## Call and load

The program is an application for Windows operating systems 7, 8, 8.1, 10. It can be run from the "Start" menu or by using the shortcut on the desktop.

After starting the main application window will appear:



## Input

Input data are text messages that can be administered either in the "Field data entry."

Also, the user can manually enter the value of the numbers P and Q, and also the values ​​of the opening and closing keys.

Note:

* P and Q should be a simple numbers.
* public / private key must be entered in this format: {key result\_of\_multily\_numbers\_PQ}.

## Output

Result of the program will be:

* encrypted text in the second field (after pressing the "Зашифровать")
* decrypted text in the third field (after you clicking the “Расшифровать”)

The text in the third field will be correspond to the text of the first field.

The user can clear all fields at once by clicking the "Очистить окна". It should take into account that you can not make encryption operations over the empty fields (1 and 2). If a user attempts to do this, the program will give a warning.