*Выполнил студент ПК-12-2, Бекленищев Владислав*

# Описание программы

## Общие сведения

Программа “RSA cipher” является результатом выполнения лабораторной работы для курса “Методы защиты информации” и создана только в учебных целях, для демонстрации зашифровывания / расшифровывания различных текстовых сообщений.

Для запуска программы необходимо следующее программное обеспечение:

* Операционная система Windows 7, 8, 8.1;
* Библиотека .NET Framework версии 4.5.

Данная программа была написана с помощью средств языка C# на платформе .NET Framework в среде Microsoft Visual Studio 2012.

## Функциональное назначение

Приложение предназначено для расшифровывания / зашифровывания текстовых сообщений разной длины с помощью асимметричного алгоритма шифрования RSA.

Программа позволяет шифровать текстовые сообщения разной длины.

## Описание логической структуры

Как уже было сказано выше, в основе программы “RSA cipher” лежит алгоритм шифрования RSA.

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

Криптосистема RSA стала первой системой, пригодной и для шифрования, и для цифровой подписи

### Описание алгоритма шифрования RSA

#### Поиск открытого и закрытого ключей

* Возьмем два больших простых числа p and q.
* Определим n, как результат умножения p on q (n= p\*q).
* Выберем случайное число, которое назовем d. Это число должно быть взаимно простым (не иметь ни одного общего делителя, кроме 1) с результатом умножения (p-1)\*(q-1) (функции Ейлера).
* Определим такое число е, для которого является истинным следующее соотношение (e\*d) mod ((p-1)\*(q-1))=1.
* Назовем открытым ключем числа e и n, а секретным - d и n.

#### Процесс шифрования

Для того, чтобы зашифровать данные по открытому ключу {e,n}, необходимо следующее:

* разбить шифруемый текст на блоки, каждый из которых может быть представлен в виде числа M(i)=0,1,2..., n-1( т.е. только до n-1).
* зашифровать текст, рассматриваемый как последовательность чисел M(i) по формуле C(i)=(M(I)^e)mod n.

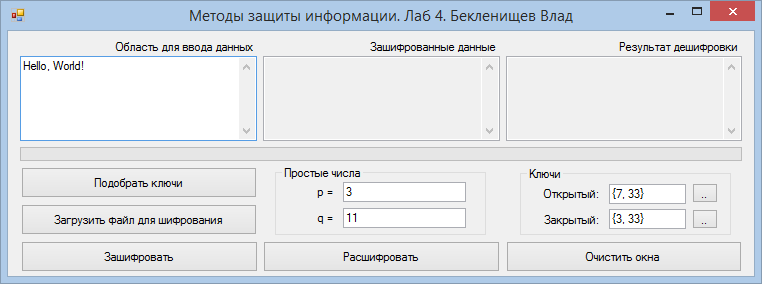
#### Процесс расшифровывания

Чтобы расшифровать эти данные, используя секретный ключ {d,n}, необходимо выполнить следующие вычисления: M(i) = (C(i)^d) mod n. В результате будет получено множество чисел M(i), которые представляют собой исходный текст.

## Вызов и загрузка

Так как программа является приложением под операционные системы Windows 7, 8, 8.1, 10 её можно запустить либо из меню “Пуск” либо же с помощью ярлыка на рабочем столе.

После запуска появится главное окно приложения:



## Входные данные

Входными данными являются текстовые сообщения, которые можно вводить либо в поле “Область для ввода данных”.

Также пользователю предоставляется возможности самостоятельно ввести значение чисел P и Q, а также значения открытого и закрытых ключей.

Примечание:

* P и Q должны быть простыми
* Открытый / закрытый ключ нужно вводить в таком формате: {ключ, результат\_умножения\_чисел\_PQ}.

## Выходные данные

Результатом работы программы будет:

* зашифрованный текст во втором поле (после нажатия на кнопку “Зашифровать”)
* расшифрованный текст в третьем поле (после нажатия на кнопку “Расшифровать”)

Текст в третьем поле будет однозначно соответствовать тексту из первого поля.

Также пользователь может очистить все поля сразу нажав кнопку “Очистить окна”. При этом нужно учесть, что нельзя сделать операции шифрования над пустым полем 1. Если пользователь попытается это сделать, программа выдаст предупреждение.