ЦЕЛЬ

Разработать шифрующую и дешифрующую программы, используя ассиметричное шифрование. Отправить зашифрованное письмо на почту. Программно получить зашифрованное письмо и расшифровать его.

Используемые языки программирования, технологии и протоколы:

* + язык программирования C# и технология WPF;
  + алгоритм ассиметричного шифрования RSA;
* протокол передачи почты Smtp;
* протокол получения почты Pop3.

RSA

Алгоритм RSA (буквенная 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

Первым этапом любого ассиметричного алгоритма является создание пары ключей – открытого и закрытого и распространение открытого ключа.

Создание ключей

Для алгоритма RSA этап создания ключей состоит из следующих операций:

* выбираются два очень больших простых числа p и q;
* вычисляется их произведение n=pq, которое называется модулем;
* вычисляется значение функции Эйлера от числа n:
* выбирается произвольное число, взаимно простое со значением функции .

С помощью алгоритма Евклида вычисляется число d, которое удовлетворяет условию .

* пара   открытый ключ RSA;
* пара   закрытый ключ RSA (секретный ключ).

Шифрование и расшифрование

Сообщениями являются целые числа в интервале от 0 до n-1, т.е. . На рисунке 1 представлена схема алгоритма RSA.

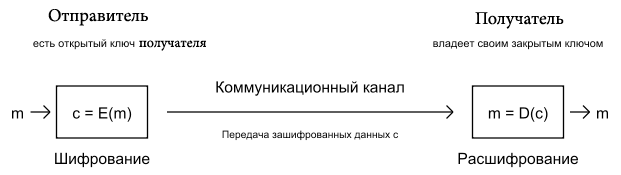


Рисунок 1 – Схема алгоритма RSA

Алгоритм Отправителя:

* взять открытый ключ (e,n) получателя;
* взять открытый текст m;
* зашифровать сообщение с использованием открытого ключа получателя:

Алгоритм Получателя:

* принять зашифрованное сообщение C;
* взять свой закрытый ключ (d,n);
* применить закрытый ключ для расшифрования сообщения:

Уравнения (1) и (2), на которых основана схема RSA, определяют взаимно обратные преобразования множества .

SMTP

SMTP (Simple Mail Transfer Protocol — простой протокол передачи почты) — это сетевой протокол, предназначенный для передачи электронной почты в сетях TCP/IP. ESMTP (англ. Extended SMTP) — масштабируемое расширение протокола SMTP. В настоящее время под «протоколом SMTP», как правило, подразумевают ESMTP и его расширения. SMTP использует порт TCP 25.

POP3

POP3 ( Post Office Protocol Version 3 — протокол почтового отделения, версия 3) — стандартный интернет-протокол прикладного уровня, используемый клиентами электронной почты для получения почты с удалённого сервера по TCP-соединению. POP3 использует порт 995, также известный как POP3S.

POP и IMAP (Internet Message Access Protocol) — наиболее распространённые интернет-протоколы для извлечения почты. Практически все современные клиенты и серверы электронной почты поддерживают оба стандарта. Протокол POP был разработан в нескольких версиях, нынешним стандартом является третья версия (POP3). Большинство поставщиков услуг электронной почты (такие как Hotmail, Gmail и Mail.ru) также поддерживает IMAP и POP3. Предыдущие версии протокола (POP, POP2) устарели.

ШИФРУЮЩЕЕ ПРИЛОЖЕНИЕ

На рисунке 2 представлен визуальный интерфейс приложения шифрации ассиметричного алгоритма шифрования RSA.

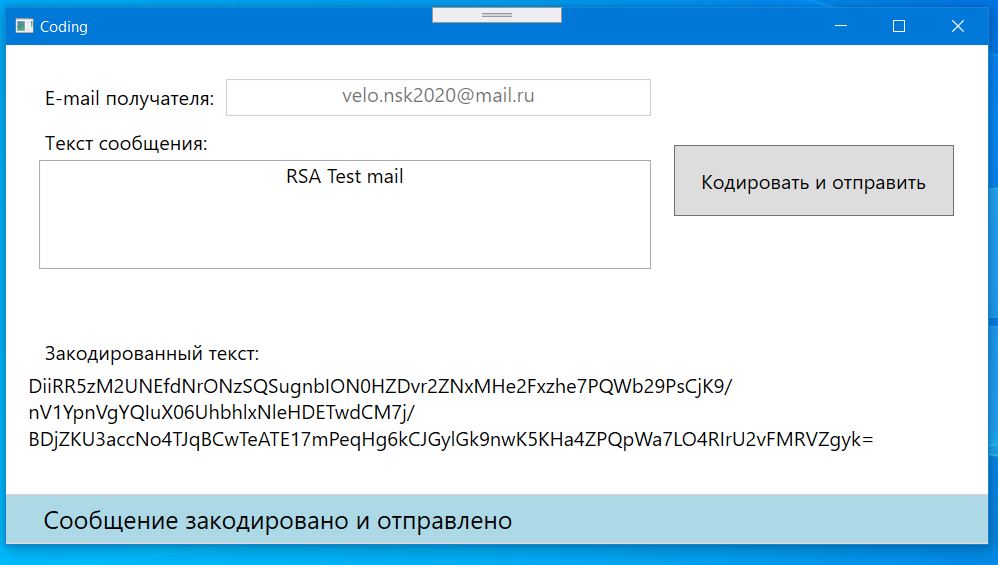


Рисунок 2 – Визуальный интерфейс приложения шифрования

Для реализации RSA шифрования в C# существует библиотеки: Cryptography и Cryptography.Xml. В данной библиотеке реализован класс RSACryptoServiceProvider, который позволяет произвести RSA шифрование. У класса RSACryptoServiceProvider есть метод FromXmlString, который возвращает строку XML, содержащую открытый и закрытый ключи текущего объекта RSA.

На рисунке 3 изображен код функции Encryption. Данная функция шифрует полученные данные при помощи ассиметричного RSA шифрования.



Рисунок 3 – Функция Encryption

На рисунке 4 изображен код функции SendEmail. Данная функция необходима для отправки зашифрованных сообщений на почту заданного пользователя, используется протокол SMTP.



Рисунок 4 – Функция SendEmail

ДЕШИФРУЮЩЕЕ ПРИЛОЖЕНИЕ

На рисунке 5 представлен визуальный интерфейс приложения дешифрации ассиметричного алгоритма шифрования RSA.

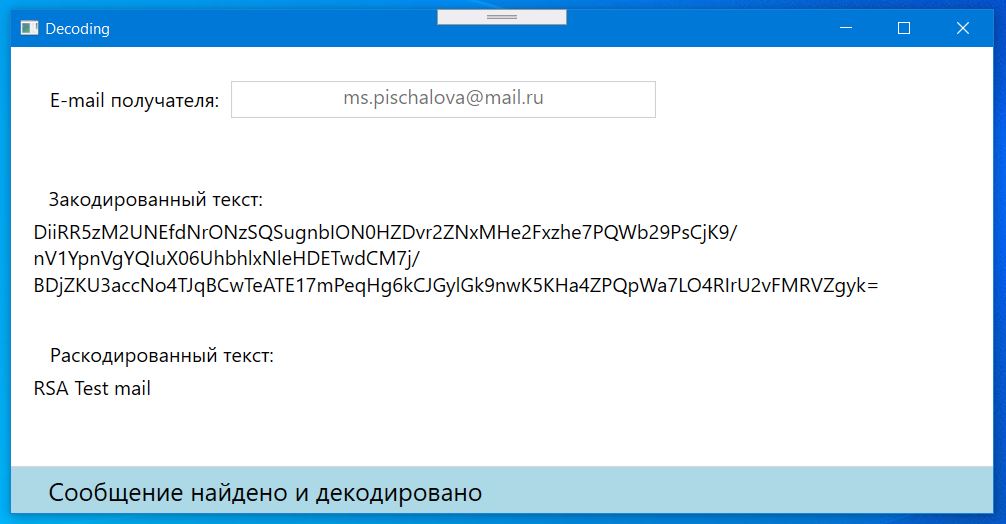


Рисунок 5 – Визуальный интерфейс приложения дешифрации

На рисунке 6 представлен код функции Decryption. Данная функция дешифрует полученные данные при помощи ассиметричного RSA шифрования.



Рисунок 6 – Функция Decryption

На рисунке 7 изображен код функции Get\_Mail. В данной функции при помощи протокола POP3 получаются сообщения из почты. После чего обрабатывается условие на поиск почты заданного пользователя и темы письма. Если оба условия поиска положительны, то письмо считывается с почты и декодируется при помощи функции Decryption.



Рисунок 7 – Функция Decryption

ВЫВОД

Были разработаны шифрующая и дешифрующая программы, использующие ассиметричное RSA шифрование, отправляющие и принимающие зашифрованную информацию по почте.

В ходе работы использовались:

* + алгоритм асимметричного шифрования RSA;
* протокол передачи почты Smtp и функции библиотеки Net.Mail;
* протокол получения почты Pop3 и функции библиотеки OpenPop.NET.

В ходе практической работы были получены знания и навыки ассиметричного шифрования, а так же работы с Smtp и Pop3 протоколами.