Лабораторная работа по криптографии №1

Алгоритм RSA

Автор: Гашков С.П., гр.22305

22.02.2024

1. Формулировка задания

Вариант 1.7.

Напишите программу формирования цифровой подписи алгоритмом RSA. Рекомендуется

использовать библиотеку для работы с длинными числами. В случае применения этой

библиотеки разрешается использовать функции сложения, вычитания, умножения,

целочисленного деления, вычисления остатка от деления. Функции возведения числа в

степень, нахождения наибольшего общего делителя, обратного элемента в

мультипликативной группе вычетов, генерации простого числа реализовать

самостоятельно. Для ускорения вычислений использовать китайскую теорему об остатках.

Выполняемые функции программы:

1. генерация пары открытый/закрытый ключ, число e должно генерироваться после вычисления p и q;
2. получения цифровой подписи для сообщения (целого числа);
3. проверки цифровой подписи для данного сообщения (целого числа).
4. Описание метода решения

***Алгоритм:***  
1. Выбрать два больших простых числа p и q, не равных друг другу

2. Криптомодуль n = p \* q

3. Функция Эйлера: φ(n) = (p − 1)(q − 1).

4. Подбираем небольшое нечётное e, взаимно простое с φ(n),

5. .

6. Открытый ключ - пара (e, n).

7. Закрытый ключ – пара (d, n).

***Использование алгоритма:***

Шифровка сообщения M (M - число):

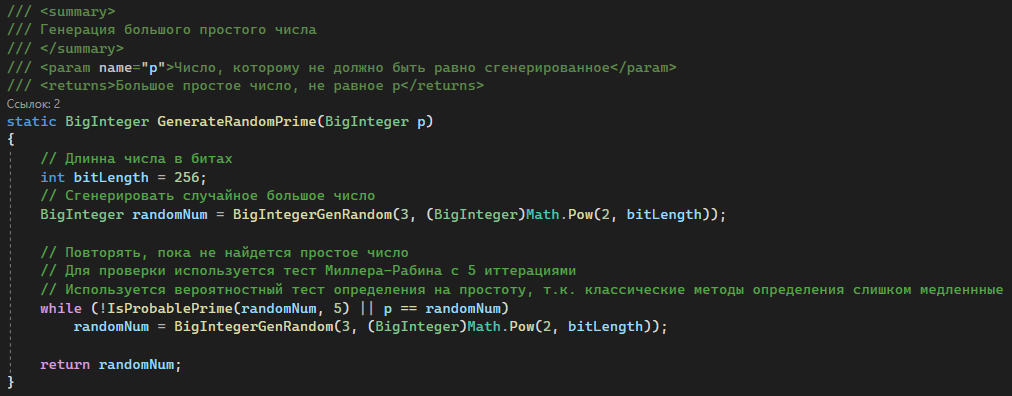
Дешифровка сообщения C:

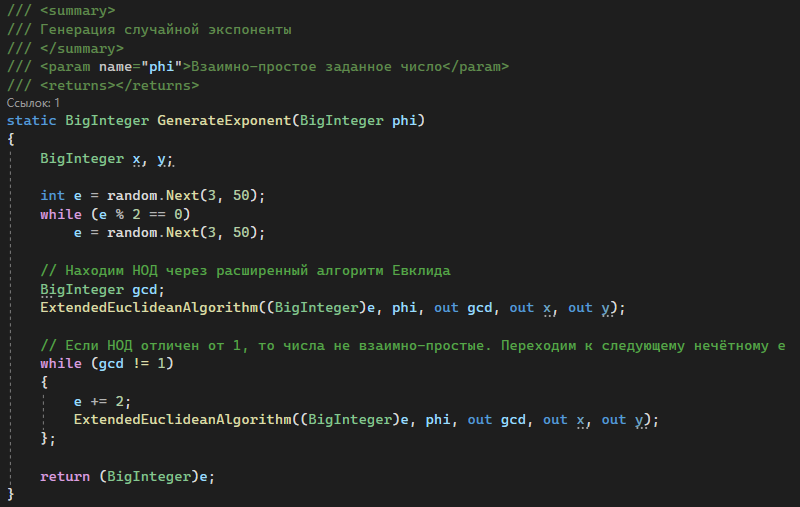
Для добавления к сообщению M цифровой подписи:

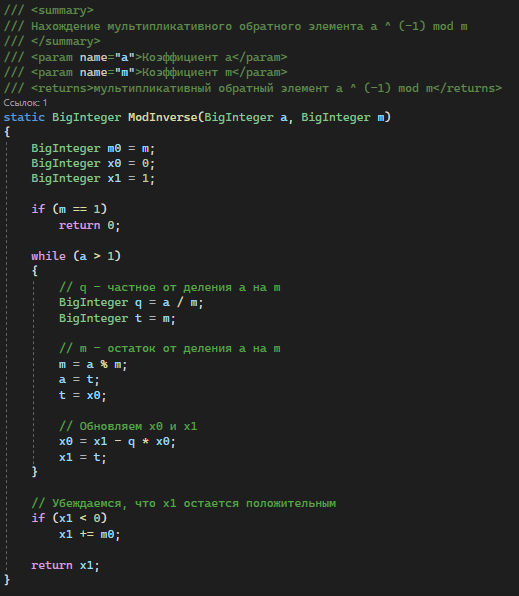
Для проверки цифровой подписи σ:

Если M = M’, то подпись верна.

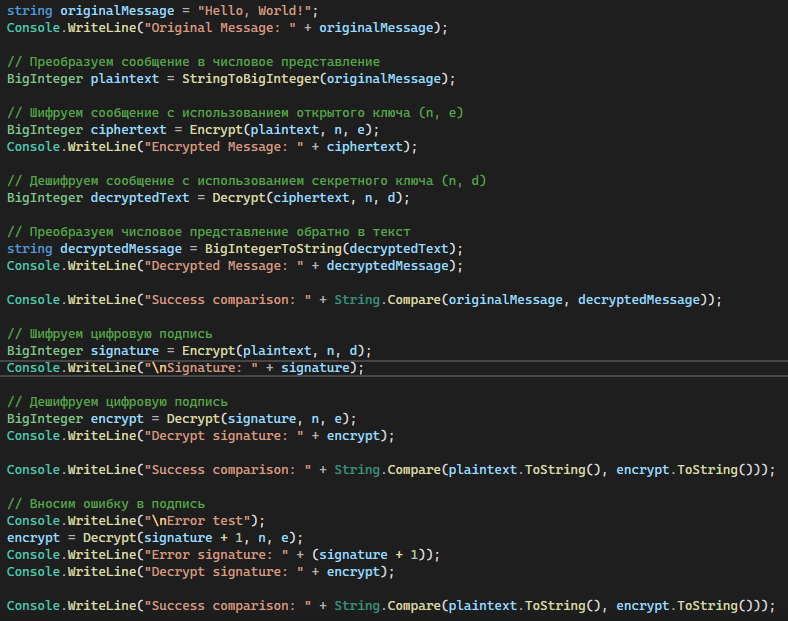
1. Примеры кода







1. Тестовые данные
   1. Шифровка/дешифровка строки – позитивный тест
   2. Получение подписи/проверка подписи – позитивный тест
   3. Проверка заведомо неправильной подписи – негативный тест



1. Ссылка на репозиторий

<https://github.com/Nemo121007/cryptography.git>