Министерство образования Республики Беларусь

Учреждение образования

“Белорусский государственный университет

информатики и радиоэлектроники”

ЛАБОРАТОРНАЯ РАБОТА 5

по дисциплине

«Средства и методы защиты информации в интеллектуальных системах»

Выполнил :

 Войткус С. А.

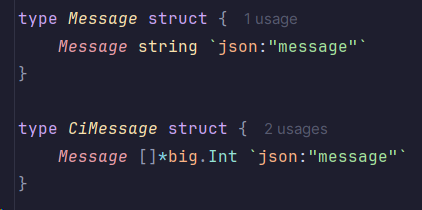
студент гр. 121703

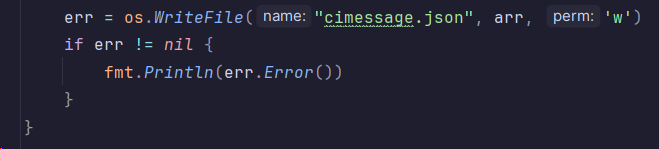
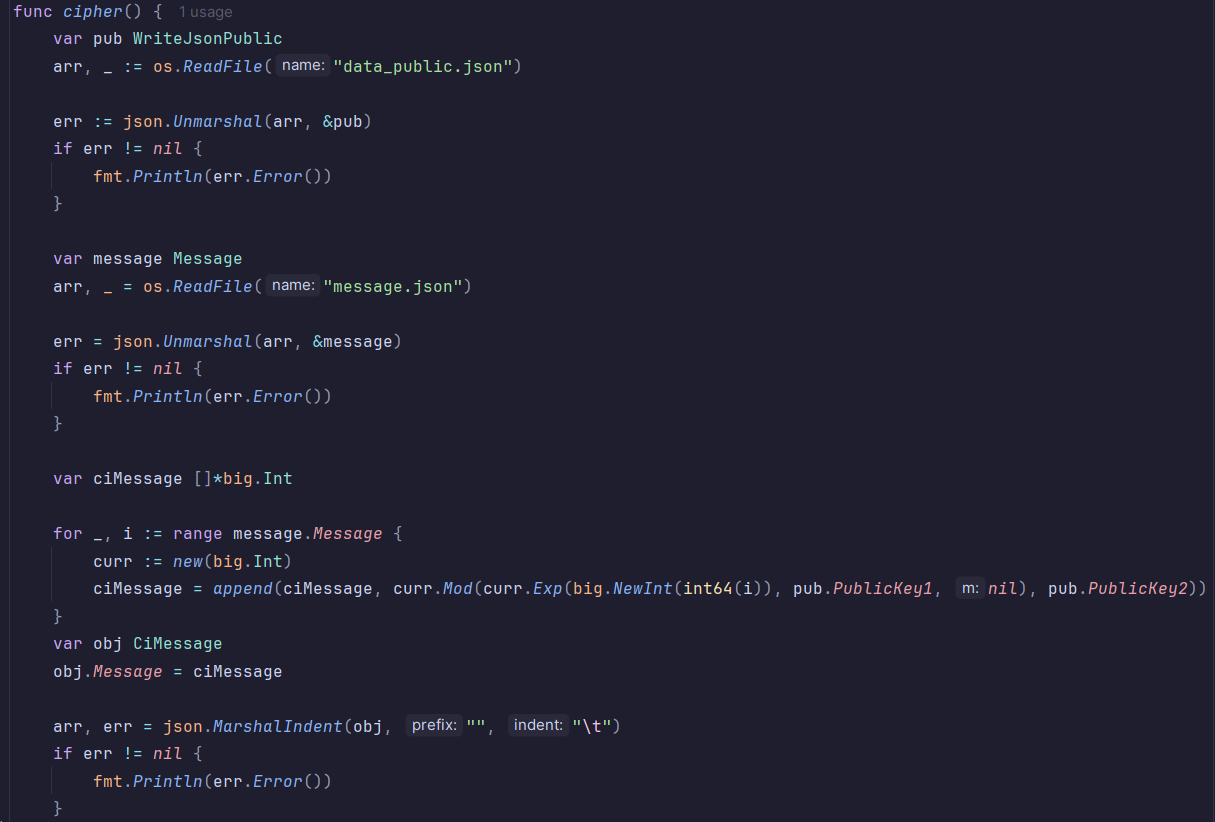
Проверил

Захаров В. В.

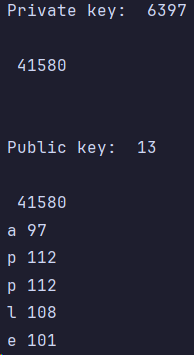
Минск 2023

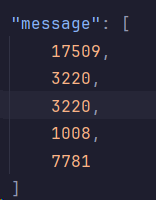














Разработать программное обеспечение, реализующее функции генерации секретного и открытого ключей, шифрования и цифровой подписи для алгоритма RSA.

Вывод:

При шифровании алгоритмом RSA необходимо сгенерировать открытый и приватный ключ. Для этого выбирают два очень больших простых числа. По условию данной лабораторной работы необходимо было взять эти числа не менее 1024 бит. Это значит, что это число может иметь 2^1024 занчений. Один из самых мощных суперкомпьютеров имеет вычислительную мощность 1,1 пфлопс/c (10^15). Значит 2^1024/1.1\*10^15 = 1,797693134862315907729305190789e+308 / 1.1\*10^15 = 5,1822250324659722445035549293996e+285 лет. Это если обычным перебором. Значит, чем больше изначальные p и q, тем дольше будет перебор пароля. Также