**ЛАБОРАТОРНАЯ РАБОТА 6**

**КРАЖЕВСКИЙ АЛЕКСЕЙ ИГОРЕВИЧ, 15 ГРУППА**

**ВАРИАНТ 8**

*Условие варианта:*



Для выполнения всех заданий необходимо

использовать "длинную" арифметику. Разрешается использовать любую готовую библиотеку или написать свою.

Шаг 1. В условиях своего варианта для заданного числа q (см. Таблица 1)

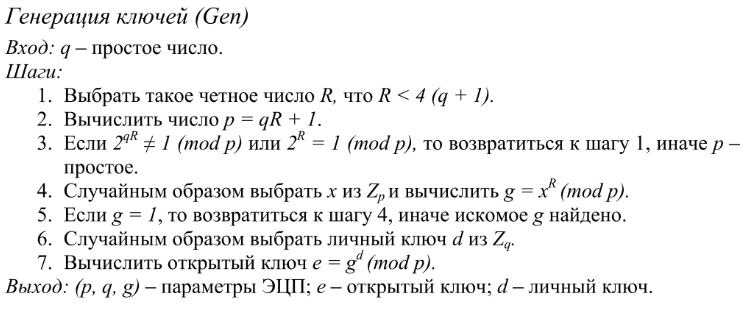
необходимо выполнить алгоритм Gen.

Шаг 2. Для параметров, полученных на шаге 1, и сообщения вида «Я, Иван Иванов, люблю КМ», где «Иван Иванов» – ваше имя и фамилия соответственно, выполнить алгоритм Sign.

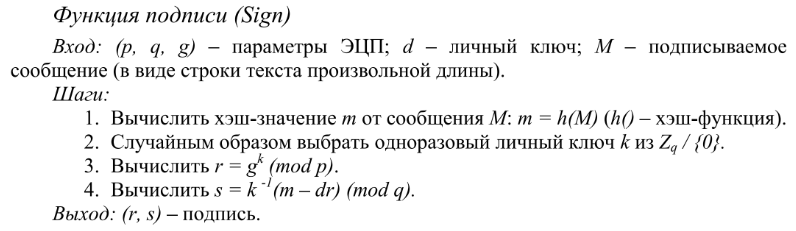
Шаг 3. Проверьте результаты подписи из Шага 2, выполнив алгоритм Verify.

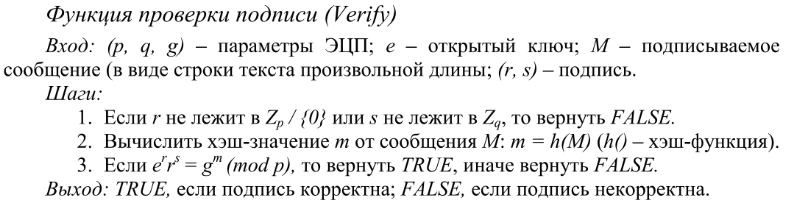
*Выполнение задания:*

В процессе выполнения задания я написал функцию генерации ключа по указанному алгоритму



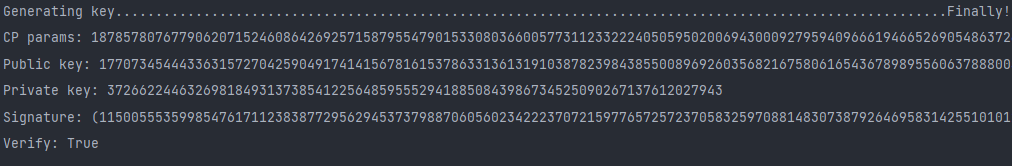
Также были написаны функции подписи и проверки подписи по следующим алгоритмам:





Также я написал хеш-функцию SHA-256. Алгоритм написал по псевдокоду из википедии: <https://en.wikipedia.org/wiki/SHA-2>

Окно вывода программы:



В скриншот не влезают все числа

Пример полученных данных:

P=1878578076779062071524608642692571587955479015330803660057731123322240505950200694300092795940966619466526905486372603733185141516636023926443133032183961

Q=70632854428090245668612719837589154263674140045063326147121864128289640672721

G=1326659204601545475520037777828939094269238714579954438216621929415064518417595205165605043860003548076224970120325838941611578770528252145237512488482460

PublicKey=1770734544433631572704259049174141567816153786331361319103878239843855008969260356821675806165436789895560637888003453697440426874012412988278137603162172

PrivateKey=37266224463269818493137385412256485955529418850843986734525090267137612027943

Signature:

R=1150055535998547617112383877295629453737988706056023422237072159776572572370583259708814830738792646958314255101011498696337504323043346880440017981922923

S=54705179457042421593327904459143145618273213694772009965433407731936416880002

Как видно по выводу, такие данные прошли верификацию, хотя наглядными их нельзя назвать…

Для возведения в степень я использовал алгоритм бинарного возведения в степень из предыдущей лабораторной, как и расширенный алгоритм Евклида для поиска обратного элемента.