**Ministerul Educaţiei Tineretului şi Sportului al Republicii Moldova**

**Universitatea Tehnică a Moldovei**

**RAPORT**

**LA CRIPTOGRAFIE**

Tema: Funcții Hash și semnături digitale

Lucrarea de Laborator nr. 6

A efectuat Studentul grupei \_SI-212\_\_

\_\_\_\_\_\_Vozian Vladimir\_\_\_\_

A verificat Andronatiev Victor

**Chisinău 2022**

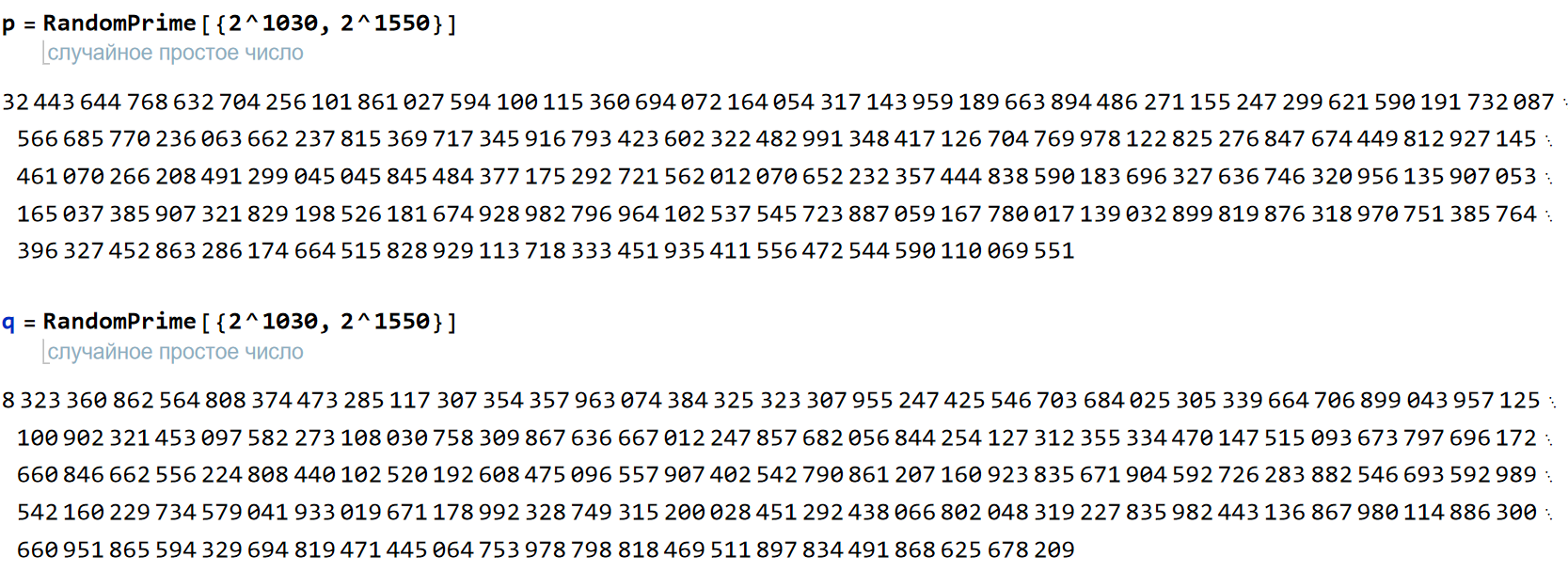
**Sarcina 1**

**RSA**

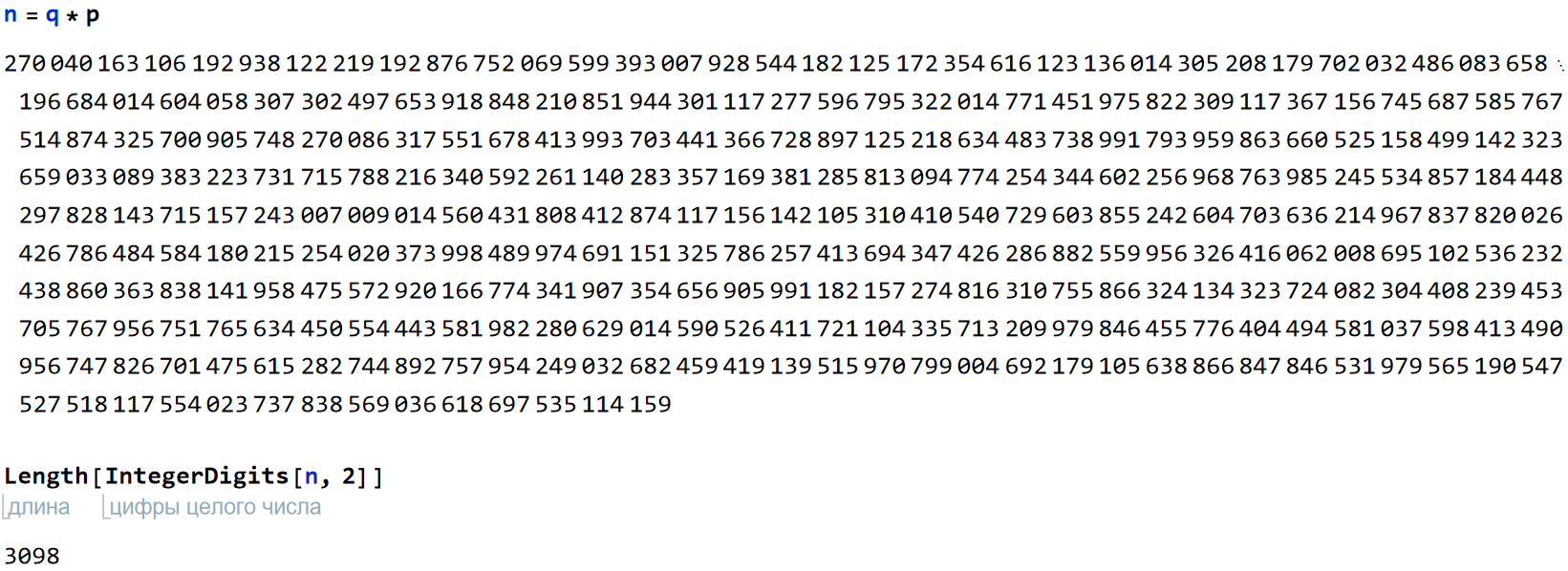
## 

## 

Alegem numerele prime mari p și q

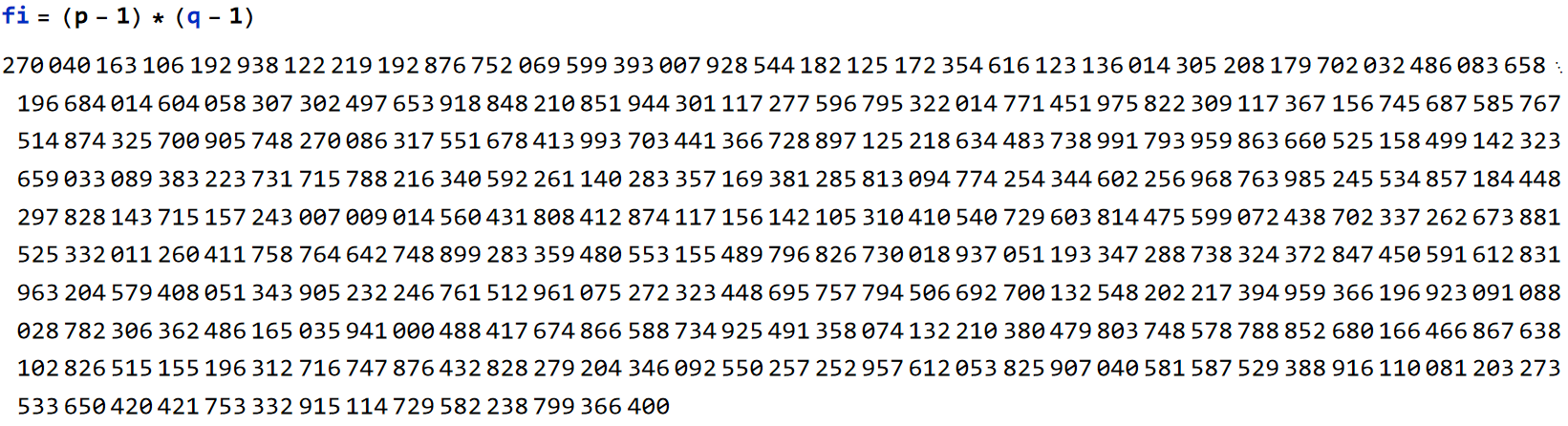


Primim numarul n conform produsului p\*q.

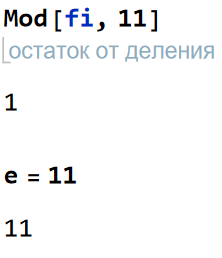


Vedem ca n are lungimea corectă conform cerinței.

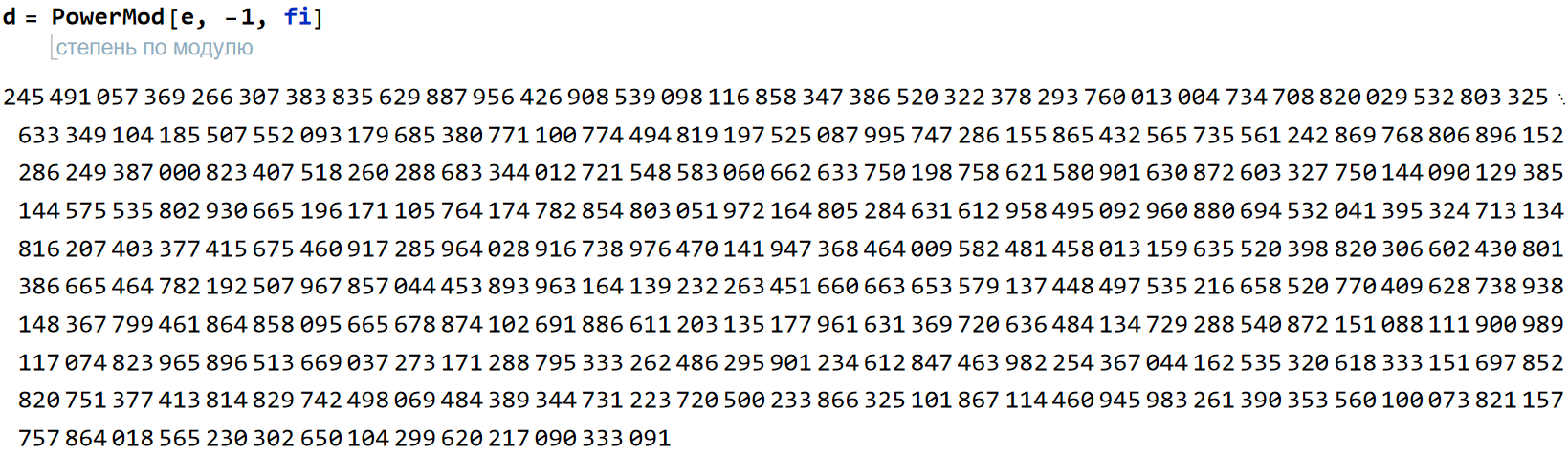
Calculam fi(n)



Alegem un numar mic e la care divizorul comun cel mai mare cu fi sa fie 1.

Sa luat ca numar mic prim e=11 si vedem ca fi nu se divide la e;

Aflăm cheia privată d fiind e^-1 mod fi(n)



Deci Mesajul din laboratorul 2 este:

**england, too, had its black chamber. it began with the cryptanalyticendeavors of john wallis, the greatest english mathematician beforenewton. after his death, it descended through his grandson to reach, onmay 14, 1716, edward willes, a 22-year-old minister at oriel college,oxford.willes embarked at once upon a career unique in the annals ofcryptology and the church. he not only managed to reconcile hisreligious calling with an activity once condemned by churchlyauthorities, but also went on to become the only man in history to usecryptanalytic talents to procure ecclesiastical rewards. within two years,he had been named rector of barton, bedfordshire, for solving more than300 pages of cipher that exposed sweden's attempt to foment an uprising in england. he virtually guaranteed hisfuture when he testified before the house of lords in 1723. here, francisatterbury, bishop of rochester, was being tried by his peers forattempting to set a pretender on the english throne.the**

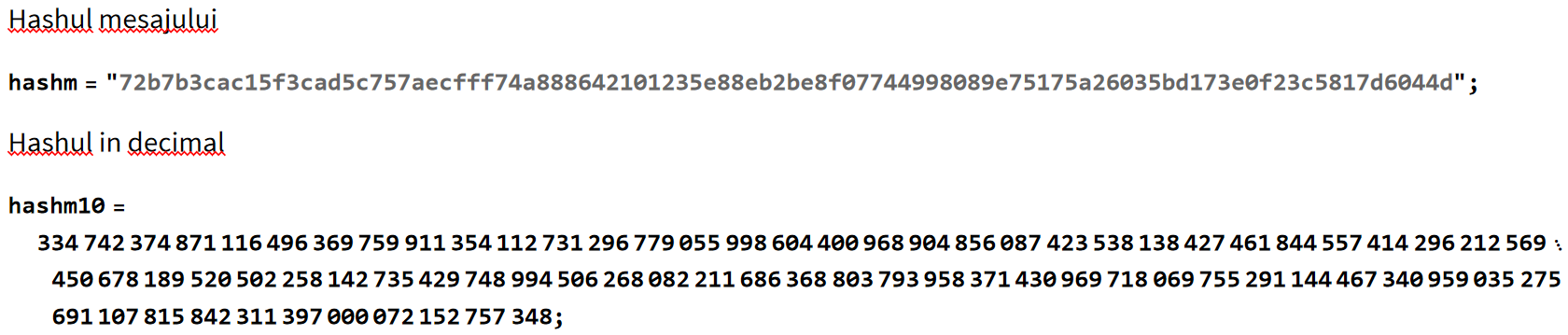
**pretender's cause exhorted the allegiance of many in england,and the nation's attention**

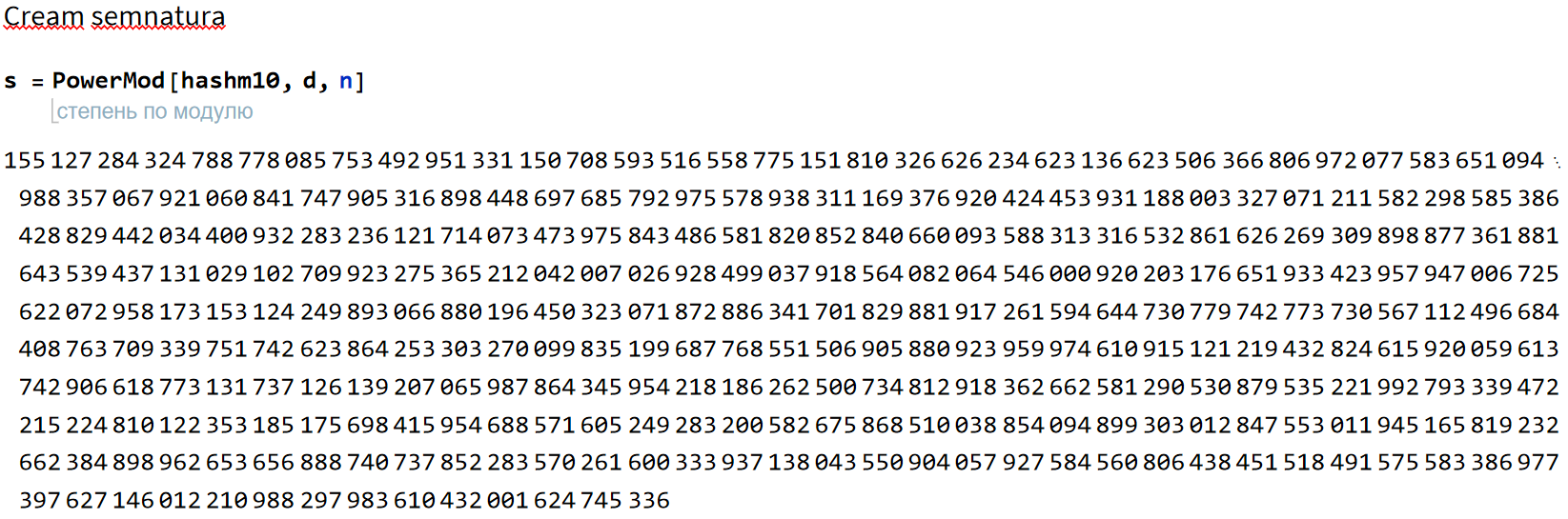
**focused on atterbury's trial. most of the factsabout the alleged conspiracy had come from his interceptedcorrespondence, and the most inculpatory evidence had been extractedfrom the portions in cipher by willes and by anthony corbiere, a formerforeign service official in his mid-thirties who had also been appointed adecypherer in 1719. the lords "thought it proper to call the decypherersbefore them, in order to their being satisfied of the truth of thedecyphering." to demonstrate this, willes and corbiere deposed, that several letters, written in this cypher, had beendecyphered by them separately, one being many miles distant inthe country, and the other in town; and yet their decypheringagreed;that facts, unknown to them and the government at the timeof their decyphering, had been verified in every circumstance bysubsequent discoveries that a supplement of this cypher, having been**

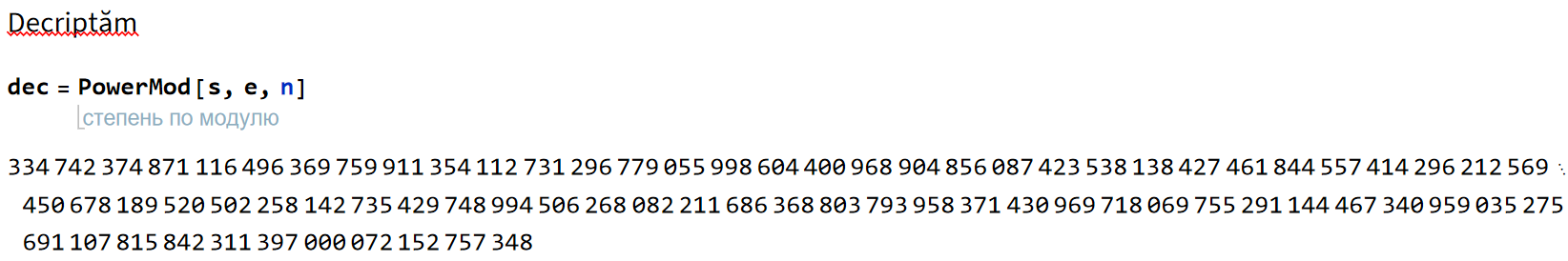
**found amongdennis kelly's papers the latter end of july, agreed with the keythey had formed of that cypher the april before;that the decyphering of the letters signed jones**

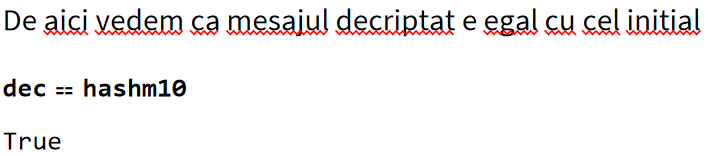
**lllington and1378, being afterwards applied by them to others written in thesame cypher, did immediately make pertinent sense, and such ashad an evident connexion and coherence with the parts of thoseletters that were out of cypher, though the words in cypher wererepeated in different paragraphs, and differently combined. the two decypherers appeared before the lords on several occasionsto swear to their solutions. attenbury twice objected and was twice overruled. but on may 7, as willes wastestifying to the cryptanalysis of the three most incriminatory letters ofall, and the bishop felt the noose tightening around him, he persisted inquestioning willes on the validity of the reading though the house hadsupported willes' refusal to answer. he raised such a commotion that heand his counsel were ordered to withdraw, and the lords voted upon theproposition, "that it is the opinion of this house that it is not consistentwith the public safety, to ask the decypherers any questions, which maytend to discover the art or mystery of decyphering." it was resolved inthe affirmative, the solutions were accepted, and atterbury, largely onthis evidence, was found guilty, deprived of office, and banished from therealm.**

Deci primim hashul mesajului conform algoritmului după variantă:





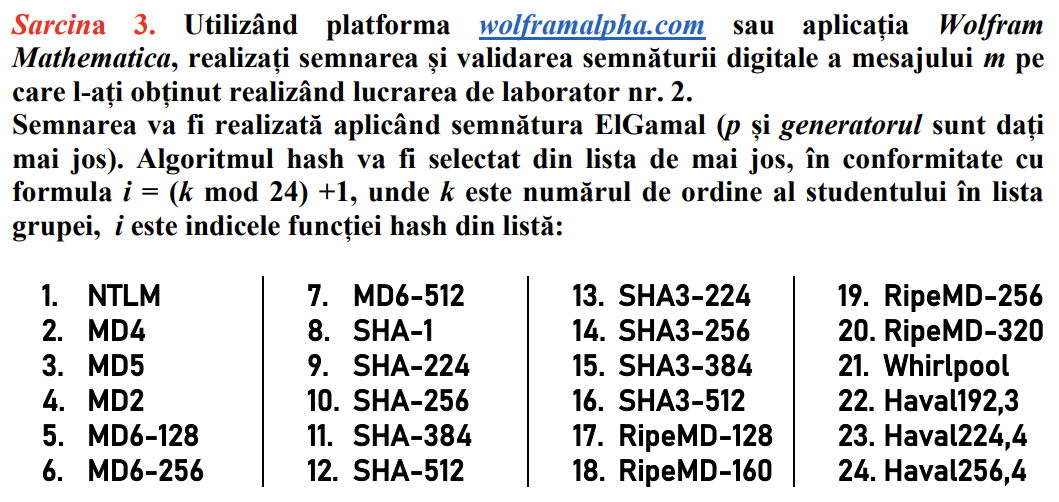


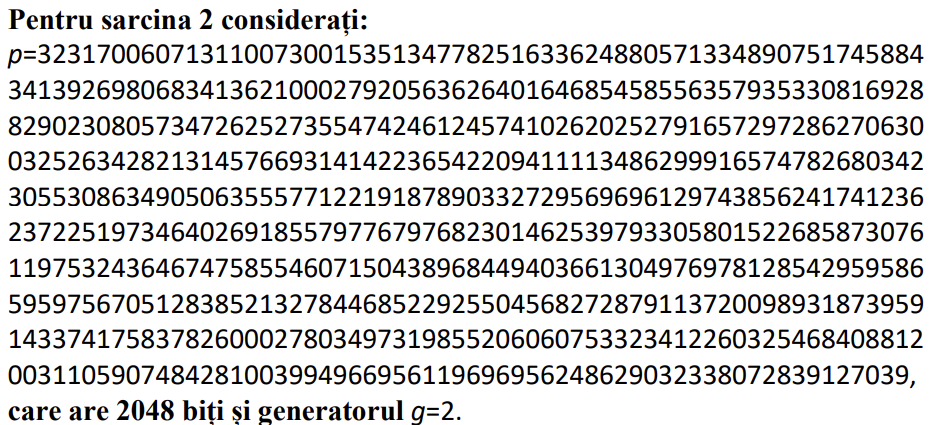


Deci algoritmul e efectuat corect.

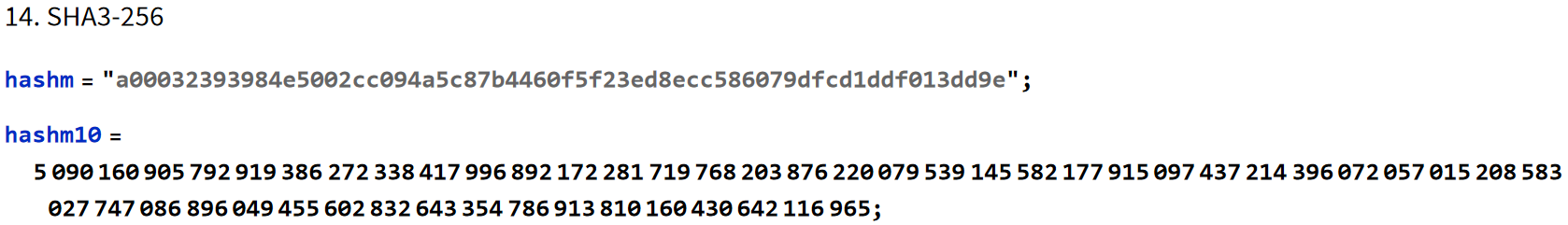
**Sarcina 2**

**ElGamal**

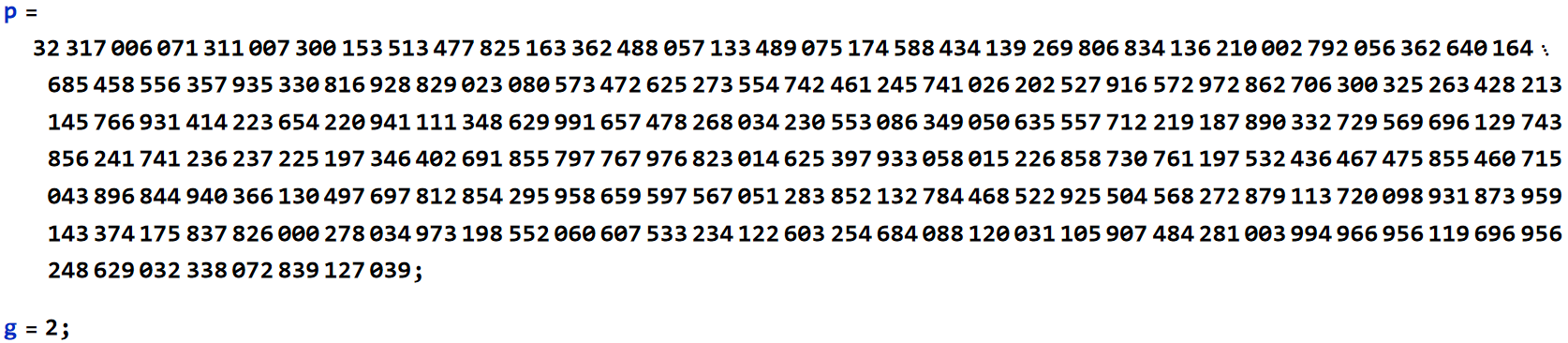


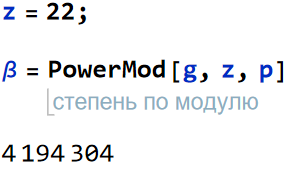


Deci conform variantei 14 aflăm hashul la mesajul nostru conform algoritmului:

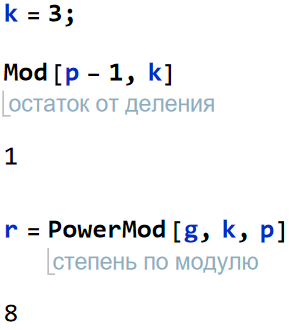


Introducem numarul p si generatorul:

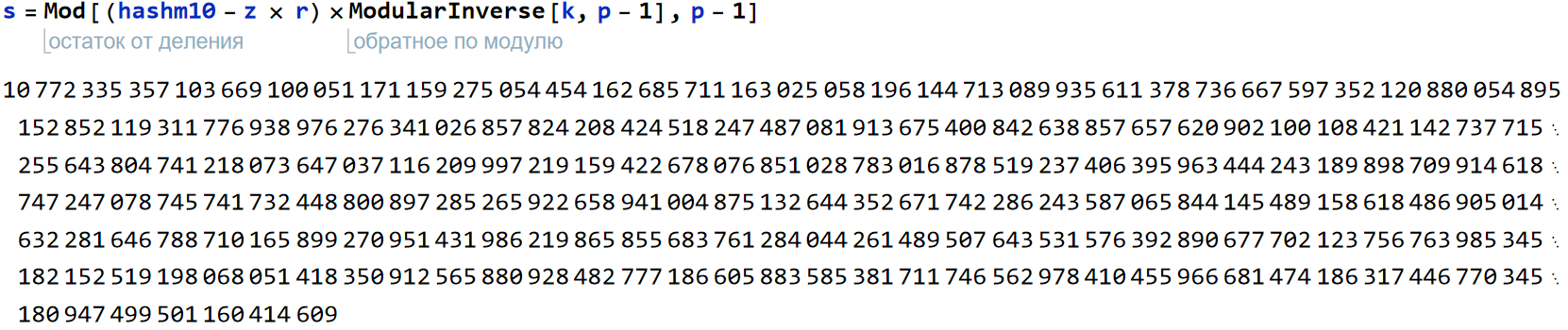


Apoi conform algoritmului alegem un numar random secret z, și aflam β(beta) Sa luat z ca 22;

Apoi alegem un numar k care are 1 ca cel mai mic divizor comun cu p-1, și aflam r.

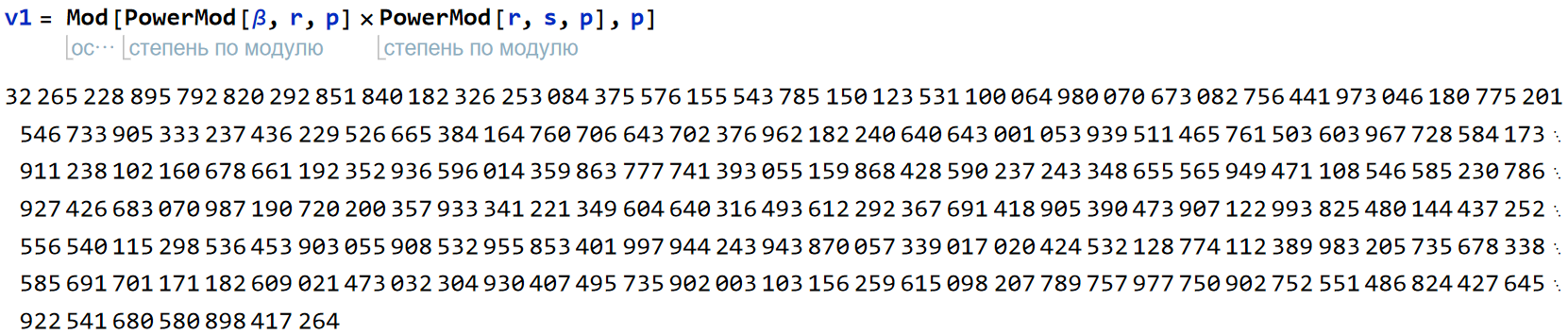


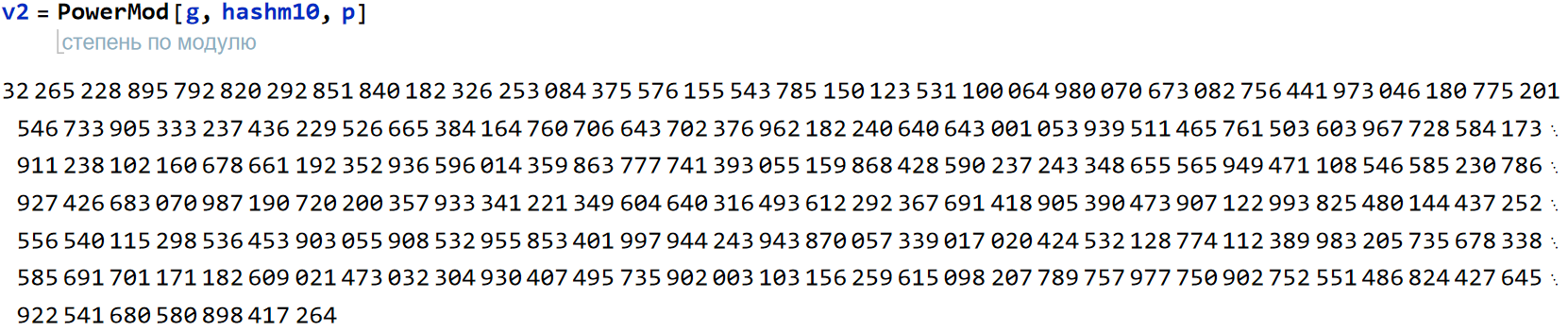
Generăm semnătura:



Deci semnătura o reprezintă tripletul (m, r, s)

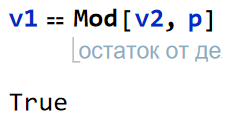
În final verificăm validatea semnăturii:





Am calculat v1 și v2

Și pentru a verifica validatea semnăturii trebuie să fie respectată egalitatea:



Deci vedem ca ele sunt egale și în rezultat algoritmul e efectuat corect.

**Concluzii:**

Am efectuat lucrarea de laborator in baza funcțiilor hash și cu semnăturile digitale, am exersat și am înțeles bazele principiilor lucrului semnăturilor digitale, algoritmul RSA și deja semnatura digitală cu ElGamal.