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

**Universitatea Tehnică a Moldovei**

**RAPORT**

**LA CRIPTOGRAFIE**

Tema: Criptografia cu chei publice

Lucrarea de Laborator nr. 5

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

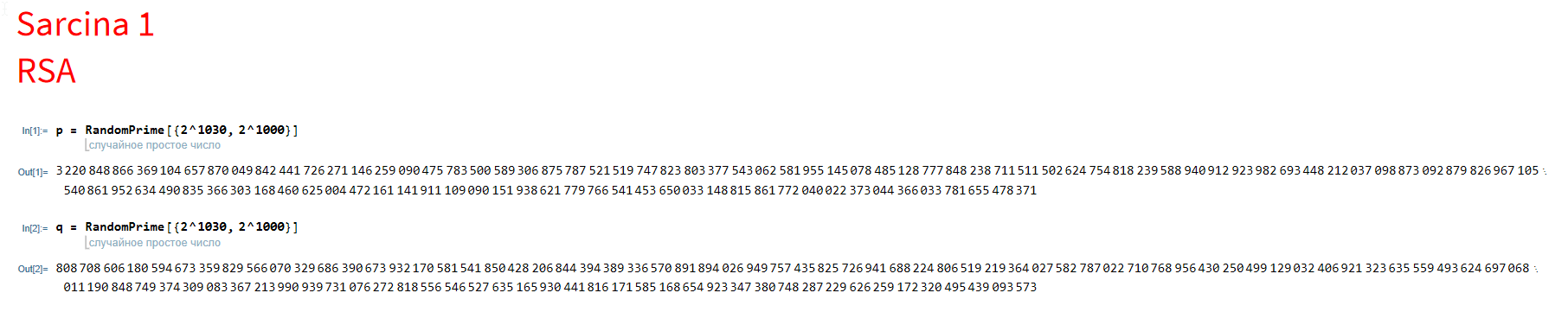
\_\_\_\_\_\_Vozian Vladimir\_\_\_\_

A verificat Andronatiev Victor

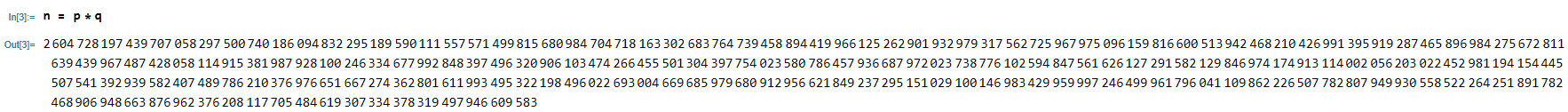
**Chisinău 2022**

## 

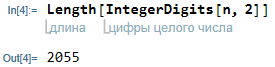
Alegem numerele prime mari p și q



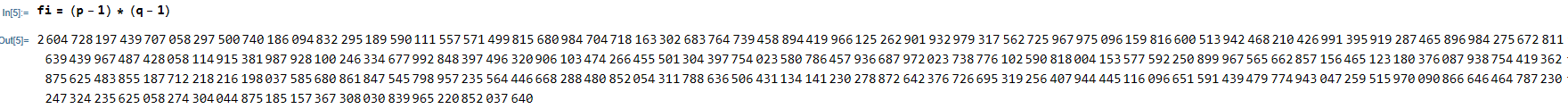
Formăm n conform produsului numerelor prime p,q



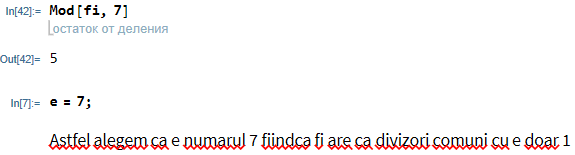
Verificăm lungimea lui n conform cerinței

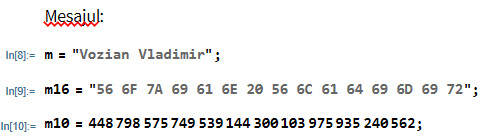


Calculăm fi(n) după formula (p-1)(q-1)

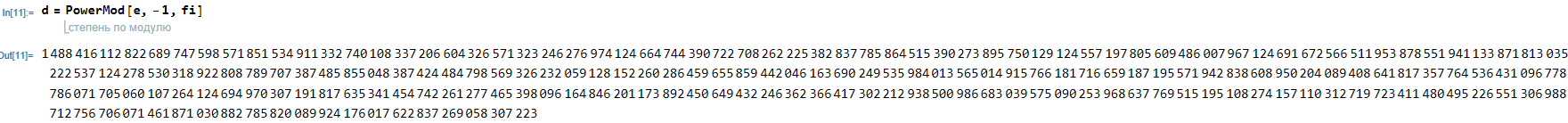


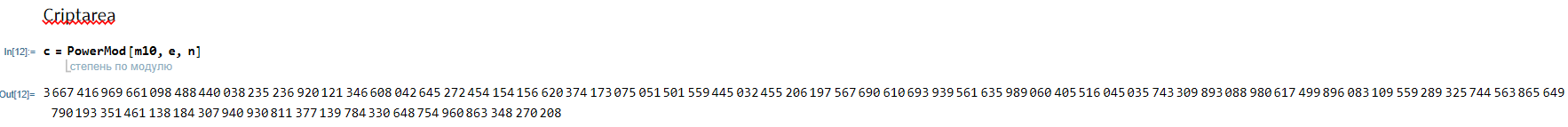
Pentru a alege nr e, ce trebuia să nu aibă divizori comuni cu fi(n), luăm e ca cel mai mic număr care nu este divizor a lui fi(n)

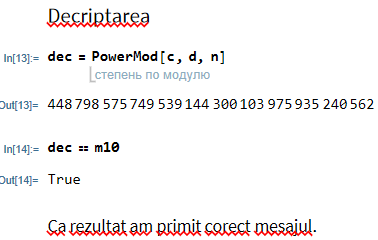




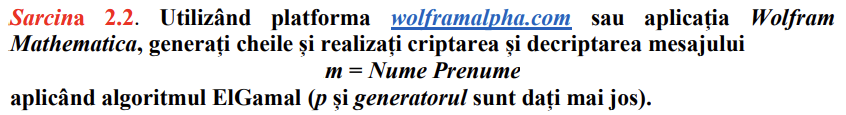
Formăm cheia privată d conform formulei







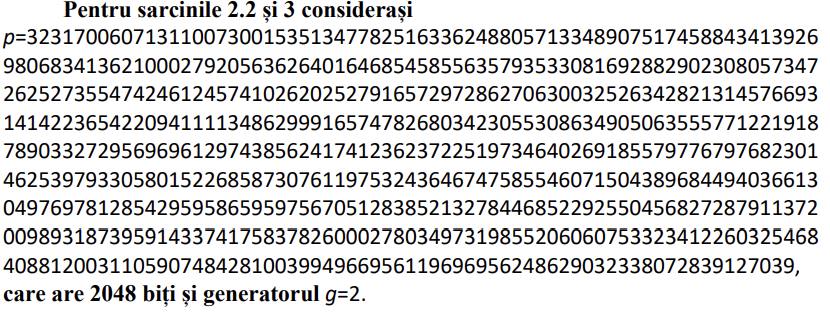
Deci mesajul sa primit corect și după decriptare și algoritmul este efectuat corect.



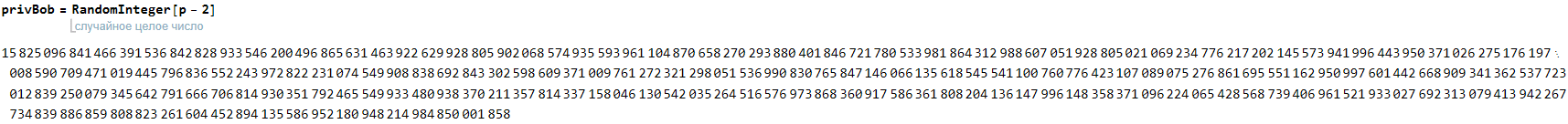
Sarcina 2

ElGamal

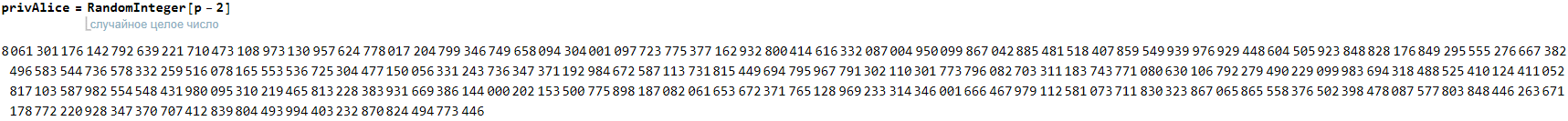
Primim p și generatorul ce este dat în sarcina



Formăm cheia privată lui Bob prin generarea unui număr random din p-2

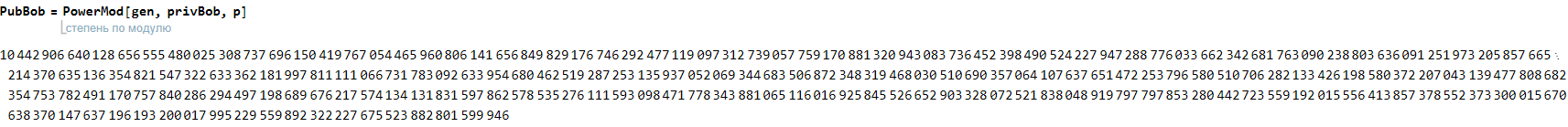


Formăm cheia privată lui Alice prin generarea unui număr random din p-2



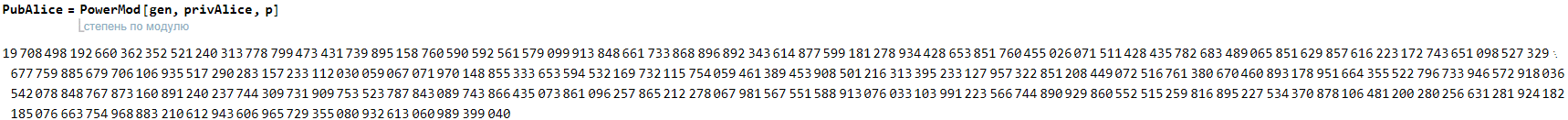
Formăm cheia publică lui Bob prin PowerMod din generator la puterea cheii lui private din p



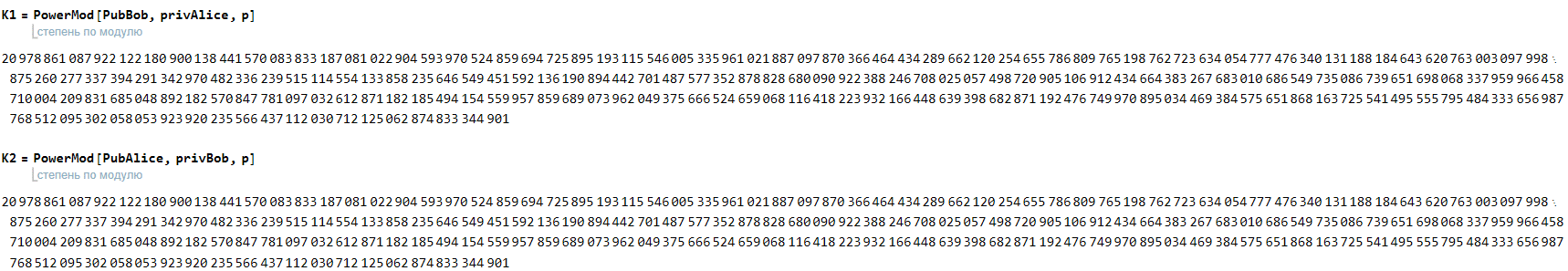


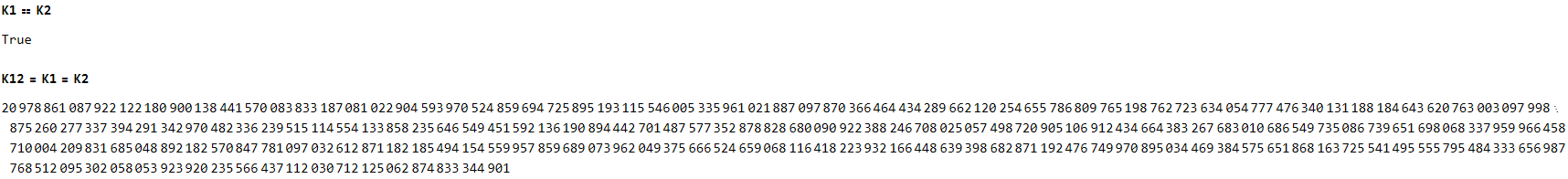
Formăm cheia publica lui Alice prin PowerMod din generator la puterea cheii ei private din p



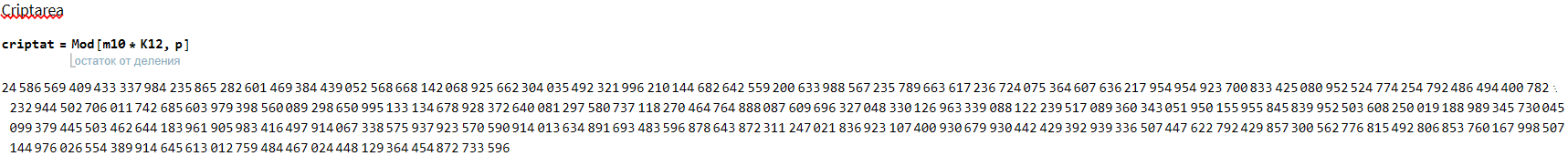


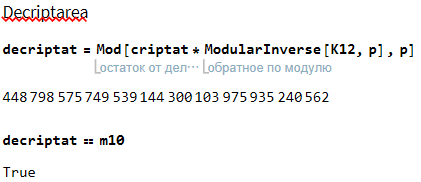
Sa efectuat schimbul de chei dintre Bob si Alice, la rândul său ei decripteaza cheia celuilalt prin cheia lor privată



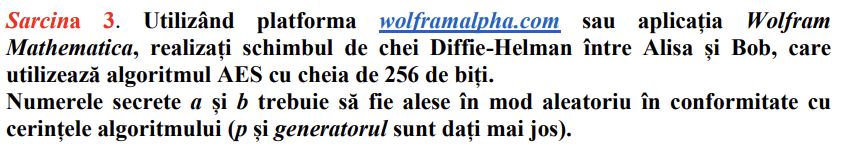


Deci amândoi au primit aceeasi cheie, ce inseamnă că algoritmul până la momentul dat e efectuat corect.





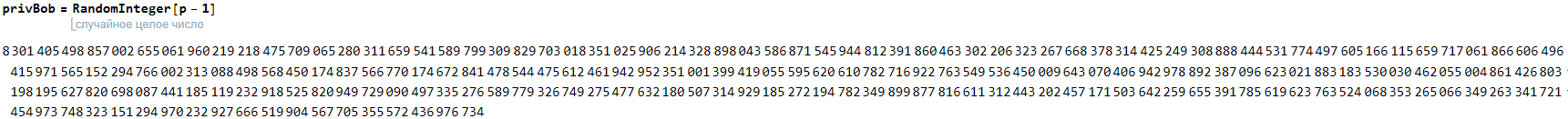
Deci mesajul sa primit corect și dupa decriptare, și algoritmul este efectuat corect.



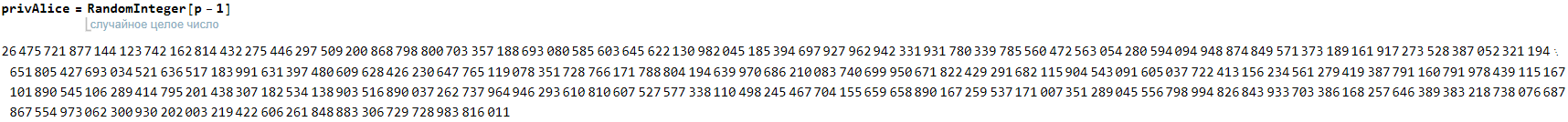
Sarcina 3

Diffie-Hellman

Formăm cheia privată lui Bob prin generarea unui număr random din deja p-1

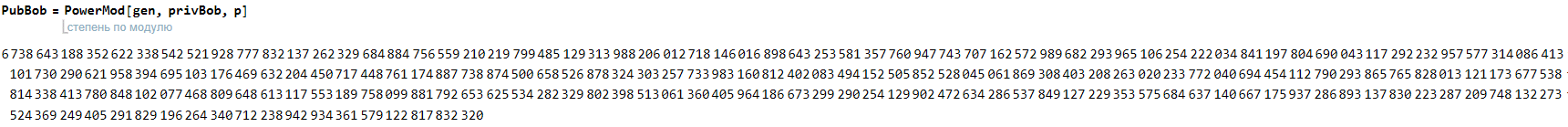


Formăm cheia privată lui Alice prin generarea unui număr random din la fel p-1



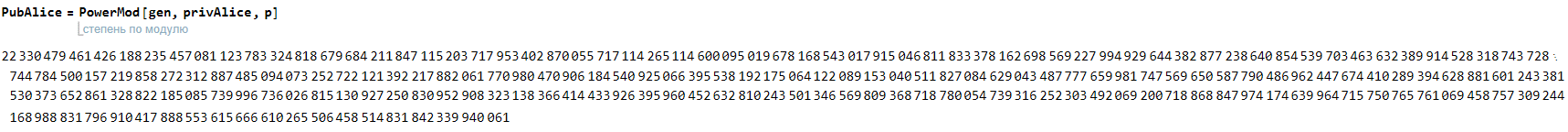
Formăm cheia publică lui Bob prin PowerMod din generator la puterea cheii lui private din p



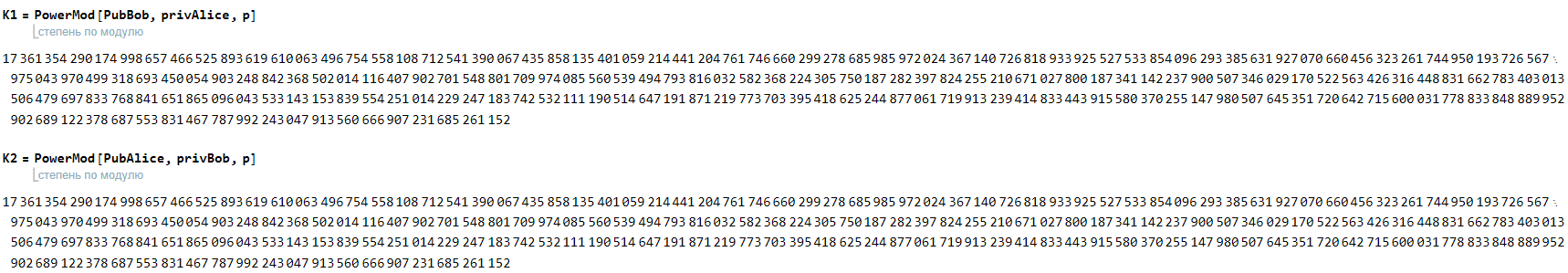


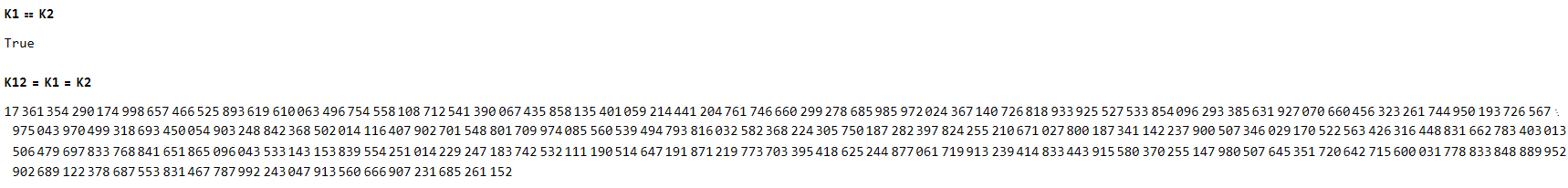
Formăm cheia publică lui Alice prin PowerMod din generator la puterea cheii ei private din p



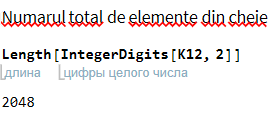


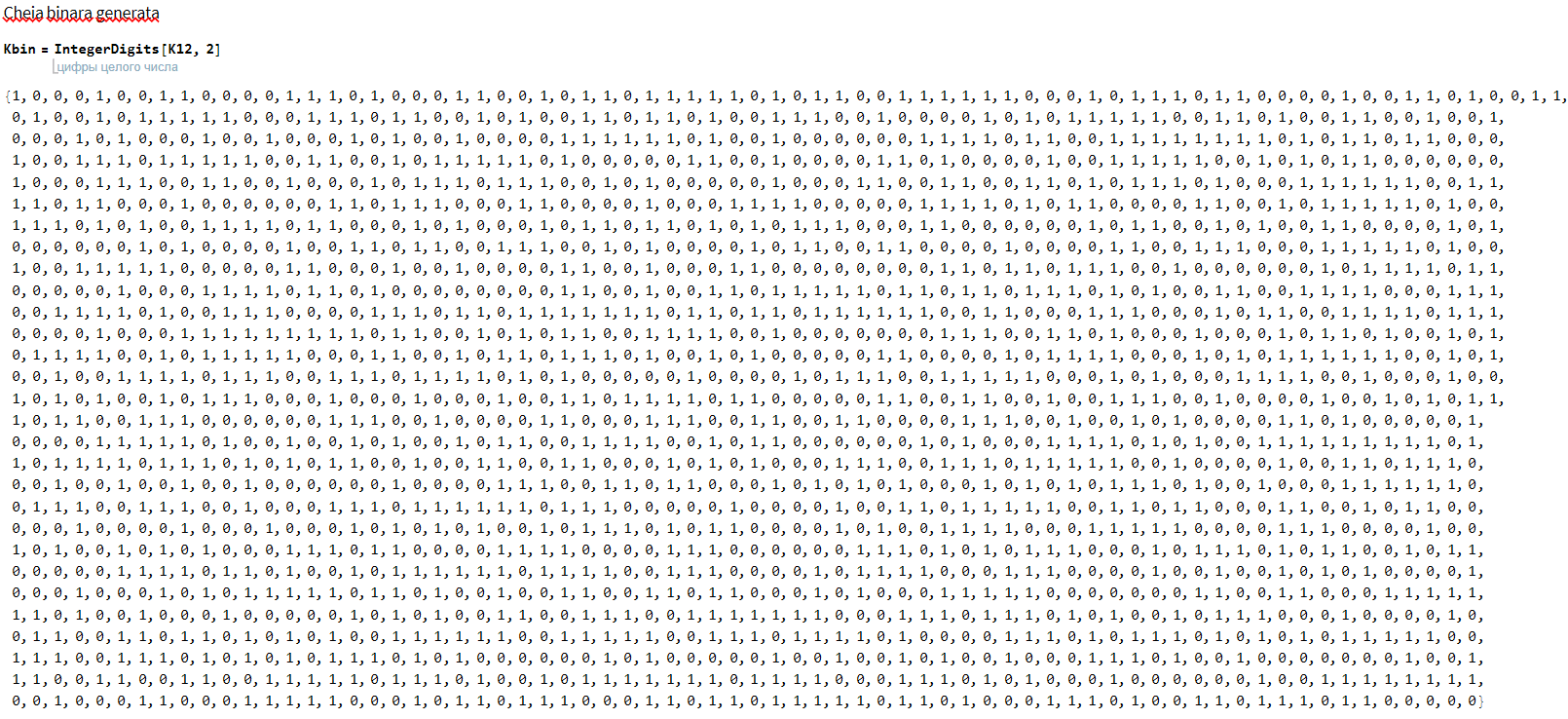
Sa efectuat schimbul de chei dintre Bob si Alice, la rândul său ei decriptează cheia celuilalt prin cheia lor privată



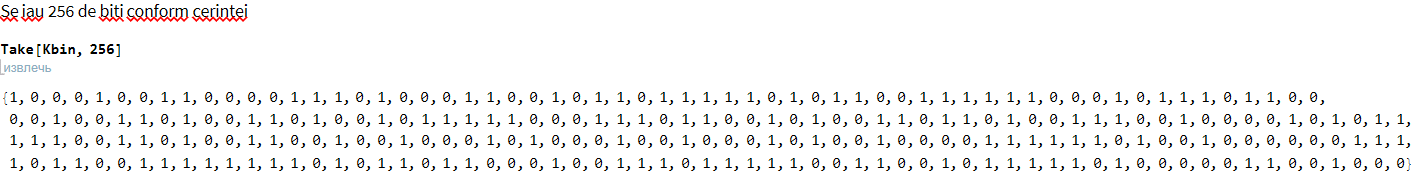


Deci amândoi au primit aceeași cheie, ce inseamnă că algoritmul până la momentul dat e efectuat corect.





Sa generat cheia binară din cheia finală primita de Bob si Alice



Conform algoritmului AES se iau 256 de biți din cheia binară

**Concluzii:**

Am efectuat lucrarea de laborator in baza criptării asimetrice cu cheile publice și private, lucrând asupra algoritmilor RSA, și Diffie-Hellman/ElGamal care sunt foarte asemănătoare.