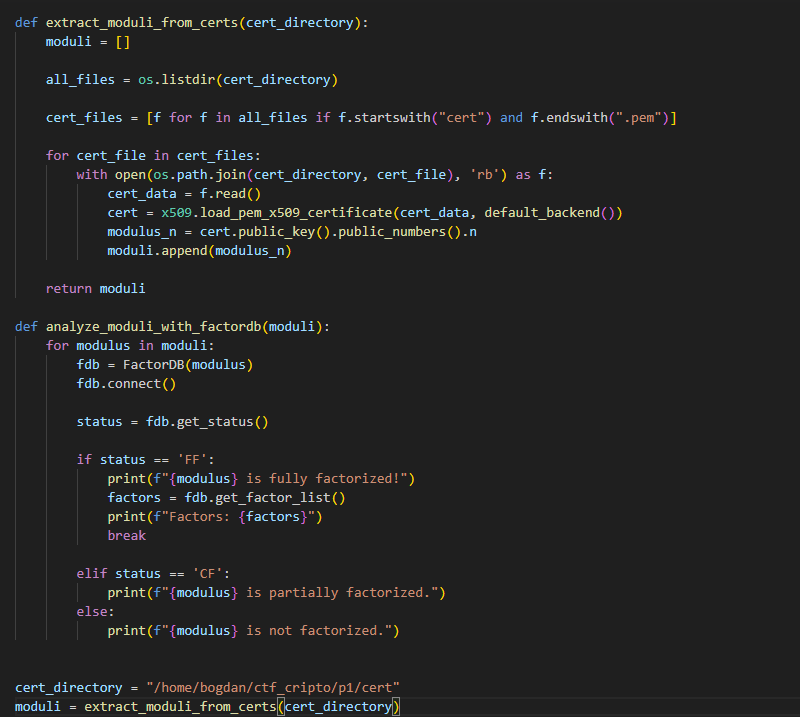
Pasul 1: Extragerea Modulilor

Am inceput prin extragerea modulilor din certificatele date. Fiecare certificat contine o cheie publica si aceasta cheie publica are un modul asociat. Pentru a face acest lucru, am folosit biblioteca cryptography pentru a incarca si a analiza certificatele.

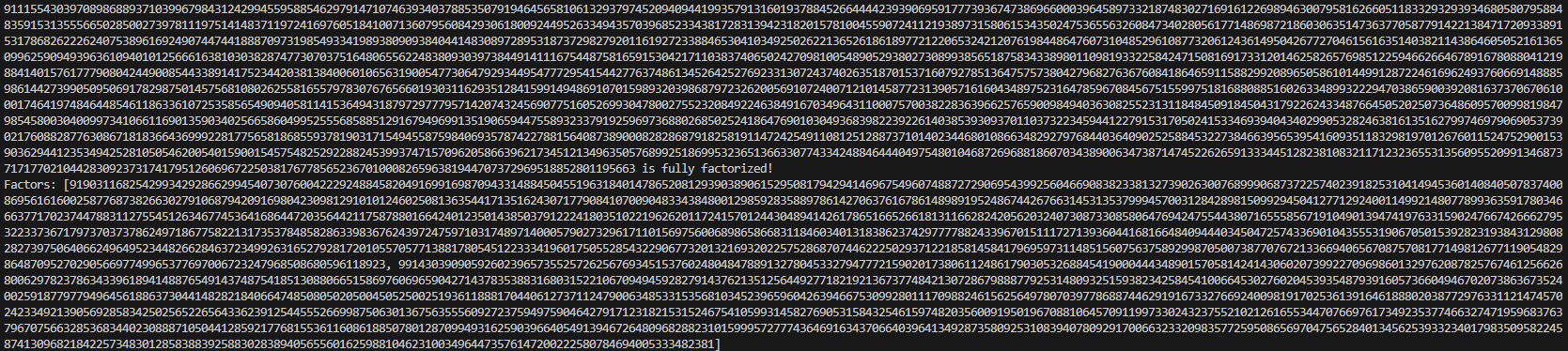


Pasul 2: Analizarea Modulilor cu FactorDB

Dupa ce am extras modulii, am vrut sa vad daca aceste numere au fost factorizate inainte. Daca modulul unui certificat a fost factorizat, acesta reprezinta o vulnerabilitate majora in cheia RSA.

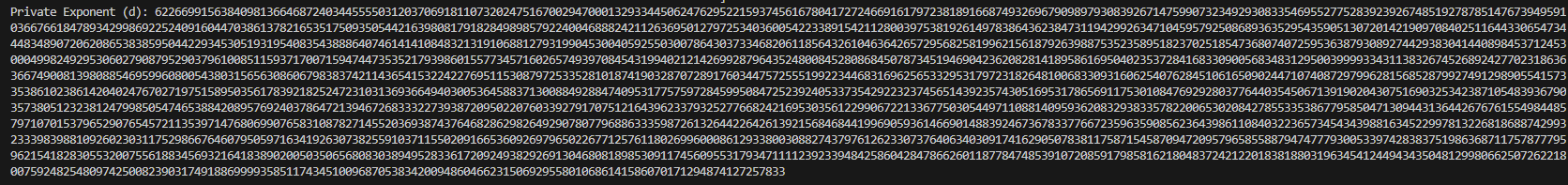
Am folosit API-ul FactorDB pentru a verifica daca modulii nostri sunt factorizati. Daca gasim un modul factorizat, putem obtine factorii p si q si folosi aceste valori pentru a calcula exponentul privat d.





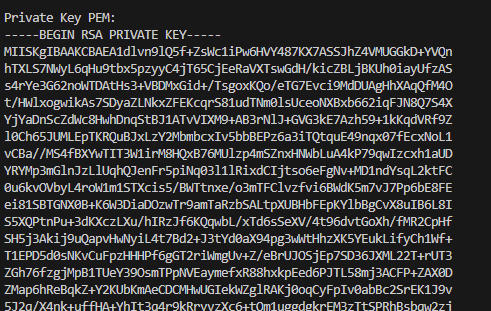
Pasul 3: Calcularea Exponentului Privat

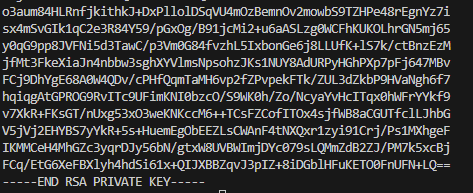
Avand factorii p si q pentru modulul nostru, calculez exponentul privat d folosind formula matematica pentru RSA.



Pasul 4: Generarea Cheii Private Complete

Dupa ce avem toate valorile necesare, generez cheia privata completa in format PEM folosind biblioteca Crypto.

 …



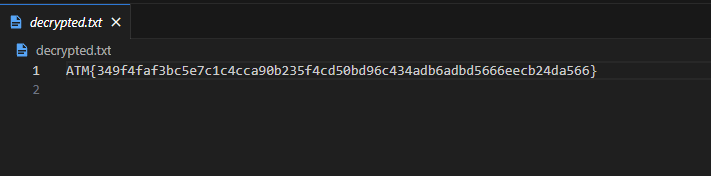
Pasul 5: Decriptarea Mesajului folosind OpenSSL

Odata ce avem cheia privata, putem utiliza comanda openssl pentru a decripta mesajul.

Comanda:

openssl smime -decrypt -in message.mail -inkey private\_key.pem -out decrypted.txt

Aceasta comanda ia mesajul criptat din message.mail si il decripteaza folosind cheia privata din private\_key.pem. Mesajul decriptat este salvat in decrypted.txt



Flag : ATM{349f4faf3bc5e7c1c4cca90b235f4cd50bd96c434adb6adbd5666eecb24da566}