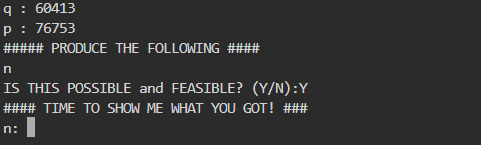
<https://play.picoctf.org/practice/challenge/61?category=2&page=2>

first question:



python code:

p=60413

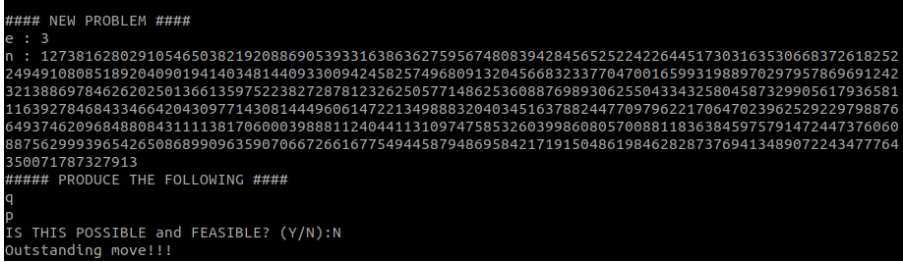
q= 76753

n=p\*q

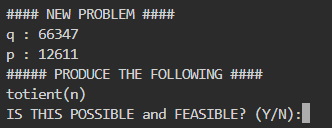
print(n)

->4636878989

Third question is insane :

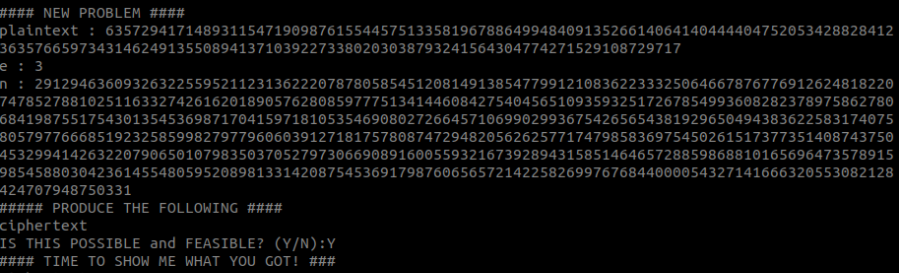


the size of n is crazy :v



just compute (p-1)\*(q-1) -> 836623060

next problem:



remember that c =plt^e (mod n)

I tried this :

n=29129463609326322559521123136222078780585451208149138547799121083622333250646678767769126248182207478527881025116332742616201890576280859777513414460842754045651093593251726785499360828237897586278068419875517543013545369871704159718105354690802726645710699029936754265654381929650494383622583174075805797766685192325859982797796060391271817578087472948205626257717479858369754502615173773514087437504532994142632207906501079835037052797306690891600559321673928943158514646572885986881016569647357891598545880304236145548059520898133142087545369179876065657214225826997676844000054327141666320553082128424707948750331

pt =6357294171489311547190987615544575133581967886499484091352661406414044440475205342882841236357665973431462491355089413710392273380203038793241564304774271529108729717

e=3

ct = pow(pt,e,n)

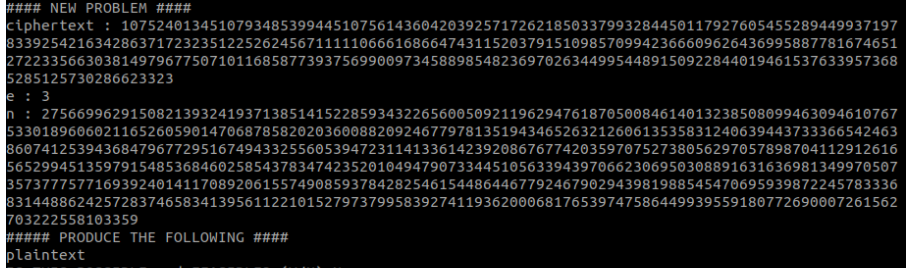
print(ct)

Admittedly, I don’t know that python can handle such a big size-number like this.

output:

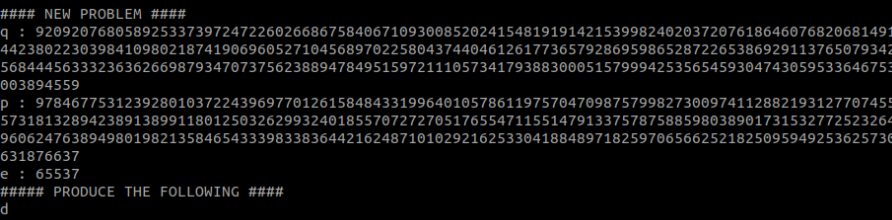
256931246631782714357241556582441991993437399854161372646318659020994329843524306570818293602492485385337029697819837182169818816821461486018802894936801257629375428544752970630870631166355711254848465862207765051226282541748174535990314552471546936536330397892907207943448897073772015986097770443616540466471245438117157152783246654401668267323136450122287983612851171545784168132230208726238881861407976917850248110805724300421712827401063963117423718797887144760360749619552577176382615108244813

Next one,

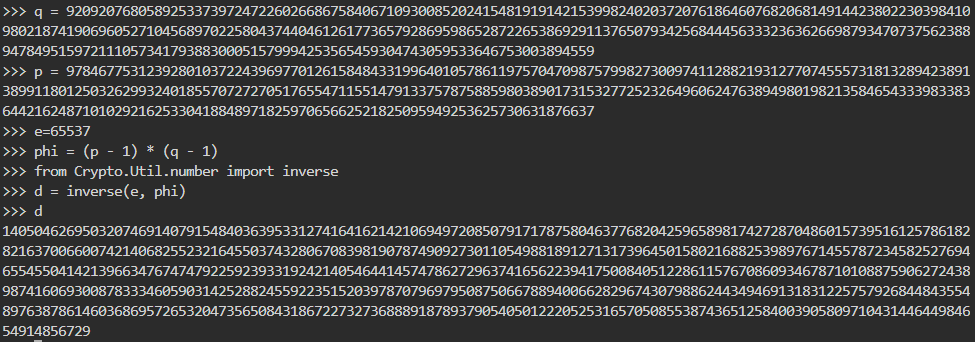


n,e and c -> impossible to find p

another “big” problem



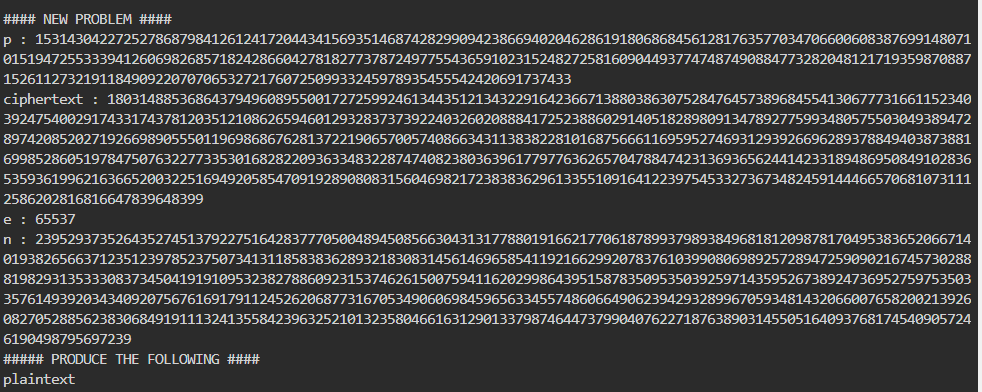
Let’s call for python help again :3



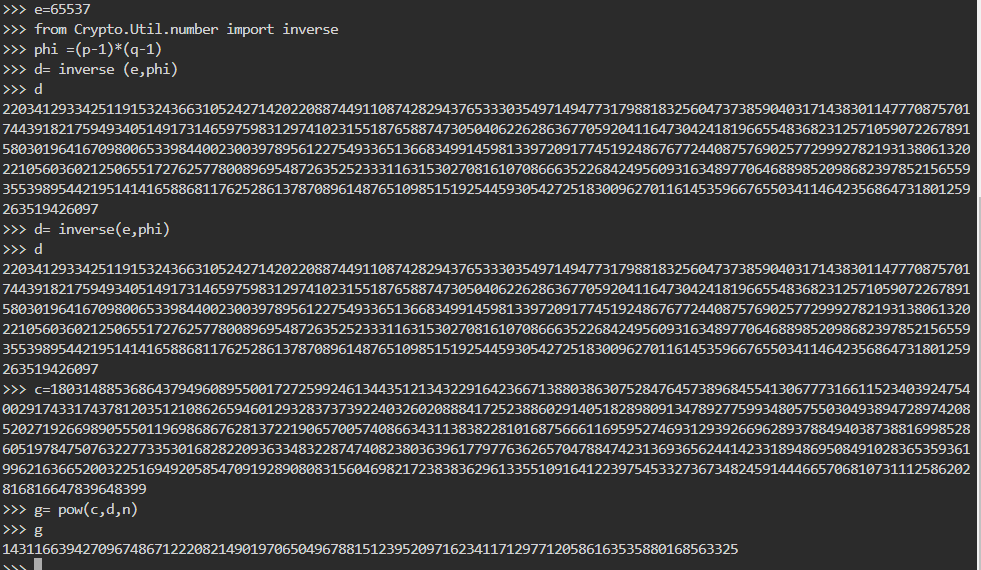
answer:

1405046269503207469140791548403639533127416416214210694972085079171787580463776820425965898174272870486015739516125786182821637006600742140682552321645503743280670839819078749092730110549881891271317396450158021688253989767145578723458252769465545504142139663476747479225923933192421405464414574786272963741656223941750084051228611576708609346787101088759062724389874160693008783334605903142528824559223515203978707969795087506678894006628296743079886244349469131831225757926844843554897638786146036869572653204735650843186722732736888918789379054050122205253165705085538743651258400390580971043144644984654914856729

The last question:

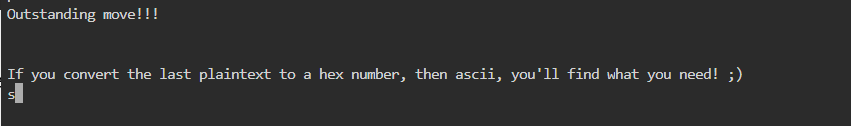


Ask python for help :3



output: 14311663942709674867122208214901970650496788151239520971623411712977120586163535880168563325

This is what you will get:





picoCTF{wA8\_th4t$\_ill3aGal..ode01e4bb}

Pheww, after this, I become familiar with RSA