Find

p1=401327687854144602104262478345650053155149834850813791388612732559616436344229998525081674131271

p2=500233813775302774885494989064149819654733094475237733501199023993441312997760959607567274704359

p3=969568679903672924738597736880903133415133378800072135853678043226600595571519034043189730269981

e1 = 398119

e2 = 283609

e3 = 272383

c=104229015434394780017196823454597012062804737684103834919430099907512793339407667578022877402970

c\_p=m^e mod p

c\_q=m^e mod q

thì dựa trên định lý số dư trung hoa sẽ tìm ra m^e duy nhất thoả đc cái này

theo extended euclidean thì mình có m, l sao cho mp+lq=1

dùng extended euclidean thì em kiếm đc m, l

rồi có

m^e+kN=c\_q.m.p+c\_p.l.q

lấy m^e +kN mod N ra c rồi lấy c bỏ vào tool

cp2+dp3=1

ap1 +bcp2 + bdp3=1

ae1 + bce2 + bde3 = 1

e3\*dk3-1=k(p3+1)

m=-15276757306724895970269469482138942339714165623952653641732988103136771603950632377178417168039

l=142108848993331702897135269329778819517833834889751388581903650650035559009095675288192504284558

d3=3559578534283244272728465935395759402808300733893349202606910281576312014962457400216569060

d2=1763815019182405265296570239534534586895102392643525887758142456669010197129713653683653462

d1=1008059619998404000070990026463570071147445449352615151220144561198075038730203779586208330

phi(p3)/e3=kp3=3559578534283244272728465935395759402808300733893349202606910281576312014962457400216569060