## UNEXPECTED

Alice, Bob, and Carol are really close friends; in fact, they are so close, they even share the same primes in their RSA public keys! Alice has N = P\*Q, Bob has N = QR, and Carol has N = PR, where P,Q,R are 1024 bit primes. All three also use the same public exponent e = 65537. Can you recover the three ciphertexts?

After opening the file given in the above question its content was :

N1 = 3895738302299059518129198422310169628530536557191890566210939781698372336257482186582163630847612416277492034959243510457939210010336159061758606919109259916143600981918456942199762738624796190838889500238780675229383463267807384154074134251073572174392024892486431125499446924573006208711810847272390619510395812856188247531815920797526102562723333957594242603466996229335924848954210939152042149332307810693239925149256224795031982752752336401872520016106145667479144091130160998875256860809091721275069193773739370057334041922519998813268278574260846083883264261920589114740823464192397850923545998904365370408113

N2 = 3036683903819675505741091164945461947189004916494633766372176282409409694958701211748277050499101511956962003835932755555293255586827283990400451317444723234406968971873530093281591689832798646915816609347861047534121792409030834659241904646743453387504496246791081682741245482378149293399372654558929658582070853972454887854658545741800574343930155288517185535533201220281739954820271979667081052363406511938025061398551356675540358212449132781674832812796443378476387659729623581274433769056775163718782871879747276327458473970177451591251859530403032170215968101310739004163533767679394201611410832974546802038041

N3 = 4793455677299549137382284585015750073239112414361680529255951318217960300841340399094743130287927996565298160174555422185410320841942637374406558835150138631140265626020072464652973386772727192540062051929655235552439145036105501434801984612127808829810146844869487529177642676245549299371487478280457673839725488195812744535928488844735950540356920273038857127652414836352483913807655170699520816765863272825856765769043174406026964068017257738085400965661973681558654658747878342173984592411085018242201038877382766239487564503728442821348064764166024851080258629751476765613997512620274759264076272801682962144457

E = 65537

C1 = 396708474546125804352894757436683688457291028695044217325853929491171136935487190613513217479209066321213697066977005912522338337419604329864854419961723570625025089500459612736934675744115710978556346050350466970024450696226499749911198313775828281699871502987873199226066403667788132060336882800770615332190939846610876881382430101512212915247532319827304296610854802037475047119525110795533529161852951539770153761419387662527094415537933400873451490021233979268224054475360645920086811082803271848565851436058022797610887635287190533293980480191482625531855511415716253479184799509403767653927424232672209598509

C2 = 355006513750551550798931713354683491263062473879176656452255051848683497534660576981575518851351256702360823676609578259232763677292692743319345273559085724516350773319337226043634439282120083618718026203533033564167432280901197175559735572797382863132012675404876908914335941746393221402727788260354881773319480220225939283398326940847106630716629330817737251316474369640273632208347751866683363389016722969822345738247486942531821199790024647950924227337611907877819668593060172268197128413003269501597578146759488894526193598933152416894414296396043283131502951693668167550687432080480619240585408701379144341703

C3 = 924835278307680480966328618545268895077532556525413716080960421925985654497130329688156219485942736928562517552888163928270855659413958949301590302010862666331053838345196518237383846281768395909801043955047640003147798786793258813501366000503338638933238548605016169865688228297750780710248359326295693845663887055907900967535999885217905972006140096240831305484619796964713673839223632057905454213937054336962510051529266336629730913756688411854427999570223208667606703681762027957427028839409594591627448224813082072169775916331655060221445546199171668136050686471357710989346885039441000083764142021784018773006

It was an interesting question as I solved it using some basic math substitution. As N1, N2, N3 were not factorisable through factordb I tried to do some basic math.

In RSA, N=p\*q. So N1=p\*q, N2=q\*r and N3=p\*r.

Therefore p=N1/q . Substituting this p in N3 we get N3=(N1\*r)/q

Also q=N2/r. Substituting this in N3 we get N3=(N1\*r^2)/N2.

From this r can be calculated and simultaneously p and q.

After this it was a basic RSA decryption problem. I used the below python script to decrypt :

from Crypto.Util.number import inverse

e=65537

#n=(All the Three values of n one by one)

#in relation to n select p and q

phi=(p-1)\*(q-1)

d=inverse(e, phi)

m=pow(c, d, n)

print(hex(m)[2:])

After giving all the values correctly three hex strings were received :

666c61677b6e305f306e335f337870, 336374355f7468335f7370346e6973, 685f696e71756973697469306e217d

After converting this to ascii the flag was retrieved : flag{n0\_0n3\_3xp3ct5\_th3\_sp4nish\_inquisiti0n!}