Đề bài như sau :

N =
153527791283477910070856485034324814241578039253931719113365199593030419127930034451509252549694195198848856276029495314182182253262413303585786772642912994990451563528569677738740927402479544691167856974974703591674645148479167960709372225026786509711420250274857098036615075040656633597349639952615572050743066806107894593710277098419836798284016504121185817582238280228809637922794866685718180114660553184881926462589475128006942944150859629512563710666088092902726100366778089854464628439785180626810577335071430780316463462084134853102653722178304031503530558606751126255865597117013858615693152206973338616243 79

e = 65537

c =
152342360890353756973246925336700872915065189401190361634163983919677801689193183547078467786243546985160632636175265521280380763845597995898929223398426172505125446970387023863595267505261789073828349582495472651930396488898261941553096488689361929998521330958132220745611160011510127353348026561123380518096501501331515937439329992034644906677687754274692474388293476719418880123668722570095785535255577270890613802085052276018708074132189756832759745054712935684738282501024563689134426446331801811343607636874377162613711506737364443893419620031888485533551416775989754869371340004201181291703595765830294035579 42

N =
159827185554356182887549528250317691175473876928708199169284761824865526314505495250380043842995009284722764582950 66

30413736901437716018757103362365788906261380174240049764180764398004480897644067686220127212714395757657514960659715470939848309903452537159654659280111012837681397066499348501319871801822600195792312470502704209538918583877602875543405282240615843480516595264945073471970479028739858736374403194015146573431944220665165459980513581807830859376674664374776280123358153505285205750010287011511441804497769103377389443061925908748111247050763456865855379625292986335707187667270866751214835174634353111714

e = 65537

c = 14885607973375889007078519123100974115225353700683145848346940830215842296236022064741140177725928924596370430750080147304522857101387236773374040772176304410951702328717963740412312728751613954861413504364980527717532790500428309863862561124898893373142700396901730889636915098343789818475628485817239154487704058551986711609340589253536488388398979374511706211200806320134259212830624064308312622387468199391611528640492645158491457258448456704967213884906875441766539265807657769147443850357508881684012458065494838709615700471413080742522071409893826661777251684652098457627030289338034729867701502662269612568405

+ Mình thấy N và c xuất hiện hai lần nên mình sẽ tìm p, q bằng cách gcd(N1,N2) {mình đặt cho N thứ tự là N1,N2 }

+, Và đây là phần mình làm :

```python
from Crypto.Util.number import *
from numpy import gcd


n1 = 153527791283477910070856485034324814241578039253931719113365199593030419127930034451509252549694
n2 = 159827185554356182887549528250317691175473876928708199169284761824865526314505495250380043842995
c1 = 152342360890353756973246925336700872915065189401190361634163983919677801689193183547078467786243
c2 = 148856079733758890070785191231009741152253537006831458483469408302158422962360220647411401777259
e = 65537
p = (gcd(n1, n2))
q = n1//p
phi = (p-1)*(q-1)
d = inverse(e, phi)
m=pow(c1, d, n1)
print(long_to_bytes(m))

```

Chạy chương trình mình được

```
In [5]: runfile('C:/Users/Admin/Desktop/tuyen ban cm kcsc/cách giải và đáp
án/babyrsa python.py', wdir='C:/Users/Admin/Desktop/tuyen ban cm kcsc/cách
giải và đáp án')
b'KCSC{All_I_Want_for_Chrismas_is___a_girlfriend T_T}'

In [6]:
```

Flag :

KCSC{All_I_Want_for_Chrismas_is___a_girlfriend T_T}

+ Mình copy code ra đây :

```
from Crypto.Util.number import *
from numpy import gcd


n1 =
153527791283477910070856485034324814241578039253931719113365199593030419127930034451509252549694195198848856276029495314182182253262413303585786772642912994990451563528569677738740927402479544691167856974974703591674645148479167960709372225026786509711420250274857098036615075040656633597349639952615572050743066806107894593710277098419836798284016504121185817582238280228809637922794866685718180114660553184881926462589475128006942944150859629512563710666088092902726100366778089854464628439785180626810577335071430780316463462084134853102653722178304031503530558606751126255865597117013858615693152206973338616243791
n2 =
159827185554356182887549528250317691175473876928708199169284761824865526314505495250380043842995009284722764582950663041373690143771601875710336236578890626138017424004976418076439800448089764406768622012721271439575765751496065971547093984830990345253715965465928011101283768139706649934850131987180182260019579231247050270420953891858387760287554340528224061584348051659526494507347197047902873985873637440319401514657343194422066516545998051358180783085937667466437477628012335815350528520575001028701151144180449776910337738944306192590874811124705076345686585537962529298633570718766727086675121483517463435311171
```

c1 =
152342360890353756973246925336700872915065189401190361634163983919677801689193183547078467786243546985160632636175265521280380763845597995898929223398426172505125446970387023863595267505261789073828349582495472651930396488898261941553096488689361929998521330958132220745611160011510127353348026561123380518096501501331515937439329992034644906677687754274692474388293476719418880123668722570095785535255577270890613802085052276018708074132189756832759745054712935684738282501024563689134426446331801811343607636874377162613711506737364443893419620031888485533551416775989754869371340004201181291703595765830294035579 42

c2 =
148856079733758890070785191231009741152253537006831458483469408302158422962360220647411401777259289245963704307500801473045228571013872367733740407721763044109517023287179637404123127287516139548614135043649805277175327905004283098638625611248988933731427003969017308896369150983437898184756284858172391544877040585519867116093405892535364883883989793745117062112008063201342592128306240643083126223874681993916115286404926451584914572584484567049672138849068754417665392658076577691474438503575088816840124580654948387096157004714130807425220714098938266617772516846520984576270302893380347298677015026622696125684 05

e = 65537

p = (gcd(n1, n2))

q = n1//p

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

d = inverse(e, phi)

```
m=pow(c1, d, n1)
print(long_to_bytes(m))
```