Problem 4

By Noel Santillana Herrera

Note: The mathematical parts of this task was solved by using magma and python.

Elgamal digital scheme

Given:

p =
172471720944269739125606601541029487739340755626635772583971303759438419175772663669593721846550197442744469656080602946644927061951111688637275362803660140005841509436858417187894094969161813013831722315776185924842099093899593568334696592964516617033076246061593684511550344711963113062475271615663164060997

g = 3

d = 333

- **Compute public key (p, g, β)**

  First, find β because p and g is already known.

  Formula to find β:
  $$\beta = g^d \pmod p$$

  $\beta = 3^{333} \pmod p$ =
  760988023132059809720425867265032780727896356372077865117010037035791631439306199613044145649378522557935351570949952010001833769302566531786879537190794573523

  Pub_{key} (3, 333,
  760988023132059809720425867265032780727896356372077865117010037035791631439306199613044145649378522557935351570949952010001833769302566531786879537190794573523)

- **Message x**
  Message x = A3FB8FCE (32 bits)
  A3FB8FCE is 2751172558 in hexadecimal
  2751172558 mod p = 2751172558

- **Sign the message *x*, by computing the signature (x, (r, s))**

First, we need to find the ephemeral key(Key_e). To find the right Key_e, the GCD of Key_e and p-1 must be equals 1.

I randomly chose $Key_e = 101$

And to prove it is equals to 1, I chose to solve this on magma.

Key_e =

```
p:=1724717209442697391256066015410294877393407556266357725839713037594384191757726
GCD(101, p-1)
```

Clear Submit

```
1
```

Then, we need to find r:

$$r = g^{Key_e} \bmod p$$

$r = 3^{101} \bmod p = 1546132562196033993109383389296863818106322566003$

Then, we need to find s:

$$s = (x - d * r) K_e^{-1} \bmod p-1$$

$(x - d * r) =$

```
>>> (2751172558-333*1546132562196033993109383389296863818106322566003)
-514862143211279319705424668635855651429402663306441
```

$K_e^{-1} \bmod p-1 =$

1536876721285571932802435063236896425400066139247249458669051221618758190675201953491429204573219581172970521687846956950301330255009906136371760658646476495101558004882896786822818668042035957548995545388104627053048407767422120905952741917505593617126421994608260555053418913274918829269581628258384630246

Multiply both and get:

s = -
79127964257261354844763290661153611461992901683519821812990166293738999737382505533564586937943326727972579362812260447582382776922919609182614554672890614633472723641110210838229779227933056062277080974032443416744597917613201938615617401117013451759638718148906839028014266221519241452786022201228577960844378710442634047539527296600882402274509090686770 65

The signed message is:

(2751172558, (1546132562196033993109383389296863818106322566003,
7912796425726135484476329066115361146199290168351982181299016629373899973738250553356458693794332672797257936281226044758238277692291960918261455467289061463347272364111021083822977922793305606227708097403244341674459791761320193861561740111701345175963871814890683902801426622151924145278602220122857796084437871044263404753952729660088240227450909068677065))

- **Verifying signature**

  First find t by using the formula:

  $$t = \beta^r r^s \pmod p$$

  t =
  46521955892376287894073819866951634435052777238463242903041720375066441762066532851687922655411530943140218735781929651596183562244989 2921

1625869078407680532355038413783830656645541143052035546940551191056589401499979255540355721375966887039321329361406321776463925777583266116269139073181444524029276618 4231

Accept it if and only if:

$$t = g^x \pmod p$$

Compute $g^x \pmod p$, which also give the same as above:

46521955892376287894073819866951634435052777238463242903041720375066441762066532851687922655411530943140218735781929651596183562244989292116258690784076805323550384137838306566455411430520355469405511910565894014999792555403557213759668870393213293614063217764639257775832661162691390731814445240292766184231

<u>The signature is therefore verified.</u>