**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:

β = gd (mod p)

β = 3333 (mod p) = 760988023132059809720425867265032780727896356372077865117010037035791631439306199613044145649378522557935351570949952010001833769302566531786879537190794573523

Pubkey (3, 333, 760988023132059809720425867265032780727896356372077865117010037035791631439306199613044145649378522557935351570949952010001833769302566531786879537190794573523)

* **Message x**

Message x = A3FB8FCE (32 bits)

A3FB8FCE is 2751172558 in hexadecimal

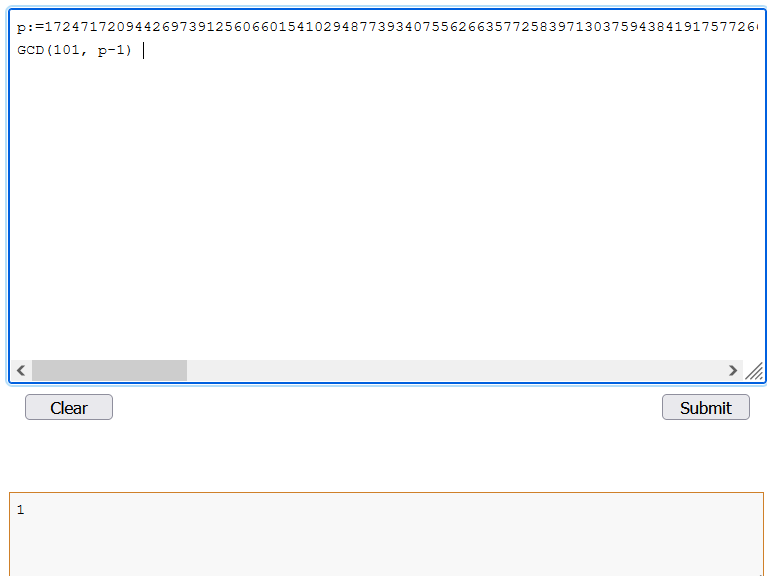
2751172558 mod p = 2751172558

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

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

I randomly chose Keye = 101

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

Keye = 

**Then, we need to find r:**

r = gKeye mod p

r = 3101 mod p = 1546132562196033993109383389296863818106322566003

**Then, we need to find s:**

s = (x – d \* r) Ke-1 mod p-1

(x – d \* r) =



Ke-1 mod p-1 =

15368767212855719328024350632368964254000661392472494586690512216187581906752019534914292045732195811729705216878469569503013302550099061363717606586464764951015580048828967868228186680420359575489955453881046270530484077674221209059527419175055936171264219946082605550534189132749188292695816282583846302465

Multiply both and get:

s = -7912796425726135484476329066115361146199290168351982181299016629373899973738250553356458693794332672797257936281226044758238277692291960918261455467289061463347272364111021083822977922793305606227708097403244341674459791761320193861561740111701345175963871814890683902801426622151924145278602220122857796084437871044263404753952729660088240227450909068677065

The signed message is:

(2751172558, (1546132562196033993109383389296863818106322566003, 7912796425726135484476329066115361146199290168351982181299016629373899973738250553356458693794332672797257936281226044758238277692291960918261455467289061463347272364111021083822977922793305606227708097403244341674459791761320193861561740111701345175963871814890683902801426622151924145278602220122857796084437871044263404753952729660088240227450909068677065))

* **Verifying signature**

First find t by using the formula:

t = βrrs (mod p)

t = 46521955892376287894073819866951634435052777238463242903041720375066441762066532851687922655411530943140218735781929651596183562244989292116258690784076805323550384137838306566455411430520355469405511910565894014999792555403557213759668870393213293614063217764639257775832661162691390731814445240292766184231

Accept it if and only if:

t = gx (mod p)

Compute gx (mod p), which also give the same as above:

46521955892376287894073819866951634435052777238463242903041720375066441762066532851687922655411530943140218735781929651596183562244989292116258690784076805323550384137838306566455411430520355469405511910565894014999792555403557213759668870393213293614063217764639257775832661162691390731814445240292766184231

The signature is therefore verified.