CS641 - Assignment 3

Nishtha - 180489

Text on the wall :

"As you move closer to the boulder, you realize that it has something written on it!
Wiping the dust from the boulder with your hand - and getting your hand very dirty in the process - you see strange symbols on the boulder -- it appears like some code:
... . -.-. ..- .-. .. - -.--
The spirit of Cave Man is the keeper of the chamber.
To navigate through the chamber, you must pay respect to him first. When you bow down, you hear a faint voice-
"You have been blessed, my child. Keep in mind that you must always believe in yourself and PLAY FAIR".

TR XYCB MH AFC MUVY EOHPTCS, AFCSS TE QCSI NTYIMS TNA AFCSC. EMRBH XAA VAFR MIUCQPUH "LMRL_CCETOT" FN HM AKUXAHK. OTA WANA OTXT FFU EISCWNAF HME BFU MCVA UGTOTRE. BM HYLF IFU UVTY ANE HBSEI QYOQM OUVSF AM EAFTE PYHYS XNSKE IFUSC."

Cryptanalysis

- **Commands to get to cipher**

  go -> put -> back -> enter -> pick -> back -> give -> back -> back -> thrnxxtzy -> read

- **Analysis**

  The multiplicative group Z_p^* uses multiplication as the basic operation with integers between 1 and p -1. The remainder is taken after division with p to obtain the result. Also, in a multiplicative group each element has an inverse. We use the equation $x * x^{-1}$ mod p = 1 to get this inverse. Now in the question, we are given multiplicative group Z_p^* and 3 pairs of numbers forming <a_1, password * g^{a_1}>, <a_2, password * g^{a_2}>, <a_3, password * g^{a_3}>. Also it is given that the missing number maybe g.

We have p = 19,807,040,628,566,084,398,385,987,581

We have

$$a_1 = 324$$
$$a_2 = 2,345$$
$$a_3 = 9,513$$

Let

$$password * g^{a_1} = x_1$$
= 11,226,815,350,263,531,814,963,336,315 - (1)

$$password * g^{a_2} = x_2$$
= 9,190,548,667,900,274,300,830,391,220 - (2)

$$password * g^{a_3} = x_3$$
= 4,138,652,629,655,613,570,819,000,497 - (3)

Now, we first need to find the value of g and then calculate the password.

Dividing eqn (2)/(1), we get:

$$g^{(a_2 - a_1)} = \frac{x_2}{x_1}$$
$$\implies g^{(2021)} = x_2 * x_1^{-1} \text{ mod p}$$

Similarly, we get using eqn (3)/(2) and eqn (3)/(1),

$$g^{(a_3 - a_1)} = \frac{x_3}{x_1} = g^{(9189)} = x_3 * x_1^{-1} \text{ mod p}$$
$$g^{(a_3 - a_2)} = \frac{x_3}{x_2} = g^{(7168)} = x_3 * x_2^{-1} \text{ mod p}$$

Division here is performed sequentially and by taking inverse applying modular arithmetic. In order to make power of g to be 1, Deophantine eqaution 2021*x*+7168*z*−9189*y*=1 gives the solution as *x* = 632+9189*r*−9188*s*

Therefore we solve sequentially to get the values as:

$$x_1^{-1} = 17,983,774,594,023,309,985,368,857,902$$

Use this to solve for x_2, x_3

$$x_2 * x_1^{-1} \text{ mod p}$$
= 7,021,284,369,301,638,640,577,066,679

$$x_3 * x_1^{-1} \text{ mod p}$$
= 3,426,347,385,144,995,225,825,016,781

Then,

$(x_2 * x_1^{-1})^{(632)}$ mod p

= 9,145,714,735,161,140,899,390,199,931

$(x_3 * x_1^{-1})^{(139)}$ mod p

= 17,064,457,453,994,872,811,494,067,145

$(x_3 * x_1^{-1})^{(-139)}$ mod p

= 9,337,479,922,712,664,552,660,519,694

Therefore, we obtain g as 192,847,283,928,500,239,481,729.

Using the equation $password * g^{a_1} = x_1$, we get

$password = x_1 * g^{(-a_1)}$ mod p

$\implies password = x_1 * (g^{(a_1)})^{-1}$ mod p

We get $g^{(a_1)}$ mod p = 10,900,623,124,966,429,218,667,385,137

Therefore, *password* = 3,608,528,850,368,400,786,036,725

- **Password**

  3,608,528,850,368,400,786,036,725