

## Q1 Team name

0 Points

CryptoCreeks

## Q2 Commands

10 Points

List the commands used in the game to reach the ciphertext.

enter -> enter -> pluck/pick ->c ->c ->  
back -> give -> back -> back -> thrnxtzy  
-> read

## Q3 Analysis

50 Points

Give a detailed analysis of how you figured out the password? (Explain in less than 500 words)

On entering the chamber, we find an open door. We use the "enter" command to enter into a small chamber. There, we saw a small hole next to a large hole. We used "put" command to insert our hand in the small hole, but it got bit by something, so we pulled our hand back. We then realized that the large hole opens to a small chamber, so we used "enter" command. There, we saw some mushrooms, so we plucked them using "pluck" command. We then came out of the large hole and gave those mushrooms using the "give" command. The rat sitting inside the hole grabbed those mushrooms and spelled the magic words

"thrnxtzy" for the hidden door in the main chamber to become visible. So, we then returned back to the main chamber using the "back" command twice, and then used "thrnxtzy". We then saw a glass panel, and used "read" command. There we saw some information related to a multiplicative group, and also three pairs of the form  $(a, password * g^a)$ . We were required to find the value  $g$ , using which we can find the required  $password$ . The calculations have been described below:

NOTE : All the mathematical operations performed are modular arithmetic operations, i.e., modulus has been taken after each arithmetic operation.

Given,

A group  $Z_p^*$ , where  $p = 19807040628566084398385987581$  is prime, and  $password$  and  $g$  are elements of  $Z_p^*$  and  $a$  is an integer.

Three pairs of form  $(a, password * g^a)$  :

(324, 11226815350263531814963336315)

(2345, 9190548667900274300830391220)

(9513, 4138652629655613570819000497)

pattern of  $g$  : 1\_\_4\_2\_\_\_\_\_0\_\_\_94\_\_\_\_9

We can write the pairs in the form of equations as:

$$password * g^{324} \equiv 11226815350263531814963336315 \mod p \text{ --- (1)}$$

$$password * g^{2345} \equiv 9190548667900274300830391220 \mod p \text{ --- (2)}$$

$$password * g^{9513} \equiv 4138652629655613570819000497 \mod p \text{ --- (3)}$$

Multiplying both sides of equation (1) with  $g^{-324}$ , we get

$$password * g^{324} * g^{-324} \equiv 11226815350263531814963336315 * g^{-324} \mod p$$

$$password \equiv 11226815350263531814963336315 * g^{-324} \mod p$$

Substituting this value of password in the (2) equation , we get

$$11226815350263531814963336315 * g^{-324} * g^{2345} \equiv 9190548667900274300830391220 \mod p$$

$$11226815350263531814963336315 * g^{2021} \equiv 9190548667900274300830391220 \mod p$$

Multiplying both sides with modular inverse of 11226815350263531814963336315 , we get

$$g^{2021} \equiv 9190548667900274300830391220 * 11226815350263531814963336315^{-1} \mod p$$

$$\implies g^{2021} \equiv (9190548667900274300830391220) * (11226815350263531814963336315)^{-1} \mod p$$

Calculating modular inverse using Fermat's theorem which says

$$a^{p-1} \equiv 1 \mod p$$

Multiplying both sides by  $a^{-1}$

$$\implies a^{-1} * a^{p-1} \equiv a^{-1} \mod p$$

$$\implies a^{-1} \equiv a^{p-2} \mod p$$

calculating modular inverse by using the above formula, we get

$$(11226815350263531814963336315)^{-1} = 17983774594023309985368857902$$

substituting this value into the equation, we get

$$\implies g^{2021} \equiv (9190548667900274300830391220) * (17983774594023309985368857902) \mod p$$

$$\implies g^{2021} = 7021284369301638640577066679 - - - - - (4)$$

Repeating the above steps for equations (2) and (3) , we get ,

$$g^{7168} = 6339248851737327508924059257 - - - - - (5)$$

Multiplying equation (5) with  $g^{7168}$  with modular inverse of  $g^{2021*3}$  ,

$$g^{1105} = 1332524359715193692493602650 - - - - - (6)$$

Multiplying equation (4) with modular inverse of  $g^{1105}$  ,

$$g^{916} = 16928329349929603757418032233 - - - - - (7)$$

Multiplying equation (6) with modular inverse of  $g^{916}$  ,

$$g^{189} = 7233340894988383169873081319 - - - - - (8)$$

Multiplying equation (7) with modular inverse of  $g^{189*4}$  ,

$$g^{160} = 15480832131739101784049259744 - - - (9)$$

Multiplying equation (8) with modular inverse of  $g^{160}$  ,

$$g^{29} = 14409628835368808838382787765 - - - (10)$$

Multiplying equation (9) with modular inverse of  $g^{29*5}$  ,

$$g^{15} = 9862566087568179051837025782 - - - (11)$$

Multiplying equation (10) with modular inverse of  $g^{15}$  ,

$$g^{14} = 11662011900497299711580345247 - - - (12)$$

Multiplying equation (11) with modular inverse of  $g^{14}$ ,

$$g^1 = 192847283928500239481729 - - - (13)$$

Hence, we got the value of g as 192847283928500239481729

Using the following equation and placing the value of g we get ,

$$password \equiv 11226815350263531814963336315 * g^{-324} \text{ mod } p$$

$$password \equiv 11226815350263531814963336315 * \\ 7280920143223660694435112264 \text{ mod } p$$

$$password = 3608528850368400786036725$$

## Q4 Password

10 Points

What was the final command used to clear this level?

3608528850368400786036725

## Q5 Codes

0 Points

Upload any code that you have used to solve this level.

► Assignment 3.ipynb

Download

## Assignment 3

● GRADED

### GROUP

SHRUTI WASNIK

PRADEEP KUMAR TIWARI

TANISHA RASTOGI

 View or edit group

### TOTAL POINTS

**69 / 70 pts**

### QUESTION 1

Team name

0 / 0 pts

### QUESTION 2

Commands

10 / 10 pts

### QUESTION 3

Analysis

49 / 50 pts

### QUESTION 4

Password

10 / 10 pts

### QUESTION 5

