

Q1 Team Name

0 Points

DECODERS

Q2 Commands

10 Points

List the commands used in the game to reach the ciphertext

1. enter
2. put
3. back
4. enter
5. pluck
6. back
7. give
8. back
9. back
10. thrnxtzy
11. read

Q3 Analysis

50 Points

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

We have got three pairs in the form of $(a, password * g^a)$ and we formed 3 equations from it as below:

(i) $password * g^{429} = 431955503618234519808008749742$

(ii) $password * g^{1973} = 176325509039323911968355873643$

(iii) $password * g^{7596} =$

98486971404861992487294722613

We then divided equation (ii) by equation (i) and equation (iii) by equation (ii) and got the following equations respectively.

$$(iv) g^{1544} = \frac{176325509039323911968355873643}{431955503618234519808008749742}$$

$$(v) g^{5623} = \frac{98486971404861992487294722613}{176325509039323911968355873643}$$

Since, g is an element of the multiplicative group Z_p^* , where $p=455470209427676832372575348833$ is a prime, all the arithmetic operations like multiplication, division, etc. will be done using modular arithmetic and its properties. Here, we will perform the operations by taking modulo with respect to given p . Hence, the division to the RHS of equations (iv) and (v) will be done using the following formula.

$$(a/b) \bmod p = (a \bmod p) * (b^{-1} \bmod p) \bmod p,$$

Here, b^{-1} is the modular multiplicative inverse of b , which is calculated using Fermat's little theorem as follows:

$$b^{(p-1)} \bmod p = 1 \text{ which implies } b^{-1} = b^{(p-2)} \bmod p.$$

Thus, equations (iv) and (v) becomes

$$(iv) g^{1544} = (176325509039323911968355873643 \bmod p) * (431955503618234519808008749742^{-1} \bmod p) \bmod p$$

$$g^{1544} = 111590994894663139264552154672$$

$$(v) g^{5623} = (98486971404861992487294722613 \bmod p) * (176325509039323911968355873643^{-1} \bmod p) \bmod p$$

$$g^{5623} = 420413074251022028027270785553$$

If we can somehow make power of g equal to 1, we can then easily figure out the password.

We noticed that the powers of g in equations (iv) and (v) are co-prime to each other i.e.

$GCD(1544, 5623) = 1$. Hence, we can use the EXTENDED EUCLIDEAN ALGORITHM to make the power of g as 1.

According to EXTENDED EUCLIDEAN ALGORITHM, we can find x and y such that the below equation holds.

$$ax + by = GCD(a, b)$$

here a and b are 1544 and 5623 respectively. Now we have to find two numbers x and y such that $1544x + 5623y = 1$.

We applied the EXTENDED EUCLIDEAN ALGORITHM and found out that,

$$x = -2298 \text{ and } y = 631.$$

Now we will raise both sides of equation (iv) by -2298 and equation (v) by 631 . to get

$$\begin{aligned} \text{(iv)} (g^{1544})^{-2298} &= \\ (111590994894663139264552154672)^{-2298} \text{ mod } p &= \\ (g^{1544})^{-2298} &= 63673345919111482928118052957 \end{aligned}$$

$$\begin{aligned} \text{(v)} (g^{5623})^{631} &= \\ (420413074251022028027270785553)^{631} \text{ mod } p &= \\ (g^{5623})^{631} &= 347267008389877298374017667230 \end{aligned}$$

Now we multiply equation (iv) and (v). to get equation (vi) as below:

$$\begin{aligned} \text{(vi)} (g^{1544})^{-2298} * (g^{5623})^{631} &= \\ (63673345919111482928118052957 * & \\ 347267008389877298374017667230) \text{ mod } p & \end{aligned}$$

$$\begin{aligned} g^{(1544)*(-2298) + (5623)*(631)} &= \\ 52565085417963311027694339 & \\ g^1 = g = 52565085417963311027694339 & \text{ (using the identity} \\ ax+by=gcd(a,b)) & \end{aligned}$$

Thus, we got the value of g as 52565085417963311027694339 which matches with the pattern 5__50__4____31____94__9, hence we are sure that the value of g we found is correct. Using this value we can easily find out the value of the password by putting the value of g in any of the three initial equations. Putting g in equation (i) gives,

$$\begin{aligned} & (password * \\ & (52565085417963311027694339)^{429}) \bmod p = \\ & 431955503618234519808008749742 \bmod p \end{aligned}$$

$$\begin{aligned} password &= ((52565085417963311027694339)^{-429} * \\ & (431955503618234519808008749742)) \bmod p \end{aligned}$$

$$\begin{aligned} password &= \\ & ((52565085417963311027694339)^{-429} \bmod p) * \\ & (431955503618234519808008749742 \bmod p) \bmod p \end{aligned}$$

$$\begin{aligned} password &= (442956820316148690889301696615 * \\ & 431955503618234519808008749742) \bmod p \end{aligned}$$

$$password = 134721542097659029845273957$$

Hence, the password is 134721542097659029845273957 and g is 52565085417963311027694339

Q4 Password

10 Points

What was the final command used to clear this level?

134721542097659029845273957

Q5 Codes

0 Points

Upload any code that you have used to solve this level

 No files uploaded

Assignment 3


● GRADED

GROUP

Akash Gajanan Panzade

Abhishek Dnyaneshwar Revskar

Manthan Kojage

 [View or edit group](#)

TOTAL POINTS

70 / 70 pts

QUESTION 1

Team Name0 / 0 pts

QUESTION 2

Commands10 / 10 pts

QUESTION 3

Analysis50 / 50 pts

QUESTION 4

Password10 / 10 pts

QUESTION 5

Codes0 / 0 pts