Q1 Team Name
0 Points

Cryptophilic

Q2 Commands
10 Points

List the commands used in the game to reach the ciphertext

enter,
enter,
pluck,
c,
back,
give,
back,
back,
thrnxxtzy
read

Q3 Analysis
50 Points

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

After using 'read' for the glass panel, there were equations related to multiplicative groups. Therefore, we used Modular arithmetics to proceed.

Given, p = 455470209427676832372575348833 is the prime modulo for the multiplicative group.

Let the password be K.
Given,
$Kg^{429} = 431955503618234519808008749742 = A(modp)$ ----> eq 1
$Kg^{1973} = 176325509039323911968355873643 = B(modp)$ ----> eq 2
$Kg^{7596} = 984869714048619924872947226 13 = C(modp)$ ----> eq 3

eq 2 ÷ eq 1 : $g^{1544} = B * A^{-1}$
eq 3 ÷ eq 2 : $g^{5623} = C * B^{-1}$
eq 3 ÷ eq 1 : $g^{7167} = C * A^{-1}$

Using the properties of multiplicative group, A and B are coprime to p. So, their modular inverse exists under modulo p.

Let $A^{-1} = a$ such that (A * a) % p = 1

Since it is given that p is prime, we can use Fermat's Little Theorem.
Therfore, $x^{p-1} = 1(modp)$
Multiply both sides of eqn. by x^{-1} :=> $x^{-1} = x^{p-2}(modp)$

Using this analysis with Euclidian algorithm :
$g^{1544} = 11159099948946631392645521546 72$
$g^{5623} = 42041307425102202802727078555 3$
$g^{5623} * g(-1544 * 3) = g^{991} = 161798558270556961732424822635$
$g^{1544} * g(-991) = g^{553} = 559602640915038103624421977 78$
$g^{991} * g(-553) = g^{438} = 327597482298082119695568192760$
$g^{553} * g(-438) = g^{115} = 212427760325417336316893638262$
$g^{438} * g(-115) = g^{93} = 213701625154445213529342267 24$
$g^{115} * g(-93) = g^{22} = 628758645601568765778312781 1$
$g^{93} * g(-22 * 4) = g^{5} = 254662155980870723273334022569$
$g^{22} * g(-5 * 4) = g^{2} = 108044907665466013935627786069$
$g^{5} * g(-2 * 2) = g = 525650854179633110276943 39$
which matches with the hints given.

Therefore, we use g to find the value of K = password = 13472154209765902984527395 7

(The values computed using python code)

Q4 Password
10 Points

What was the final command used to clear this level?

13472154209765902984527395 7

Q5 Codes
0 Points

Upload any code that you have used to solve this level

No files uploaded

Assignment 3 — GRADED

GROUP
Shubhi Kesarwani
Tanishq Rajesh Chourishi
Abhinav Maheshwari
View or edit group

TOTAL POINTS
70 / 70 pts

QUESTION 1
Team Name — **0** / 0 pts

QUESTION 2
Commands — **10** / 10 pts

QUESTION 3
Analysis — **50** / 50 pts

QUESTION 4
Password — **10** / 10 pts

QUESTION 5
Codes — **0** / 0 pts


Select a question.
Group Members
Submission History
Next Question