Q1 Team Name

0 Points

The_Kryptonians

Q2 Commands

10 Points

List the commands used in the game to reach the ciphertext

go
climb
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)

First, we went to a small chamber; there were two holes, one large and the other small. We plucked some mushrooms from the large hole and gave them to a rat sitting inside another hole. The rat told us the magic word "**thrnxxtzy**" for the hidden door to become visible at the main chamber. There we read the glass panel and got our ciphertext.

We were given that the $password$ and g are the elements of a multiplicative group $\mathbb{Z}_p^*$ where p is a prime number.
The prime number was $p =$

$455470209427676832372575348833$ and three pairs of numbers were given of the form $(a, password \times g^a)$. Let the three pairs be $(a_1, b_1); (a_2, b_2); (a_3, b_3)$.

$(a_1, b_1) = (429, 431955503618234519808008749742)$
$(a_2, b_2) = (1973, 176325509039323911968355873643)$
$(a_3, b_3) = (7596, 984869714048619924872947226 13)$

$b_1 = (password * g^{a_1})$ mod p
$b_2 = (password * g^{a_2})$ mod p
$b_3 = (password * g^{a_3})$ mod p

Our main aim was to eliminate the $password$ and find g and then substitute the value of g in one of the above equations and solve for the password. So dividing the given equations was the best choice. For this first we calculated the modular inverses of b_1 and b_2:

$b_1^{-1} = 707499967902234717329046816 40$
$b_2^{-1} = 228947149478752602606353685125$

Now, let $b_{21} = (\frac{b_2}{b_1})\%p = (b_2 \times b_1^{-1})\%p$
Similarly, $b_{31} = (\frac{b_3}{b_1})\%p = (b_3 \times b_1^{-1})\%p$
and $b_{32} = (\frac{b_3}{b_2})\%p = (b_3 \times b_2^{-1})\%p$

So, we got three equations from these calculations :

1. $\frac{g^{a_2}}{g^{a_1}} = g^{1544} = b_{21} =$
$111590994894663139264552154672$
2. $\frac{g^{a_3}}{g^{a_1}} = g^{7167} = b_{31} =$
$110411376670918912626907526185$
3. $\frac{g^{a_3}}{g^{a_2}} = g^{5623} = b_{32} =$
$420413074251022028027270785553$

Let us consider equations 1 and 3. Exponent power of g in equations 1 and 3 are coprime. We used Extended Euclidean Algorithm to compute coefficients of Bézout's identity.
let c = 1544 and d = 5623. By Bézout's identity :

c*x + d*y = gcd (c, d) = gcd (1544 , 5623) = 1

here x and y are coefficients of Bézout's identity.
By the Extended Euclidean Algorithm, $(1544) \times (-2298) +$

$(5623) \times (631) = 1$

Therefore, $g = ((g^{1544})^{2298})^{-1} \times ((g^{5623})^{631}) = ((b_{21})^{2298})^{-1} \times ((b_{32})^{631})$
$g = g\%p = ((b_{21})^{2298})\%p)^{-1})\%p \times ((b_{32})^{631})\%p)$

$\implies g = [(1557511415488269554466967301 54)^{-1} \times 347267008389877298374017667230]\%p$
$\implies g = [(6367334591911148292811805 2957) \times 347267008389877298374017667230]\%p$
$\implies \boxed{\mathbf{g = 525650854179633110276943 39}}$

This satisfied the given hint that g is of the form $5\_\_\_50\_\_4\_\_\_\_\_31\_\_\_\_\_94\_\_9$

Now, substituting this value of g in the initial step, we get :

$password = [b_1 \times (g^{a_1})^{-1}]\%p$
$password = [(b_1\%p) \times ((g^{a_1})^{-1})\%p]\%p$
$\implies password = [4319555036182345198080087497 42 \times 442956820316148690889301696615]\%p$

Finally, the
$\boxed{\mathbf{Password = 13472154209765902984527 3957}}$

We have used modulus property : (a*b) % p = ((a% p) * (b % p)) % p
We have used fermat's little theroem for prime number p to calculate modular multiplicative inverse
$a^{p-1} \equiv 1(mod p)$

$a^{p-2} \equiv a^{-1}(mod p)$
References :
https://www.extendedeuclideanalgorithm.com/calculator.php
https://planetcalc.com/3311/
https://planetcalc.com/8326/

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

Maryam Raza Khan
Maulik Singhal
Pranshu Gaur

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