Q1 Team name

0 Points

cryptoEngineers

Q2 Commands

10 Points

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

1. go (to move in small chamber),
2. enter (to enter into dark underground chamber),
3. pick/pluck (to pluck the mushroom out of floor),
(Pressing c two times),
4. back (move back to small chamber),
5. give (to give the mushrooms plucked from underground chamber in small holes),
6. back,
7. back (2 backs to move to main chamber),
8. thrnxxtzy,
9. read (to read glass panel)

Q3 Analysis

50 Points

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

As we are in main chamber and saw an open door to another chamber. On applying command "go", we entered next little chamber. Now, "enter" command to enter the underground chamber. We saw mushrooms here, so pluck it by "pluck/pick" command and move back using "back" command. Now, provided the mushrooms into the holes using "give" command. Squeaky voice, then told us the magic words and also to speak it up in main chamber. So, used 2 "back" commands to reach main chamber and spoke up the magic words "thrnxxtzy". Door gets appeared and then used "read" command to read the text on glass panel.

Now, the analysis to figure out the password is as follows :

Given, Multiplicative group Z_p^*, where p is prime
Three Pairs of form (a, Password*g^a)

$Pair_1$: (324, 1122681535026353181496333631 5)
$Pair_2$: (2345, 919054866790027430083039122 0)
$Pair_3$: (9513, 413865262965561357081900049 7)
Let the second element of these pairs be $x1, x2, x3,$ as
$x1$ = 1122681535026353181496333631 5
$x2$ = 919054866790027430083039122 0
$x3$ = 413865262965561357081900049 7

p = 198070406285660843983859875 81

Using given pairs, we derived three equations
Password*g^{324} = $x1$
Password*g^{2345} = $x2$
Password*g^{9513} = $x3$

Applying Modular Arithmetic, above equations can be written as

Password*g^{324} ≡ $x1$ mod p ...eq(1)
Password*g^{2345} ≡ $x2$ mod p ...eq(2)

Password*g^{9513} ≡ $x3$ mod p ...eq(3)

From eq(2),

Password*g^{324}*g^{2021} ≡ $x2$ mod p

$x1$*g^{2021} ≡ $x2$ mod p

g^{2021} ≡ $(x1)^{-1}$*$x2$ mod p ....eq(4)

From eq(3),

Password*g^{324}*g^{9189} ≡ $x3$ mod p

$x1$*g^{9189} ≡ $x3$ mod p

g^{9189} ≡ $(x1)^{-1}$*$x3$ mod p ....eq(5)

Now, from eq(4) and eq(5), we calculated the value of g as follows ,

g^{9189} can be written as $(g^{2021})^4 * g^{1105}$. As we know the value of g^{9189} and g^{2021}, we get the value of g^{1105}

$\Rightarrow g^{1105} \equiv g^{9189} * ((g^{2021})^4)^{-1}$ mod p

Continuing the above step to further reduce g^{9189} using recently obtained value of g^{1105}

$\Rightarrow g^{9189} = (g^{1105})^8 * g^{349}$

Knowing the value of g^{1105} and g^{9189}, we get value of

$\Rightarrow g^{349} \equiv g^{9189} * ((g^{1105})^8)^{-1}$ mod p.

Likewise,

$\Rightarrow g^{9189} = (g^{349})^{26} * g^{115}$, from this we get $g^{115} \equiv g^{9189} * ((g^{349})^{26})^{-1}$ mod p

$\Rightarrow g^{9189} = (g^{115})^{79} * g^{104}$, from this we get $g^{104} \equiv g^{9189} * ((g^{115})^{79})^{-1}$ mod p

$\Rightarrow g^{9189} = (g^{104})^{88} * g^{37}$, from this we get $g^{37} \equiv g^{9189} * ((g^{104})^{88})^{-1}$ mod p

$\Rightarrow g^{9189} = (g^{37})^{248} * g^{13}$, from this we get $g^{13} \equiv g^{9189} * ((g^{37})^{248})^{-1}$ mod p

$\Rightarrow g^{9189} = (g^{13})^{706} * g^{11}$, from this we get $g^{11} \equiv g^{9189} * ((g^{13})^{706})^{-1}$ mod p

$\Rightarrow g^{9189} = (g^{11})^{835} * g^{4}$, from this we get $g^{4} \equiv g^{9189} * ((g^{11})^{835})^{-1}$ mod p

$\Rightarrow g^{9189} = (g^{4})^{2297} * g$, from this we get $g \equiv g^{9189} * ((g^{4})^{2297})^{-1}$ mod p

At the end, we get the value of $g = 192847283928500239481729$.

Now, substituting the value of g in eq(1),
$\Rightarrow$ password $\equiv (g^{324})^{-1} * x1$ mod p

we get $password = 360852885036840078603672 5$

NOTE :
1. Inverse is calculated using Fermat's little theorem,
a^{p-1} mod p ≡ 1
$a^{p-2} * a$ mod p ≡ 1
$a^{-1} \equiv a^{p-2}$ mod p
inverse.py contains the code of calculating inverse.
2. findG.py is code which calculates value of g using g^{9189} and g^{2021}.
3. findPassword.py is a code to calculate password using g and eq(1).

Q4 Password

10 Points

What was the final command used to clear this level?

360852885036840078603672 5