Q1 Team name

0 Points

NULL

Q2 Commands

10 Points

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

go, enter, pick, c, 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)

The problem statement is to find the solution to the following system of equations:

$$password * g^{324} = b_1 - (1)$$
$$password * g^{2345} = b_2 - (2)$$
$$password * g^{9513} = b_3 - (3)$$

where $password, g, b1, b2, b3 \in F_p^*$ and

$$p = 19807040628566084398385987581$$
$$b1 = 1122681535026353181496333631 5$$
$$b2 = 91905486679002743008303912 20$$
$$b3 = 41386526296556135708190004 97$$

Our strategy is to first find g and then substitute it in one of the equations to find $password$. To pursue this approach, we first eliminate $password$ and obtain equations which only involve g. Multiplying Equation 2 with the inverse of Equation 1 and

Equation 3 with inverse of Equation 2 gives us the following set of Equations.

$$g^{2021} = b_2 * b_1^{-1} - (4)$$
$$g^{7168} = b_3 * b_2^{-1} - (5)$$

The modular inverses b_1^{-1} and b_2^{-1} can be calculated using extended euclidean algorithm by solving the equations $p * x + b_i * y = gcd(p, b_i) = 1$ which gives $b_i^{-1} = y \ mod \ p$ or alternatively b_i^{-1} can be found using fermat's little theorem since $b_i^{p-1} = 1 \ mod \ p$, multiplying with b_i^{-1} on both sides gives $b_i^{-1} = b_i^{p-2} \ mod \ p$ and $b_i^{p-2} \ mod \ p$ can be calculated using binary exponentiation.

The next crucial observation is that $gcd(2021, 7168) = 1$ which guarantees that there exists an integer linear combination of 2021 and 7168 which equals 1 due to Bezout's Identity and one of such coefficients can be found using Extended Euclid Algorithm. Let x and y denote the coefficients obtained by using the Extended Euclidean Algorithm.

$$x * 2021 + y * 7168 = gcd(2021, 7168) = 1$$

Now exponentiating both sides of Equation 4 to the power x and Equation 5 to the power y and multiplying them gives us the following.

$$g^{x*2021+y*7168} = b_1^{-x} * b_2^{x-y} * b_3^{y}$$

which implies

$$g = b_1^{-x} * b_2^{x-y} * b_3^{y}$$

Now substituting this in Equation 1 gives us $password = b_1 * g^{-324}$.
The values of various quantities calculated as stated above are as follows

$$x = 439$$
$$y = -139$$
$$g = 19284728392850023948 1729$$

$$password = 360852885036840078603672 5$$

.
As we can see, the value of g obtained matches the pattern given in the hint.

The code for calculating these values using the Extended Euclidean Algorithm and Binary Exponentiation is attached in the code section below.

Q4 Password

10 Points

What was the final command used to clear this level?

360852885036840078603672 5

Q5 Codes

0 Points

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

1.py Download

```python
def extended_gcd(a, b):
    """returns gcd(a, b), s, r s.t. a * s + b * r == gcd(a, b)"""
    s, old_s = 0, 1
    r, old_r = b, a
    while r:
        q = old_r // r
        old_r, r = r, old_r - q * r
        old_s, s = s, old_s - q * s
    return old_r, old_s, (old_r - old_s * a) // b if b else 0


def modinv(a, m):
    """returns the modular inverse of a w.r.t. to m, works when a and m are coprime"""
    g, x, _ = extended_gcd(a % m, m)
    return x % m if g == 1 else None


def binpow(a, n, m):
    res = 1
```

```
    while n > 0:
        if n % 2 != 0:
            res = res*a % m
        a = a*a % m
        n = n//2
    return res


p = 19807040628566084398385987581

a1 = 324
a2 = 2345
a3 = 9513

b1 = 112268153502635318149633363 15
b2 = 91905486679002743008303912 20
b3 = 41386526296556135708190004 97


g, p1, p2 = extended_gcd(a2-a1, a3-a2)
g = binpow(b2*modinv(b1, p) % p, p1, p) * \
    binpow(b3*modinv(b2, p) % p, p-1+p2, p) % p
passwd = b1*binpow(g, p-1-324, p) % p

print(g)
print(passwd)
assert (passwd * binpow(g, a1, p) % p == b1)
assert (passwd * binpow(g, a2, p) % p == b2)
assert (passwd * binpow(g, a3, p) % p == b3)

```

Assignment 3

● UNGRADED

GROUP

A5 - SURYADEVARA SAI KRISHNA
A11 - GARIMELLA MOHAN RAGHU
AJAY PRAJAPATI
View or edit group

TOTAL POINTS

- / 70 pts

QUESTION 1

Team name — 0 pts

QUESTION 2

Commands — 10 pts

QUESTION 3

Analysis — 50 pts

QUESTION 4

Password — 10 pts

QUESTION 5

Codes — 0 pts