Q1 Team Name
0 Points

Lazarus

Q2 Commands
10 Points

List the commands used in the game to reach the ciphertext

go
enter
pick
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)

A group theory problem was given to us to clear this level. This problem mentioned that password for the level is a member of the multiplicative group of modulo p where $p = 455470209427676832372575348833$ is a prime number.

We were given 3 pairs of the form $(a, password * g^a)$.
We formed equations using the above pairs as

$$(password * g^{429}) \pmod p = 43195550361823451980800874 9742 \dots (i)$$
$$(password * g^{1973}) \pmod p = 17632550903932391196835587 3643 \dots (ii)$$
$$(password * g^{7596}) \pmod p = 98486971404861992487294722613 \dots (iii)$$

Let,

$$x_1 = 431955503618234519808008749742$$
$$x_2 = 176325509039323911968355873643$$
$$x_3 = 984869714048619924872947226 13$$

To get equations in only variable g we eliminate password from above equations :
Dividing iii by ii

$$\frac{g^{7596}}{g^{1973}} \equiv \frac{x_3}{x_2} \pmod p$$

As division operation is not defined in modulo arithmetic we take mod inverse instead

$$g^{7596} * g^{-1973} \equiv x_3 * (x_2^{-1}) \pmod p$$

$$g^{7596-1973} \equiv x_3 * x_2^{-1} \pmod p$$

$$g^{5623} \equiv x_3 * x_2^{-1} \pmod p \dots (iv)$$

Note - x^{-1} denotes the inverse of x in group Z_p^*
Similarly by dividing ii by i and iii by i

$$g^{1544} \equiv x_2 * x_1^{-1} \pmod p \dots (v)$$

$$g^{7167} \equiv x_3 * x_1^{-1} \pmod{p} \dots (vi)$$

As p is prime, inverse of all elements exists. If y is inverse of x then $x * y \equiv 1 \pmod{p}$.
Using Fermat's little theorem

$$a^{p-1} \equiv 1 \pmod{p}$$

Multiplying by a^{-1} on both sides

$$a^{-1} \equiv a^{p-2} \pmod{p}$$

Using above formula we calculate inverse :

$$x_1^{-1} = 707499967902234717329046816 40$$

$$x_2^{-1} = 228947149478752602606353685125$$

Substituting the value of x_2^{-1} and x_1^{-1} in equations iv, v, vi

$$g^{5623} \equiv 420413074251022028027270785553 \pmod{p} \dots$$

$$g^{1544} \equiv 11159099489466313926455215467 2 \pmod{p} \dots$$

$$g^{7167} \equiv 110411376670918912626907526185 \pmod{p} \dots$$

Multiplying both sides of equation vii by inverse of $(g^{1544})^3$

$$g^{5623} * ((g^{1544})^3)^{-1} \equiv 420413074251022028027270785553$$

$$g^{991} \equiv 161798558270556961732424822635$$

We iteratively reduce the power of g to 1

$$g^{7167} * ((g^{991})^{7})^{-1} \equiv 1104113766709189126269075261$$

$$g^{230} \equiv 263509268584013168241508095725$$

$$(g^{230})^{7} * (g^{1544})^{-1} \equiv (263509268584013168241508095$$

$$g^{66} \equiv 816670148923172141519678245$$

$$(g^{66})^{4} * (g^{230})^{-1} \equiv (816670148923172141519678245$$

$$g^{34} \equiv 454838375047265263248274620636$$

$$(g^{34})^{2} * (g^{66})^{-1} \equiv (454838375047265263248274620636)^{2}$$

$$g^{2} \equiv 108044907665466013935627786069$$

$$g^{991} * ((g^{2})^{495})^{-1} \equiv 161798558270556961732424822635$$

$$g \equiv 525650854179633110276943 39$$

Value of g computed above matches the hint (5___50__4_____31_____94__9) given for the value of g in

problem so we move ahead with this.

$$g = 525650854179633110276943 39$$

Substituting value of g in equation (i), we get:

$$(password * (525650854179633110276943 39)^{429}) \pmod{}$$

Multiplying both sides by inverse of g^{429}

$$password \equiv 43195550361823451980800874974 * 44295($$

$$password = 191337636400793823899716432097855887$$

Taking $\pmod{p}$

$$password = 13472154209765902984527 3957$$

Q4 Password

10 Points

What was the final command used to clear this level?

13472154209765902984527 3957

Q5 Codes

0 Points

Upload any code that you have used to solve this level

Assign3.ipynb Download

```
In [1]: import gmpy2
```

In [2]:
```
x1 = 43195550361823451980800874 9742
x2 = 17632550903932391196835587 3643
x3 = 98486971404861992487294722613
p = 45547020942767683237257534 8833
```

In [3]:
```
invx1 = gmpy2.invert(x1,p)
invx1
```

Out [3]:
```
mpz(70749996790223471732904681640)
```

In [4]:
```
invx2 = gmpy2.invert(x2,p)
invx2
```

Out [4]:
```
mpz(22894714947875260260635368 5125)
```

In [5]:
```
g5623 = (x3 * invx2)%p
g5623
```

Out [5]:
```
mpz(42041307425102202802727078 5553)
```

In [6]:
```
g1544 = (x2 * invx1)%p
g1544
```

Out [6]:
```
mpz(11159099489466313926455215 4672)
```

In [7]:
```
g7167 = (x3* invx1)%p
g7167
```

Out [7]:
```
mpz(11041137667091891262690752 6185)
```

In [8]:
```
g991 = (g5623 *
gmpy2.invert(pow(g1544,3,p),p))%p
g991
```

Out [8]:
```
mpz(16179855827055696173242482 2635)
```

In [9]:
```
g230 =
(g7167*gmpy2.invert(pow(g991,7,p),p))%p
g230
```

Out [9]:
```
mpz(26350926858401316824150809 5725)
```

In [10]:
```
g66 =
(pow(g230,7,p)*gmpy2.invert(g1544,p))%p
g66
```

Out [10]:
```
mpz(816670148923172141519678245 18)
```

In [11]:
```
g34 =
(pow(g66,4,p)*gmpy2.invert(g230,p))%p
g34
```

Out [11]:
```
mpz(45483837504726526324827462 0636)
```

In [12]:
```
g2 = (pow(g34,2,p)*gmpy2.invert(g66,p))%p
g2
```

Out [12]:
```
mpz(10804490766546601393562778 6069)
```

In [13]:
```
g = (g991*gmpy2.invert(pow(g2,495,p),p))%p
g
```

Out [13]:
```
mpz(52565085417963311027694339)
```

In [14]:
```
invg429 = gmpy2.invert(pow(g,429,p),p)
invg429
```

Out [14]:
```
mpz(44295682031614869088930169 6615)
```

In [15]:
```
password = (invg429*x1)%p
password
```

Out [15]:
```
mpz(13472154209765902984527 3957)
```

Assignment 3

GRADED

GROUP
Varun Vankudre
Aditya Loth
Harsh Agarwal
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

✔	+ 15 pts	Finding at least two distinct powers of g.
✔	+ 25 pts	Finding the values of g by repeated division or Extended Euclid's algorithm or any other method.
✔	+ 5 pts	The value of g is 525650854179633110276943 39
✔	+ 5 pts	Finding *password* using the information of g Password: 13472154209765902984527 3957
	+ 0 pts	Wrong
	+ 50 pts	Solving the assignment using an entirely different approach.

QUESTION 4
Password
10 / 10 pts

QUESTION 5
Codes
0 / 0 pts