Q1 Team Name

0 Points

Enigma

Q2 Commands

10 Points

List the commands used in the game to reach the ciphertext

go
enter
pluck
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)

T In this question, we have a multiplicative group,

$(Z_p, *)$

where p is prime and * is binary operation(modulo multiplication) in g, and we have tuples of the form

$(r, password * g^r)$

$Prime\ p = 455470209427676832372575348833$
The given pairs are:
$(429, 43195550361823451980800874 9742)$
$(1973, 17632550903932391196835587 3643)$
$(7596, 98486971404861992487294722613)$

Mathematical expression behind this: $h = g^{r_i} * password$ (will run i from 1 to 3). Given pairs can be expressed rs:

$g^{429} * password =$
$43195550361823451980800874 9742 = h1 \ ...(1)$
$g^{1973} * password =$
$17632550903932391196835587 3643 = h2 \ ...(2)$
$g^{7596} * password =$
$98486971404861992487294722613 = h3 \ ...(3)$

Using these equations we get:

Dividing (2) by (1),
$g^{1973-429} = g^{1544} = \frac{h2}{h1} mod\ p = b1(let)$
Dividing (3) by (2),
$g^{7596-1973} = g^{5623} = \frac{h3}{h2} mod\ p = b2(let)$
Dividing (3) by (1),
$g^{7596-429} = g^{7167} = \frac{h3}{h1} mod\ p = b3(let)$

Algorithm:

1. initialize q=1 mod p
2. for (i=n-1;i>=0;i--)

   $if(m_i == 1)$
   $set\ q = q * g\ mod\ p$
3. $q = q^2 mod\ p$
4. return q

Following computation helps to find g.

1. $c1 = \frac{b2}{(b1)^3} = g^{5623-3\times1544} = g^{991}$
2. $c2 = \frac{b3}{(c1)^7} = g^{7167-7\times991} = g^{230}$
3. $c3 = \frac{c1}{(c2)^4} = g^{991-4\times230} = g^{71}$
4. $c4 = \frac{c2}{(c3)^3} = g^{230-3\times71} = g^{17}$
5. $c5 = \frac{c1}{(c3)^14} = g^{991-14\times71} = g^{-3}$
6. $c6 = c4 * (c5)^5 = g^{17+5h(-3)} = g^2$
7. $c7 = c5 * (c6)^2 = g^{-3+4} = g$

Hence c7 = g. Modular reduction has been done after each step of the computation.

Now from given equation we can write

$password = h_i \cdot (g^{r_i})^{-1}$ mod p

For i = 1,

password = 43195550361823451980800874974 2 $* (g)^{429}$ mod p

Now, we perform the computation using the GP-PRRI calculator[**GP**]. Other freely available number theoretic libraries are NTL, GMP library. We put the command to find g and password.

p = 455470209427676832372575348833;

h1 = 43195550361823451980800874974 2;

h2 = 17632550903932391196835587364 3;

h3 = 98486971404861992487294722613;

b1 = Mod(h2/h1,p);

b2 = Mod(h3/h2,p);

b3 = Mod(h3/h1,p);

c1 = Mod(b2/(b1\^3),p);

c2 = Mod(b3/(c1\^7),p);

c3= Mod(c1/(c2\^4),p);

c4=Mod(c2/(c3\^3),p);

c5=Mod(c1/(c3\^14),p);

c6=Mod(c4*c5\^5,p);

c7=Mod(c6\^2*c5,p);

g=c7;

t=Mod(g\^429,p);

password=Mod(h1/q,p);

At the end of the computation, we got
g = 525650854179633110276943 39;
password: 13472154209765902984527 3957;

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

Gajender Sharma
Kajal Sethi
Pranshu Sahijwani
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