

We obtained three tuples of integers in the cipher text of the form  $(a, \text{password} * g^a)$ . Since, multiplication operation is from the group  $Z_p^*$  therefore it has to be done modulo  $p$ .

Let the password for the game be  $x \in Z_p^*$  and let the three tuples be  $(a, n_1)$ ,  $(b, n_2)$  and  $(c, n_3)$ . Therefore we will end up with three modular equations as shown below.

$$\begin{aligned}x * g^a &\equiv n_1 \pmod{p} \\x * g^b &\equiv n_2 \pmod{p} \\x * g^c &\equiv n_3 \pmod{p}\end{aligned}$$

Now, since  $\gcd(a, b) = 1$  therefore we can see that there exists a solution to the equation

$$\alpha \times a + \beta \times b + \gamma \times c = 0$$

Setting another constraint, on  $\alpha, \beta$  and  $\gamma$  i.e.

$$\alpha + \beta + \gamma = 1$$

, and solving it simultaneously with the above equation we will get

$$\beta \times (b - a) + \gamma \times (c - a) = -a$$

. Now, the last equation also has a solution since,  $\gcd(b - a, c - a) = 1$  in our case. Hence, we came up with the values of  $\beta$  and  $\gamma$  by solving the diophantine equation using Extended euclid's algorithm on this diophantine equation. On analysis using the C++ program, we got  $\beta = -204768$  and  $\gamma = 45036$ . Now, using the fact that sum of  $\alpha, \beta$  and  $\gamma$  is 1, we got  $\alpha = 159733$ .

Now, we did the following manipulations to obtain the final password or  $x$ .

$$\begin{aligned}x^\alpha \cdot g^{\alpha \cdot a} &\equiv n_1^\alpha \pmod{p} \\x^\beta \cdot g^{\beta \cdot b} &\equiv n_2^\beta \pmod{p} \\x^\gamma \cdot g^{\gamma \cdot c} &\equiv n_3^\gamma \pmod{p}\end{aligned}$$

Multiplying them together, we get

$$x^{\alpha+\beta+\gamma} \cdot g^{\alpha \cdot a + \beta \cdot b + \gamma \cdot c} \equiv n_1^\alpha \cdot n_2^\beta \cdot n_3^\gamma \pmod{p}$$

Plugging in the equations above for  $\alpha, \beta$  and  $\gamma$ , we get

$$x \equiv n_1^\alpha \cdot n_2^\beta \cdot n_3^\gamma \pmod{p}$$

Hence, we wrote a program to calculate the above expression modulo  $p$  and got the value of  $x$  to be 3608528850368400786036725.

$$\begin{aligned}x * g^a &\equiv n_1 \bmod p \\x * g^b &\equiv n_2 \bmod p \\x * g^c &\equiv n_3 \bmod p\end{aligned}$$

$$\begin{aligned}g^a &\equiv x^{-1} * n_1 \bmod p \\g^b &\equiv x^{-1} * n_2 \bmod p \\g^c &\equiv x^{-1} * n_3 \bmod p\end{aligned}$$

Again, as  $\gcd(a, b) = 1$ , there exists a solution to the equation

$$\alpha \times a + \beta \times b + c = 1$$

Solving the diophantine equation using Extended euclid's algorithm on this diophantine equation in  $\alpha$  and  $\beta$ ,

$$\alpha = 6953272, \beta = -204768$$

$$\begin{aligned}g^{a \cdot \alpha} &\equiv x^{-\alpha} * n_1^{\alpha} \bmod p \\g^{\beta \cdot b} &\equiv x^{-\beta} * n_2^{\beta} \bmod p \\g^c &\equiv x^{-1} * n_3 \bmod p\end{aligned}$$

Multiplying the above three modulo equations,

$$g^{a \cdot \alpha + \beta \cdot b + c} \equiv x^{-(\alpha + \beta + 1)} \cdot n_1^{\alpha} \cdot n_2^{\beta} \cdot n_3 \bmod p$$

Which simplifies to

$$g \equiv x^{-(\alpha + \beta + 1)} \cdot n_1^{\alpha} \cdot n_2^{\beta} \cdot n_3 \bmod p$$

Which gives us the value of  $g$  as 192847283928500239481729, which also fits into the template for  $g$  given in the message. Hence we conclude that our solution is correct.