

Let $x = password$

Given, $p = 19807040628566084398385987581$ and $Z_p^* = [1, p - 1]$ where p is prime

We have following three pairs of numbers of the form $(a, x * g^a)$:

- (i) (324, 11226815350263531814963336315)
- (ii) (2345, 9190548667900274300830391220)
- (iii) (9513, 4138652629655613570819000497)

Since $x, g \in Z_p^*$ (multiplicative group), after every multiplication operation, we have to take modulo with p .

So, we can write following three corresponding to each pairs of numbers :

- (i) $(x * g^{324}) \bmod p = 11226815350263531814963336315$
- (ii) $(x * g^{2345}) \bmod p = 9190548667900274300830391220$
- (iii) $(x * g^{9513}) \bmod p = 4138652629655613570819000497$

Let us assume following :

- $y1 = 11226815350263531814963336315$
- $y2 = 9190548667900274300830391220$
- $y3 = 4138652629655613570819000497$

So, we have following three equation :

$(x * g^{324}) \bmod p = y1$	$eq(1)$
$(x * g^{2345}) \bmod p = y2$	$eq(2)$
$(x * g^{9513}) \bmod p = y3$	$eq(3)$

For further analysis we will use following theorems and properties of Modular arithmetic:

Basic property 1: $(a * b) \bmod p = ((a \bmod p) * (b \bmod p)) \bmod p$

Basic property 2: if $a \bmod p = b \bmod p$
then $a^x \bmod p = b^x \bmod p$

We have used the above property without mentioning.

Also, all the exponents and inverse of g, x will belong to Z_p^*

Theorem 1: $a^{p-1} \bmod p = 1$ if $a \in Z_p^*$

Proof: Using Fermat's little theorem, $a^{p-1} \bmod p = 1$, when a is not divisible by p and p is prime.

Since all the numbers in Z_p^* are not divisible by p as all these numbers $\in [1, p-1]$, so holds $\forall a \in Z_p^*$

Theorem 2: $a^{-1} \bmod p = a^{p-2} \bmod p$ where p is prime

Proof: Using theorem 1 we can easily prove this.

Theorem 3: if $a \bmod p = b \bmod p$ and p is prime

then $a^{-1} \bmod p = b^{-1} \bmod p$

Proof: $a \bmod p = b \bmod p$

raise both sides to $(p-2)$ power

$$\implies (a \bmod p)^{p-2} \bmod p = (b \bmod p)^{p-2} \bmod p$$

$$\implies a^{p-2} \bmod p = b^{p-2} \bmod p \quad (\text{using basic property})$$

$$\implies a^{-1} \bmod p = b^{-1} \bmod p \quad (\text{using theorem 2})$$

Theorem 4: $(x * x^{-1}) \bmod p = 1$

Proof: By definition of modular multiplicative inverse.

So, now take multiplicative inverse(similar to theorem 3) on both side of $eq(1)$ we have :

$$(x^{-1} * (g^{324})^{-1}) \bmod p = y1^{-1} \bmod p \quad eq(4)$$

Now , we will multiply $eq(2)$ with $eq(4)$,we have

$$((x * g^{2345}) * (x^{-1} * (g^{324})^{-1})) \bmod p = (y2 * y1^{-1}) \bmod p$$

$$\implies ((x * x^{-1}) * g^{2345-324} * (g^{324} * (g^{324})^{-1})) \bmod p = (y2 * y1^{-1}) \bmod p$$

$$\implies g^{2021} \bmod p = (y2 * y1^{-1}) \bmod p \quad eq(5) \quad (\text{using theorem 4})$$

Similarly , we will $eq(3)$ $eq(4)$,we have

$$((x * g^{9513}) * (x^{-1} * (g^{324})^{-1})) \bmod p = (y3 * y1^{-1}) \bmod p$$

$$\implies ((x * x^{-1}) * g^{9513-324} * (g^{324} * (g^{324})^{-1})) \bmod p = (y3 * y1^{-1}) \bmod p$$

$$\implies g^{9189} \bmod p = (y3 * y1^{-1}) \bmod p \quad eq(6) \quad (\text{using theorem 4})$$

Now we have following :

$$g^{2021} \bmod p = (y2 * y1^{-1}) \bmod p \quad eq(5)$$

$$g^{9189} \bmod p = (y3 * y1^{-1}) \bmod p \quad eq(6)$$

So, to get the value of g from the above two equations.

Let we raise both side of $eq(5)$ to y power , i.e.

$$(g^{2021})^y \bmod p = (y2 * y1^{-1})^y \bmod p \quad eq(7)$$

and we raise both sides of $eq(6)$ to z power, i.e.

$$(g^{9189})^z \bmod p = (y3 * y1^{-1})^z \bmod p \quad eq(8)$$

Now , we will multiply $eq(7)$ with $eq(8)$, we have

$$g^{(2021*y+9189*z)} \bmod p = ((y2 * y1^{-1})^y * (y3 * y1^{-1})^z) \bmod p \quad eq(9)$$

so, to find the value of g^1 we need to find the integral value of y and z satisfying following equation

$$2021 * y + 9189 * z = 1$$

We solved the above equation by writing the code and trying out different values of y (we have attached the code). We get following values for y and z :

$$y = 632$$

$$z = -139 \text{ (negative means first take inverse of } eq(8) \text{ then multiply with } eq(7) \text{)}$$

Putting these value in $eq(9)$, we got the value of g , i.e

$$g \bmod p = 192847283928500239481729$$

$$\implies g = 192847283928500239481729 \quad (\text{ because } g \in Z_p^*)$$

Also the calculated value of g matches the given pattern.

Now , if we multiply both side of $eq1$ with $(g^{324})^{-1}$,we have

$$((x * g^{324}) * (g^{324})^{-1}) \bmod p = (y1 * (g^{324})^{-1}) \bmod p$$

$$\implies x \bmod p = (y1 * (g^{324})^{-1}) \bmod p \quad (\text{using Theorem 4})$$

$$\implies x = (y1 * (g^{324})^{-1}) \bmod p \quad eq(10) \quad (\text{because } x \in Z_p^*)$$

So, we putting the value of g and $y1$ in $eq(10)$, we get

$$x = 3608528850368400786036725$$

Since $x = password$

$$\text{So, } password = 3608528850368400786036725$$