11/19/22.

ASSIGNMENT-5.

(1.) Find the Discrete log. using Baby-Step-Giant-Step Alg.

(a) Given cyclic group $\mathbb{Z}_{29}^*$, and $2^8 \bmod 29 = 27$. Find $x = \log_2 27$ in $\mathbb{Z}_{29}^*$.

Sol:- From $\mathbb{Z}_{29}^* = |28| = q$

we know that in Baby Step-Giant Step,

$g^x = h$ then,

$g = 2,\ h = 27 \ \& \ q = |28|$

Now,

Step 1: Cut the group into intervals of size 't' (Giant-step) where, $t \simeq \lfloor \sqrt{q} \rfloor$.

$\therefore t \simeq \lfloor \sqrt{28} \rfloor$

$\therefore t \simeq 5.$

Now compute the points at intervals:

$g^0, g^t, g^{2t}, \ldots, g^{\lfloor q/t \rfloor * t}$.

$2^0 \bmod 29 = 1,\ 2^5 \bmod 29 = 3,\ 2^{10} \bmod 29 = 9,$

$2^{15} \bmod 29 = 27,\ 2^{20} \bmod 29 = 23,\ 2^{25} \bmod 29 = 11.$

step-2: compute t elements: $h*g^1, h*g^2, \ldots, h*g^t$
(Baby-step)

$27 * 2^1 \bmod 29 = 25$, $27 * 2^2 \bmod 29 = 21$,
$27 * 2^3 \bmod 29 = 13$, $27 * 2^4 \bmod 29 = 26$,
$27 * 2^5 \bmod 29 = 23$.

step-3: now, Find $h * g^i \stackrel{?}{=} g^{k*t}$ (For some $k>1$)

$27 * 2^5 = 2^{4*5}$

(since we Find a match btw Grain & Baby step at $2^{20} \bmod 29 = 23$ & $27 * 2^5 \bmod 29 = 23$)

step-4: now, compute $\log_g h = (k*t - i) \bmod q$

$\log_2 27 = (4 \times 5 - 5) \bmod 28$.

$\log_2 27 = 15 \bmod 28 \Rightarrow \log_2 27 = 15$

$\therefore x = 15$.

Checking: $2^{15} \bmod 29 = 27$.

(6.) Given cyclic group $\mathbb{Z}_{37}^*$, and $2^x \bmod 37 = 6$.
Find $x = \log_2 6$ in $\mathbb{Z}_{37}^*$.

sol:-

From $\mathbb{Z}_{37}^* = |36| = q$

we know that in Baby step-Grain step,
$g^x = h$ then,

$g = 2$, $h = 6$ & $q = |36|$

Now, step 1: Cut the group into intervals of size 't' (Giant-step) where, $t \simeq \lfloor \sqrt{q} \rfloor$.

$$\therefore t \simeq \lfloor \sqrt{36} \rfloor$$

$$\therefore t \simeq 6.$$

Now compute the points at intervals: $g^0, g^t, g^{2t}, \ldots, g^{\lfloor q/t \rfloor * t}$.

$2^0 \bmod 37 = 1$, $2^6 \bmod 37 = 27$, $2^{12} \bmod 37 = 26$,

$2^{18} \bmod 37 = 36$, $2^{24} \bmod 37 = 10$, $2^{30} \bmod 37 = 11$,

$2^{36} \bmod 37 = 1$.

step-2: (Baby-step) compute 't' elements: $h*g^1, h*g^2, \ldots, h*g^t$

$6 * 2^1 \bmod 37 = 12$, $6 * 2^2 \bmod 37 = 24$,

$6 * 2^3 \bmod 37 = 11$, $6 * 2^4 \bmod 37 = 22$,

$6 * 2^5 \bmod 37 = 7$, $6 \times 2^6 \bmod 37 = 14$.

step-3: now, Find $h * g^i \stackrel{?}{=} g^{k*t}$ (for some $k > 1$)

$6 * 2^3 = 2^{5*6}$

(since we find a match btw Giant & Baby step at $2^{30} \bmod 37 = 11$ & $6 * 2^3 \bmod 37 = 11$)

Step-4: Now, compute $\log_g h = (k*t - i) \bmod q$

$$\log_2 6 = (5 \times 6 - 3) \bmod 36.$$

$$\log_2 6 = 27 \bmod 36 \Rightarrow \log_2 6 = 27$$

$$\therefore x = 27.$$

Checking: $2^{27} \bmod 37 = 6.$

(c) Given cyclic group $\mathbb{Z}_{17}^*$, and $3^x \bmod 17 = 7$.

Find $x = \log_3 7$ in $\mathbb{Z}_{17}^*$.

Sol:- From $\mathbb{Z}_{17}^* = |16| = q.$

we know that in Baby step-Gain step, $g^x = h$ then,

$$g = 3,\ h = 7 \ \&\ q = |16|$$

Now,

Step 1: Cut the group into intervals of size t (Gaint-step) where, $t \approx \lfloor \sqrt{q} \rfloor$.

$$\therefore t \approx \lfloor \sqrt{16} \rfloor$$

$$\therefore t \approx 4.$$

Now compute the points at intervals: $[g^0, g^t, g^{2t}, \ldots, g^{\lfloor q/t \rfloor * t}]$.

$3^0 \bmod 17 = 1$, $3^4 \bmod 17 = 13$, $3^8 \bmod 17 = 16$,

$3^{12} \bmod 17 = 4$, $3^{16} \bmod 17 = 1$.

step-2: compute t elements: $h*g^1, h*g^2, \ldots, h*g^t$
(Baby-step)

$7 * 3^1 \bmod 17 = 4$, $7 * 3^2 \bmod 17 = 12$,
$7 * 3^3 \bmod 17 = 2$, $7 * 3^4 \bmod 17 = 6$.

step-3: now, Find $h * g^i \stackrel{?}{=} g^{k*t}$ (For some $k>1$)

$7 * 3^1 = 3^{3*4}$ (since we Find a match btw Gain & Baby step at $3^{12} \bmod 17 = 4$ & $7 * 3^1 \bmod 17 = 4$)

step-4: now, compute $\log_g h = (k*t - i) \bmod q$

$\log_3 7 = (3 \times 4 - 1) \bmod 16$.

$\log_3 7 = 11 \bmod 16 \Rightarrow \log_3 7 = 11$.

$\therefore x = 11$.

Checking:- $3^{11} \bmod 17 = 7$.

(2) Find discrete log using Pohlig-Hellman Alg.

(a) Given cyclic group Z_{11}^*, and $2^x \bmod 11 = 10$. Find $x = \log_2 10$ in Z_{11}^*.

Sol:- From $Z_{11}^* = |10| = q$.

and $g = 2$ & $h = 10$ from $g^x = h$.

We know that in Pohlig-Hellman,

$$\left(g^{q/q_i}\right)^x = \left(g^x\right)^{q/q_i} = h^{q/q_i}, \quad \forall\ i \in 1 \ldots k.$$

where $\{q_i\}$ are the co-primes of q.

Therefore,

$$q = |10|$$

$$\therefore q_i = \{5, 2\}$$

q_{i_1} q_{i_2}

Now, H_1:

$$\left(g^{10/5}\right)^{x_1} \bmod 11 = h^{10/5} \bmod 11.$$

$$\left(2^2\right)^{x_1} \bmod 11 = h^2 \bmod 11$$

$$\left(2^2\right)^{x_1} \bmod 11 = 10^2 \bmod 11$$

$$\left(4 \bmod 11\right)^{x_1} = 100 \bmod 11$$

$$4^{x_1} \bmod 11 = 1$$

$$4^{x_1} \equiv 1 \bmod 11$$

Now, H_2:

$$(g^{10/2})^{x_2} \bmod 11 = h^{10/2} \bmod 11$$

$$(g^5)^{x_2} \bmod 11 = h^5 \bmod 11$$

$$(2^5)^{x_2} \bmod 11 = 10^5 \bmod 11$$

$$(32 \bmod 11)^{x_2} = 10.$$

$$10^{x_2} \equiv 10 \bmod 11.$$

We know, $|H_1| = q_1 = 5$; $|H_2| = q_2 = 2$.

Now, we use Extended Chinese Remainder Theorem (CRT):

$$x = [(x_1 \bmod q_1), (x_2 \bmod q_2), \ldots, (x_K \bmod q_K)]$$

$\forall\ i \in 1 \ldots K$ (K is no. of subgroups)

then, we get:

$$x = [(4^{x_1} \equiv 1 \bmod 11), (10^{x_2} \equiv 10 \bmod 11)]$$

Solving, $x = [(0 \bmod 5), (1 \bmod 2)]$

(Since, $4^{x_1} = 1$ is satisfied if $x_1 = 0$ &
$10^{x_2} = 10$ is satisfied if $x_2 = 1$)

Solving we get, $x = 5$ which satisfies the condition.

Checking: $2^5 \bmod 11 = 10$.

(6.) Given cyclic group, $\mathbb{Z}^*_{31}$, and $3^x \bmod 31 = 12$.

Find $x = \log_3 12$ in $\mathbb{Z}^*_{31}$.

Sol:- From $\mathbb{Z}^*_{31} = |30| = q$.

and $g = 3$ & $h = 12$ from $g^x = h$.

We know that in Pohlig-Hellman,

$$\left(g^{q/q_i}\right)^x = \left(g^x\right)^{q/q_i} = h^{q/q_i}, \quad \forall\, i \in 1 \ldots 15.$$

where $\{q_i\}$ are the co-primes of q.

Therefore,

$$q = |30|$$

$$\therefore q_i = \{\underbrace{5}_{q_{i1}} * \underbrace{3}_{q_{i2}} * \underbrace{2}_{q_{i3}}\}$$

Now, H_1:

$$\left(g^{30/5}\right)^{x_1} \bmod 31 = h^{30/5} \bmod 31.$$

$$\left(3^6\right)^{x_1} \bmod 31 = 4^6 \bmod 31.$$

$$(729)^{x_1} \bmod 31 = 12^6 \bmod 31$$

$$(729 \bmod 31)^{x_1} = (12^3 \times 12^3) \bmod 31$$

$$(16)^{x_1} \bmod 31 = 2$$

$$\therefore 16^{x_1} \equiv 2 \bmod 31$$

now, H_2: $\left(g^{30/3}\right)^{x_2} \bmod 31 = h^{30/3} \bmod 31.$

$$(3^{10})^{x_2} \bmod 31 = 12^{10} \bmod 31$$

$$25^{x_2} \bmod 31 = 25$$

$$\therefore 25^{x_2} \equiv 25 \bmod 31.$$

now, H_3: $\left(g^{30/2}\right)^{x_3} \bmod 31 = h^{30/2} \bmod 31.$

$$(3^{15})^{x_3} \bmod 31 = 12^{15} \bmod 31.$$

$$30^{x_3} \bmod 31 = 30$$

$$\therefore 30^{x_3} \equiv 30 \bmod 31.$$

we know, $|H_1| = q_1 = 5; |H_2| = q_2 = 3, |H_3| = q_3 = 2.$

now, we use extended Chinese Remainder Theorem (CRT):

$x = [(x_1 \bmod q_1), (x_2 \bmod q_2), \ldots, (x_K \bmod q_K)]$

$\forall\ i \in 1 \ldots K$ (K is no. of subgroups)

then, we get:

$$x = [(16^{x_1} = 2 \bmod 31), (25^{x_2} = 25 \bmod 31), (30^{x_3} = 30 \bmod 31)]$$

Solving, $x = [(4 \bmod 5), (1 \bmod 3), (1 \bmod 2)]$

Solving, we get $x = 19$, satisfies the condition.

Checking: $3^{19} \bmod 31 = 12$.

(c) Given cyclic group, $\mathbb{Z}_{23}^*$, and $5^8 \bmod 23 = 15$.
Find $x = \log_5 15$ in $\mathbb{Z}_{23}^*$.

Sol: From $\mathbb{Z}_{23}^* = |22| = q$.
and $g = 5$; $h = 15$ from $g^x = h$.

We know that in Pohlig-Hellman,

$$(g^{q/q_i})^x = (g^x)^{q/q_i} = h^{q/q_i}, \quad \forall\, i \in 1 \ldots 15.$$

where $\{q_i\}$ are the co-primes of q.

Therefore,

$$q = |22|$$

$$\therefore q_i = \{11 * 2\}$$

q_{i1} $\quad$ q_{i2}

Now, for i:

$$(g^{22/11})^{x_1} \bmod 23 = h^{22/11} \bmod 23$$

$$(5^2)^{x_1} \bmod 23 = 15^2 \bmod 23$$

$$(25 \bmod 23)^{x_1} = 18$$

$$2^{x_1} \equiv 18 \bmod 23$$

Now, H_2: $\left(g^{22/2}\right)^{x_2} \bmod 23 = h^{22/2} \bmod 23$.

$(5^{11})^{x_2} \bmod 23 = 15^{11} \bmod 23$.

$22^{x_2} \equiv 22 \bmod 23$.

We know, $|H_1| = q_1 = 11$; $|H_2| = q_2 = 2$.

Now, we use extended Chinese Remainder Theorem (CRT):

$x = [(x_1 \bmod q_1), (x_2 \bmod q_2), \ldots, (x_K \bmod q_K)]$

$\forall\ i \in 1 \ldots K$ (K is no. of subgroups)

then, we get:

$x = [(2^{x_1} = 18 \bmod 23), (22^{x_2} = 22 \bmod 23)]$

Solving, $x = [(6 \bmod 11), (1 \bmod 2)]$

Now, solving we get $x = 17$ satisfies the condition.

Checking: $5^{17} \bmod 23 = 15$.

11/20/22.

(3.) Consider a group Z_{23}^*, and a message $M = 10$.

Encrypt 'M' using ElGamal Encryption scheme to obtain ciphertext C. Now decrypt 'C' to verify you get 'M' back.

Sol:- From $Z_{23}^* = |22| = 9$.

Given, $M = 10$.

Now we have to find generator 'g' of group 'G'.

$G = Z_{23}^* = \{1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17, 18, 19, 20, 21, 22\}$

For $a = 2$: $2^0 \bmod 23 = 1$

$2^1 \bmod 23 = 2$

$2^2 \bmod 23 = 4$

$2^3 \bmod 23 = 8$

$2^4 \bmod 23 = 16$

$2^5 \bmod 23 = 9$

$2^6 \bmod 23 = 18$

$2^7 \bmod 23 = 13$

$2^8 \bmod 23 = 3$

$2^9 \bmod 23 = 6$

$2^{10} \bmod 23 = 12$

$2^{11} \bmod 23 = 1$

$2^{12} \bmod 23 = 2$

$2^{13} \bmod 23 = 4$

$2^{14} \bmod 23 = 8$

$2^{15} \bmod 23 = 16$

$2^{16} \bmod 23 = 9$

$2^{17} \bmod 23 = 18$

$2^{18} \bmod 23 = 13$

$2^{19} \bmod 23 = 3$

$2^{20} \bmod 23 = 6$

$2^{21} \bmod 23 = 12$.

∴ The elements of the Group a=2 are,

{1, 2, 3, 4, 6, 8, 9, 12, 13, 16, 18}

∴ The Group a=2 do not have all the elements of the set that are present in Z^*_{23},

and Hence 2 is not a Generator.

For a=3: $3^0 \bmod 23 = 1$

$3^1 \bmod 23 = 3$

$3^2 \bmod 23 = 9$

$3^3 \bmod 23 = 4$

$3^4 \bmod 23 = 12$

$3^5 \bmod 23 = 13$

$3^6 \bmod 23 = 16$

$3^7 \bmod 23 = 2$

$3^8 \bmod 23 = 6$

$3^9 \bmod 23 = 18$

$3^{10} \bmod 23 = 8$

$3^{11} \bmod 23 = 1$

$3^{12} \bmod 23 = 3$

$3^{13} \bmod 23 = 9$

$3^{14} \bmod 23 = 4$

$3^{15} \bmod 23 = 12$

$3^{16} \bmod 23 = 13$

$3^{17} \bmod 23 = 16$

$3^{18} \bmod 23 = 2$

$3^{19} \bmod 23 = 6$

$3^{20} \bmod 23 = 18$

$3^{21} \bmod 23 = 8$

∴ The elements of the Group a=3 are,

{1, 2, 3, 4, 6, 8, 9, 12, 13, 16, 18}.

∴ The Group a=3 do not have all the elements of the set that are present in Z^*_{23}, and

Hence 3 is not a Generator.

For $a=4$: $4^0 \bmod 23 = 1$

$4^1 \bmod 23 = 4$

$4^2 \bmod 23 = 16$

$4^3 \bmod 23 = 18$

$4^4 \bmod 23 = 3$

$4^5 \bmod 23 = 12$

$4^6 \bmod 23 = 2$

$4^7 \bmod 23 = 8$

$4^8 \bmod 23 = 9$

$4^9 \bmod 23 = 13$

$4^{10} \bmod 23 = 6$

$4^{11} \bmod 23 = 1$

$4^{12} \bmod 23 = 4$

$4^{13} \bmod 23 = 16$

$4^{14} \bmod 23 = 18$

$4^{15} \bmod 23 = 3$

$4^{16} \bmod 23 = 12$

$4^{17} \bmod 23 = 2$

$4^{18} \bmod 23 = 8$

$4^{19} \bmod 23 = 9$

$4^{20} \bmod 23 = 13$

$4^{21} \bmod 23 = 6$

∴ The elements of the Group $a=4$ are,

$\{1, 2, 3, 4, 6, 8, 9, 12, 13, 16, 18\}$

∴ The Group $a=4$, do not have all the elements of the set, that are present in $\mathbb{Z}_{23}^*$, and

Hence, 4 is not a generator.

For, $a=5$: $5^0 \bmod 23 = 1$

$5^1 \bmod 23 = 5$

$5^2 \bmod 23 = 2$

$5^3 \bmod 23 = 10$

$5^4 \bmod 23 = 4$

$5^5 \bmod 23 = 20$

$5^6 \bmod 23 = 8$

$5^7 \bmod 23 = 17$

$5^8 \bmod 23 = 16$

$5^9 \bmod 23 = 11$

$5^{10} \bmod 23 = 9$

$5^{11} \bmod 23 = 22$

$5^{12} \bmod 23 = 18$

$5^{13} \bmod 23 = 21$

$5^{14} \bmod 23 = 13$

$5^{15} \bmod 23 = 19$

$5^{16} \bmod 23 = 3$

$5^{17} \bmod 23 = 15$

$5^{18} \bmod 23 = 6$

$5^{19} \bmod 23 = 7$

$5^{20} \bmod 23 = 12$

$5^{21} \bmod 23 = 14$

∴ The elements of the group, $a = 5$ are,

$\{1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17, 18, 19, 20, 21, 22\}$

∴ The group, $a = 5$ has all the elements present in the set $\mathbb{Z}_{23}^*$ and hence 5 is a generator.

Hit upon checking all the numbers in the set $\mathbb{Z}_{23}^*$ but since group, $a = 5$ is the first generator of set $\mathbb{Z}_{23}^*$ and hence $g = 5$.

- Now, we pick x from $\mathbb{Z}_{23}^*$ randomly; $x = 2$
  - Find $h = g^x$

$$h = 5^2$$

∴ we have $PK = (G, g, q, h)$ & $SK = (G, g, q, x)$

$\therefore PK = (23, 5, 22, 5^2)$ & $SK = (23, 5, 22, 2)$

- **Encryption scheme:**

we know that in ElGamal,

- we pick y from Z_{23}^* randomly; $y = 2$.
- find $c = (g^y, h^y \cdot m) \Rightarrow (g^y, (5^2)^y \cdot m)$

$$c = ((5^2 \bmod 23), (5^4 \bmod 23)(10))$$

- **Decryption scheme:** let it be c_1, let it be c_2

we know that in ElGamal,

- $m = \dfrac{(h^y \cdot m)}{g^{yx}}$

$$\therefore m = \frac{c_2}{(c_1)^x}$$

now substitute the c_2 & c_1 in m,

$$\frac{(5^4 \bmod 23)(10)}{(5^2 \bmod 23)^2} = \frac{(5^4 \bmod 23)(10)}{(5^2)^2 \bmod 23}$$

$$\therefore \frac{(5^4 \bmod 23)(10)}{5^4 \bmod 23} = 10.$$

$\therefore$ we successfully decrypt c to verify, we get back the m.

(4.) Compute $4^{23} \bmod 187$, and $9^{36} \bmod 101$, using square-and-multiply method.

Sol:- We write the exponents in their binary values.

Therefore, for $4^{23} \bmod 187$,

I write exponent of 23 in binary as,

10111

(1, 10, 101, 1011, 10111)

which are also written as (1, 2, 5, 11, 23).

DO, $4^1 \bmod 187 = 4$.

DO, $4^2 \bmod 187 = 16$.

DO, $4^5 \bmod 187 = (4^2 \times 4^2 \times 4) \bmod 187$

$= (4^2 \bmod 187 \times 4^2 \bmod 187 \times 4 \bmod 187) \bmod 187$

$= 1024 \bmod 187$

$= 89$.

DO, $4^{11} \bmod 187 = (4^5 \times 4^5 \times 4) \bmod 187$

$= (4^5 \bmod 187 \times 4^5 \bmod 187 \times 4 \bmod 187) \bmod 187$.

$= (89 \times 89 \times 4) \bmod 187$

$= 81.$

DD, $4^{23} \bmod 187 = (4^{11} \times 4^{11} \times 4) \bmod 187$

$= (4^{11} \bmod 187 \times 4^{11} \bmod 187 \times 4 \bmod 187) \bmod 187$

$= (81 \times 81 \times 4) \bmod 187$

$= 64.$

FOR, $9^{36} \bmod 101.$

$\Rightarrow$ write exponent of 36 in binary as,

100100

(1, 10, 100, 1001, 10010, 100100)

which are also written as, (1, 2, 4, 5, 18, 36).

DD, $9^1 \bmod 101 = 9.$

DD, $9^2 \bmod 101 = 81.$

DD, $9^4 \bmod 101 = (9^2 \times 9^2) \bmod 101 = (9^2 \bmod 101 \times 9^2 \bmod 101) \bmod 101.$

$= (81 \times 81) \bmod 101$

$= 6561 \bmod 101$

$= 97.$

Do, $9^5 \bmod 101 = (9^2 \times 9^2 \times 9) \bmod 101$

$= (9^2 \bmod 101 \times 9^2 \bmod 101 \times 9 \bmod 101) \bmod 101.$

$= (81 \times 81 \times 9) \bmod 101$

$= 873 \bmod 101$

$= 75.$

Do, $9^{18} \bmod 101 = (9^5 \times 9^5 \times 9^5 \times 9^2 \times 9) \bmod 101$

$= (9^5 \bmod 101 \times 9^5 \bmod 101 \times 9^5 \bmod 101 \times 9^2 \bmod 101 \times 9 \bmod 101) \bmod 101.$

$= (75 \times 75 \times 75 \times 81 \times 9) \bmod 101$

$= 31.$

Do, $9^{36} \bmod 101 = (9^{18} \times 9^{18}) \bmod 101$

$= (9^{18} \bmod 101 \times 9^{18} \bmod 101) \bmod 101$

$= (31 \times 31) \bmod 101$

$= 961 \bmod 101$

$= 52.$