10/18/22.

Discrete Log :-

$g^x \bmod q = h$

Given, h, g, q, find x

over $\mathbb{Z}_q^*$; $x \in \mathbb{Z}_q^*$, $g, h \in \mathbb{Z}_q^*$.

Num Theory – 6 :-

(Public key) ← $PK = (N, e)$

(Shared key) ← $SK = (N, P, Q)$

RSA Decryption :-

Needs, ↘ to decrypt

decryption $(C, N, e, P, Q) \rightarrow y$

$C^d \pmod N \rightarrow y$.

↓ (after getting d, to find y)

(To find d) ← $e \cdot d \bmod \phi(n) = 1$

where, $\phi(n) = (P-1)(Q-1)$.

Example of square-and-multiply :-

(1) Find $5^{20} \bmod 35$.

$20 = 10100$

$(1, 10, 101, 1010, 10100)$

↓ ↓ ↓ ↓ ↓

1 2 5 10 20

DO, $5^1 \bmod 35 = \underline{5}$.

DO, $5^2 \bmod 35 = (5^1 \cdot 5^1) \bmod 35 = 25 \bmod 35 = \underline{25}$.

DO, $5^5 \bmod 35 = (5^2 \cdot 5^2 \cdot 5^1) \bmod 35$

$= (25 \cdot 25 \cdot 5) \bmod 35$

$= 3125 \bmod 35 = \underline{10}$.

DO, $5^{10} \bmod 35$

$= (5^5 \cdot 5^5) \bmod 35$

$= 100 \bmod 35 = \underline{30}$.

DO, $5^{20} \bmod 35$

$= (5^{10} \cdot 5^{10}) \bmod 35$.

$= (30 \cdot 30) \bmod 35 = 900 \bmod 35 = \underline{25}$

10/20/22.

Pohlig-Hellman Example:-

(1) $x^x \bmod 31 = 26$; find x.

$(p = 31)$

(3) $g^x \bmod p = h$ (26)

$(g^x)^{q/q_i} \bmod p = h^{(q/q_i)}$

$q = |\mathbb{Z}_{31}^*|$; $q_i = \mathbb{Z}_i^*$; $i \in \{2, 3, 5\}$

$\mathbb{Z}_N^* \simeq \mathbb{Z}_p^* \times \mathbb{Z}_q^*$

$\mathbb{Z}_N^* \simeq \mathbb{Z}_{x_1}^* \times \mathbb{Z}_{x_2}^* \times \mathbb{Z}_{x_3}^* \times \ldots \times \mathbb{Z}_{x_n}^*$.

where, $N = (x_1 \cdot x_2 \cdot x_3 \cdot \ldots \cdot x_n)$

Baby-Step-Giant-Step Example:-

(See slide no: 9, 10, 11, 12).

Left Side - Baby
Right Side - Giant

$$h * g^i = g^{k \cdot t}$$

$$h = \frac{g^{k \cdot t}}{g^i}$$

$$h = g^{(kt - i)}$$

So, $\log_g h = (kt - i) \bmod q$.