

09/22/22: Groups:-

Group Properties and tricks:-

use this method if and only if  $\log$  is in the group and the exponential is greater than the length of the group.

$$\text{If } a < 1, a(\text{mod } b) = a \quad (\text{Since } a, b \in \mathbb{Z}^+)$$

Num Theory - 4:-

Cyclic Groups:-

$$\mathbb{Z}_5^* = \{1, 2, 3, 4\} \text{ Since,}$$

$\hookrightarrow (\mathbb{Z}_p^* = \{1, 2, \dots, p-1\})$ .  $\left( \mathbb{Z}_p^* \text{ is a cyclic group when } p \text{ is a prime number.} \right)$

$$\text{If } \mathbb{Z}_5 = \{0, 1, 2, 3, 4\} \text{ Since,}$$

$\hookrightarrow (\mathbb{Z}_p = \{0, 1, \dots, p-1\})$ .

Discrete Logarithms:-

$$h = g^x (\text{mod } p)$$

$$x = \log_g h (\text{mod } p) ; x \in \{0, \dots, p-1\}$$

09/27/22: CDH problem (Computational Diffie-Hellman Problem):-

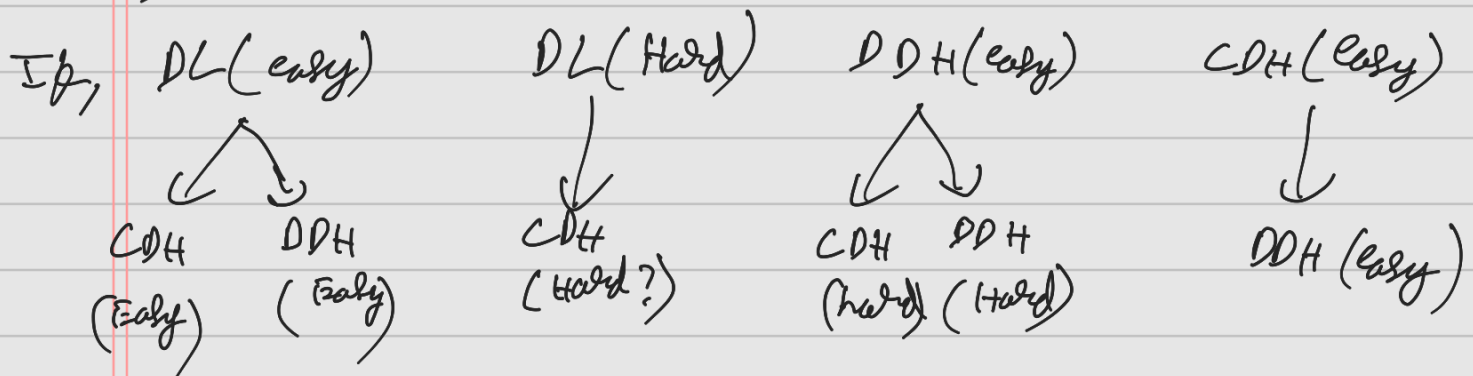
$$h_1 = g^{x_1}, \quad h_2 = g^{x_2}$$

$$x_1 = \log_g h_1 \pmod{p}$$

$$x_2 = \log_g h_2 \pmod{p}$$

$$\underline{(g^{x_2})^{x_1}}$$

Diffie-Hellman Problems:-



Group Generation Algorithm:-

$$G = (h^{x_2 = (p-1)/q} \pmod{p})$$