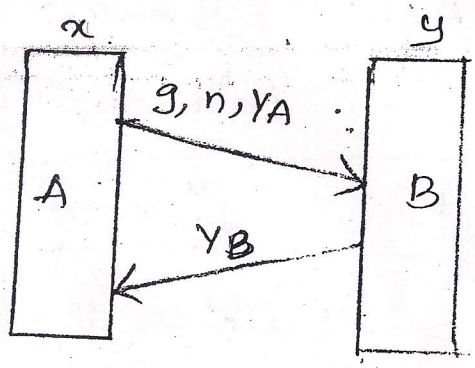
UNIT - III

* Diffie - Hellman Secret key exchange :

X → private
Y → public



$Y_A = g^x \bmod n$

$K_{AB} = Y_B^x \bmod n$

$= (g^y \bmod n)^x \bmod n$

$= g^{xy} \bmod n$

$Y_B = g^y \bmod n$

$K_{BA} = Y_A^y \bmod n$

$= (g^x \bmod n)^y \bmod n$

$= g^{xy} \bmod n$

$\therefore K_{AB} = K_{BA}$

This algorithm is used to distribute secret key b/w A & B. Both A & B assumes their private keys x & y which are kept secret.

* There are two global parameters **g, n** are considered
* A calculates his public key Y_A as,

$$Y_A = g^x \bmod n$$

* A sends the global parameters & public key (Y_A) to B

* B also calculates his public key Y_B as,

$$Y_B = g^y \bmod n$$

* B sends Y_B as response to A.

* A calculates shared secret key K_{AB} as,

$$K_{AB} = Y_B^x \bmod n$$

$$= (g^y \bmod n)^x \bmod n$$

$$\boxed{K_{AB} = g^{xy} \bmod n}$$

* Similarly, B calculates the shared secret key K_{BA} as,

$$K_{BA} = Y_A^y \bmod n$$

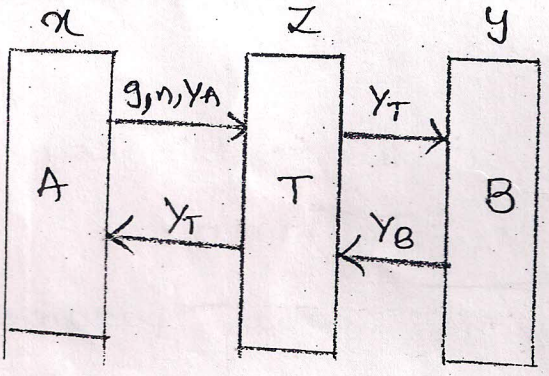
$$= (g^x \bmod n)^y \bmod n$$

$$\boxed{K_{BA} = g^{xy} \bmod n}$$

* Drawback :

This algorithm suffers with middle man attack.

* Middle man attack :



Public key Calculations :

At A :

$$Y_A = g^a \bmod n$$

At T :

$$Y_T = g^z \bmod n$$

At B :

$$Y_B = g^y \bmod n$$

Secret key Calculations :

$$k_{AT} = Y_T^a \bmod n$$

$$= (g^z \bmod n)^a \bmod n$$

$$= g^{az} \bmod n$$

$$k_{TA} = Y_A^z \bmod n$$

$$= (g^a \bmod n)^z \bmod n$$

$$= g^{az} \bmod n$$

$$\boxed{k_{AT} = k_{TA}}$$

$$k_{TB} = Y_B^z \bmod n$$

$$= (g^y \bmod n)^z \bmod n$$

$$= g^{yz} \bmod n$$

$$k_{BT} = Y_T^y \bmod n$$

$$= (g^z \bmod n)^y \bmod n$$

$$= g^{yz} \bmod n$$

$$\boxed{k_{TB} = k_{BT}}$$