**Deffie Hellman Key Exchange**

**Alice Bob Evil Eye**

Alice and Bob exchange a Prime (P) and a Generator (G) in clear-text,

such that P > G and G is Primitive Root of P

G = 7 , P = 11

Evil Eve sees

G = 7 , P = 11

Alice generates a random number : XA

XA = 6 (Secret)

Bob generates a random number : XB

XB = 9 (Secret)

YA = G XA ( mod P )

YA = 7 6 ( mod 11 )

YA = 4

YB = G XB ( mod P )

YB = 7 9 ( mod 11 )

YB = 8

Alice receives YB = 8 in clear-text

Bob receives YA = 4 in clear-text

Evil Eye sees

YA = 4 , YB = 8

Secret Key = YB XA ( mod P )

Secret Key = 8 6 ( mod 11 )

Secret Key = 3

Secret Key = YA XB ( mod P )

Secret Key = 4 9 ( mod 11 )

Secret Key = 3

Step 1

Step 2

Step 3

Step 4



