→ not an encryption Algorithm
→ used to exchange key b/w 2 users

Diffie-Hellman Key Exchange

Date

a is Primitive root of b if
we will use asymmetric Algo/encryption to exchange secret key
a mod b, a^2 mod b, a^3 mod b ... a^{b-1} mod b

Select α
$\alpha < q$ and Primitive root of q

Alice (A)	Bob (B)
① q → must be prime	① q
② $\alpha < q$ & Primitive	② $\alpha < q$ & Primitive
③ $X_A < q$ (Private key)	③ $X_B < q$ (Private key)
④ $Y_A = \alpha^{X_A} \bmod q$ (Public key)	④ $Y_B = \alpha^{X_b} \bmod q$ (Public key)

X ⇒ Private key
Y ⇒ Public key

Share key

Y_B → Alice
Y_A → Bob

Alice: $K = Y_B^{X_A} \bmod q$ → symmetric key
Bob: $K = Y_A^{X_B} \bmod q$ → symmetric key