Diffie-Hellman Key Exchange (DH Algorithm)

- First public-key type scheme proposed by Diffie & Hellman in 1976
- a practical method for public exchange of a secret key
- > used in a number of commercial products

Diffie-Hellman Key Exchange

- > a public-key distribution scheme
 - establish a common key known only to the two participants

两个用户安全的交换一个密钥 以便于以后的信息加密

> security depends on the difficulty of computing discrete logarithms

依赖于计算离散对数的难度

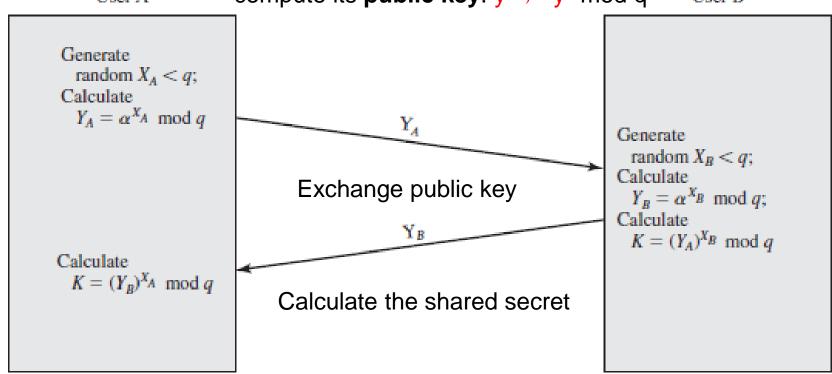
Diffie-Hellman Key Exchange Algorithm

users agree on global parameters:

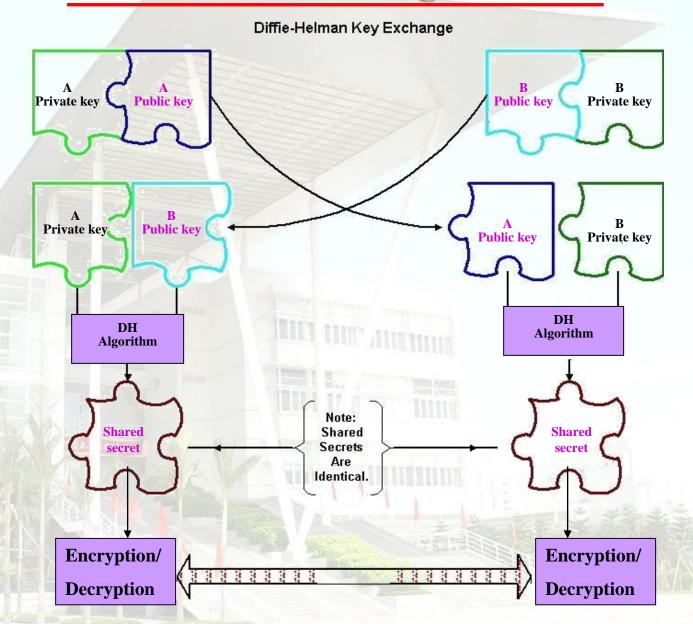
q, a each user generates its key

chooses a secret key : x^A , x^B < q

User A compute its **public key**: y^A, y^B mod q User B



Diffie-Hellman Algorithm



Diffie-Hellman Key Exchange

shared secret for users A & B is K:

$$K = y_A^{x_B} \mod q$$

$$= (a^{x_A} \mod q)^{x_B} \mod q$$

$$= (a^{x_A})^{x_B} \mod q$$

$$= (a^{x_B})^{x_A} \mod q$$

$$= (y_B^{x_A})^{x_A} \mod q$$

$$= y_B^{x_A} (which A can compute)$$



Alice

Alice and Bob share a prime number q and an integer α , such that $\alpha < q$ and α is a primitive root of q

Alice generates a private key X_A such that $X_A < q$

Alice calculates a public key $Y_A = \alpha^{X_A} \mod q$

Alice receives Bob's public key *YB* in plaintext

Alice calculates shared secret key $K = (Y_B)^{X_A} \mod q$





Bob

Alice and Bob share a prime number q and an integer α , such that $\alpha < q$ and α is a primitive root of q

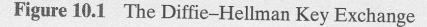
Bob generates a private key X_B such that $X_B < q$

Bob calculates a public key $Y_B = \alpha^{X_B} \mod q$

Bob receives Alice's public key Y_A in plaintext

Bob calculates shared secret key $K = (Y_A)^{X_B} \mod q$





Diffie-Hellman Example

users A & B who wish to swap keys:

- \triangleright agree on prime q=353 and a=3
- ✓ select random secret keys:

A chooses $x_A=97$, B chooses $x_B=233$

> compute respective public keys:

$$y_A = 3^{97} \mod 353 = 40$$
 (A)

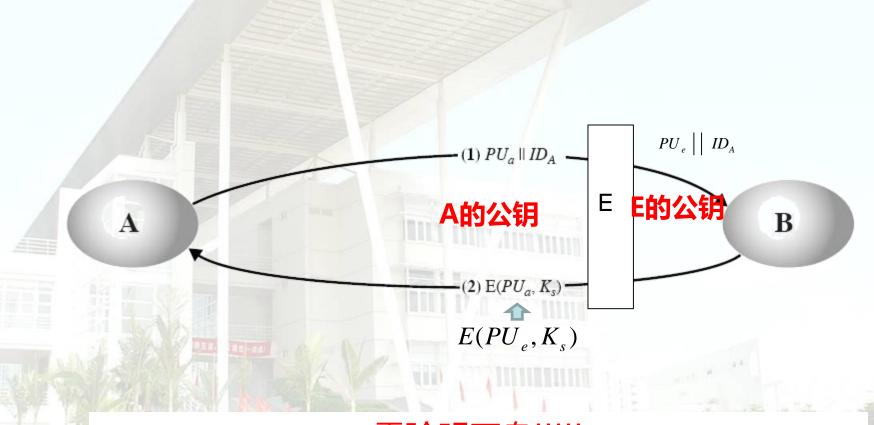
$$y_B = 3^{233} \mod 353 = 248$$
 (B)

> compute shared secret as:

$$K_{AB} = y_B^{XA} \mod 353 = 248^{97} = 160$$
 (A)

$$K_{AB} = y_A^{x_B} \mod 353 = 40^{233} = 160$$
 (B)

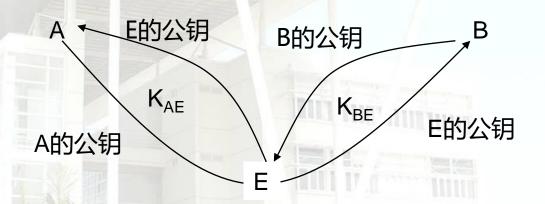
The-man-in-the-middle 中间人攻击



需验明正身!!!!!

Key Exchange

vulnerable to The-man-in-the-middle Attack
 中间人攻击



·authentication of the keys is needed

(需验明正身!!!!!)

