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

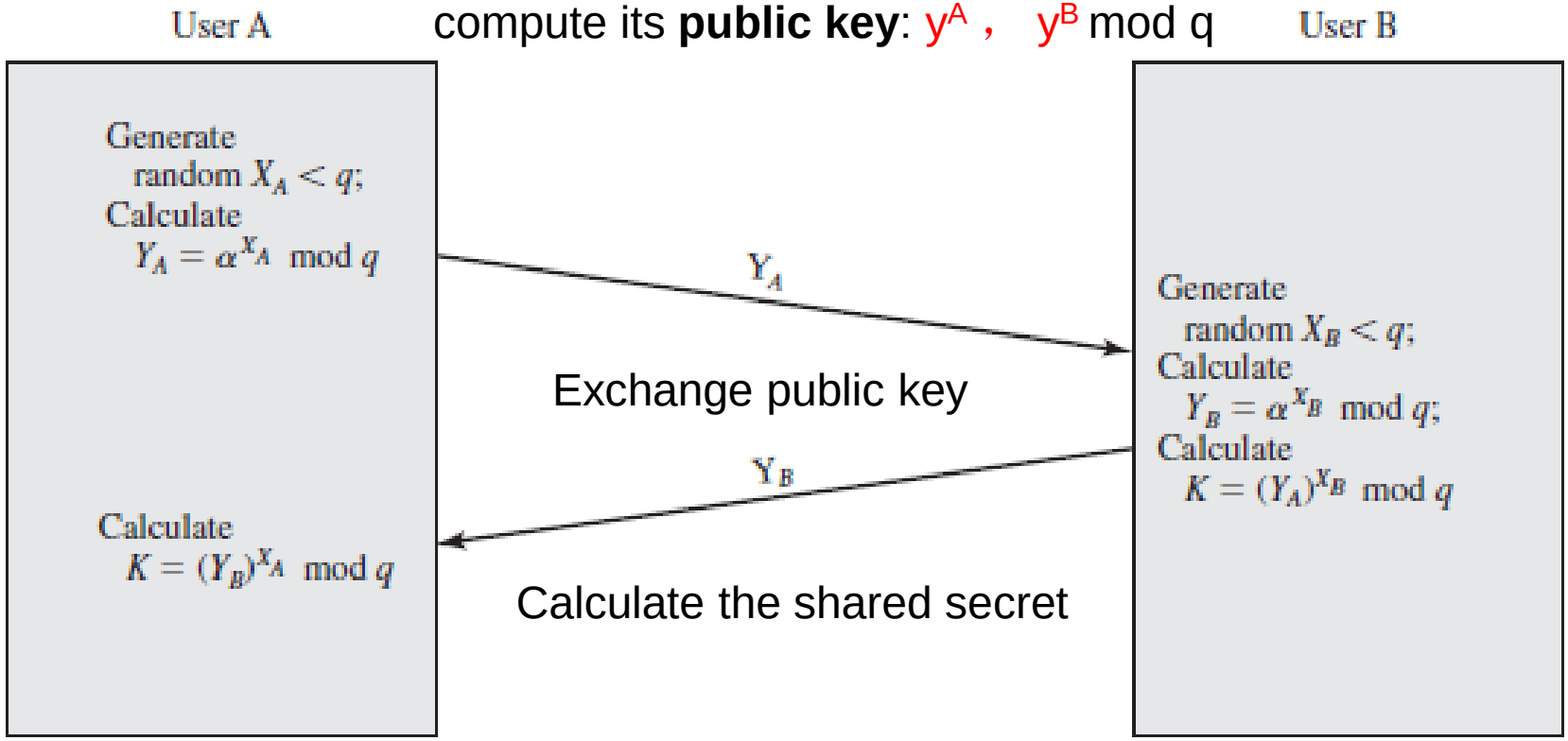
users agree on global parameters:

q， a

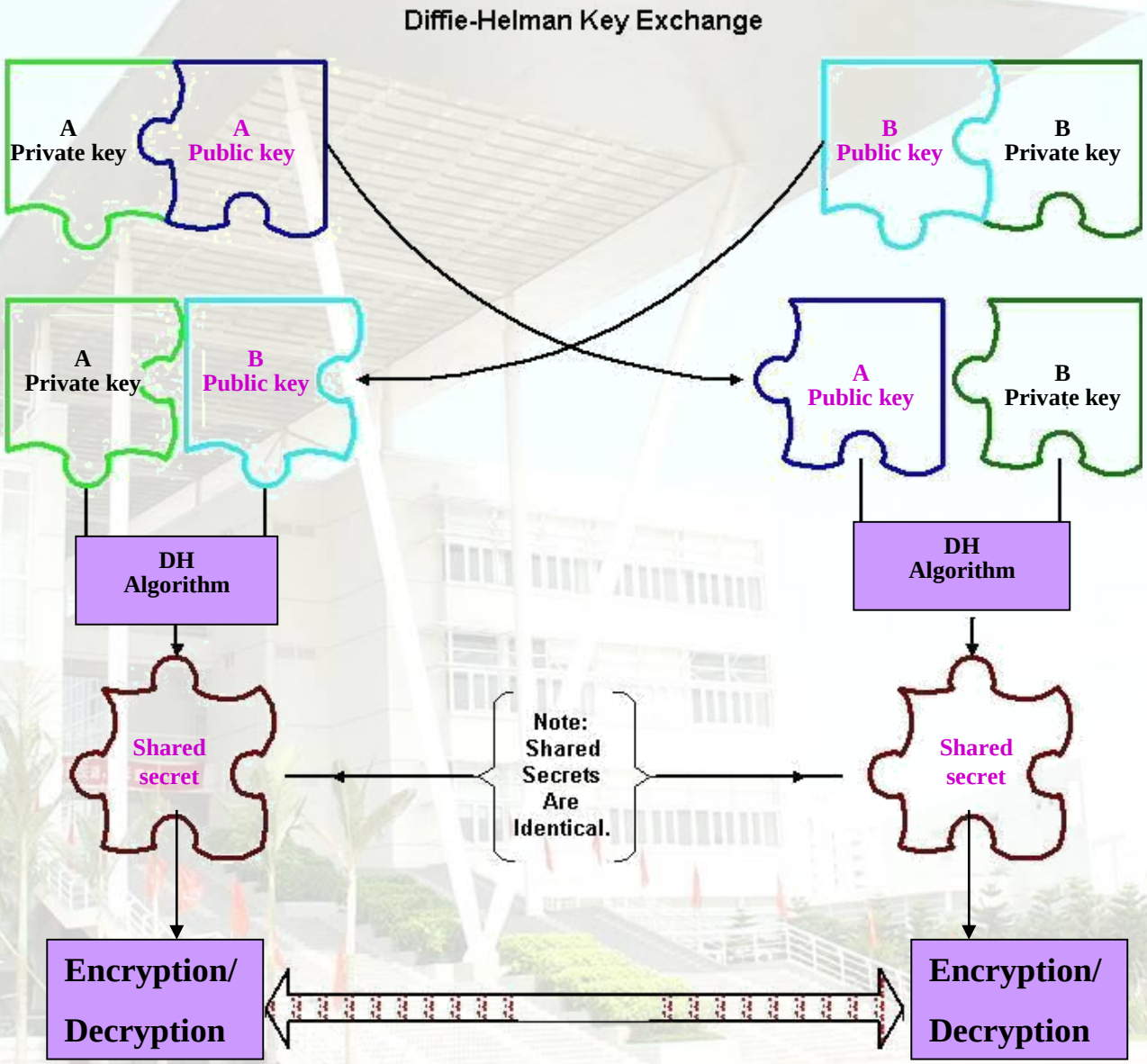
each user generates its key

chooses a secret key : x^A ， x^B < q

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



Diffie-Hellman Algorithm



Diffie-Hellman Key Exchange

shared secret for users A & B is K:

$$
\begin{aligned}
K &= y_A^{\,x_B} \bmod q \\
&= (a^{x_A} \bmod q)^{x_B} \bmod q \\
&= (a^{x_A})^{x_B} \bmod q \\
&= (a^{x_B})^{x_A} \bmod q \\
&= y_B^{\,x_A} \text{ (which } \mathbf{A} \text{ can compute)}
\end{aligned}
$$

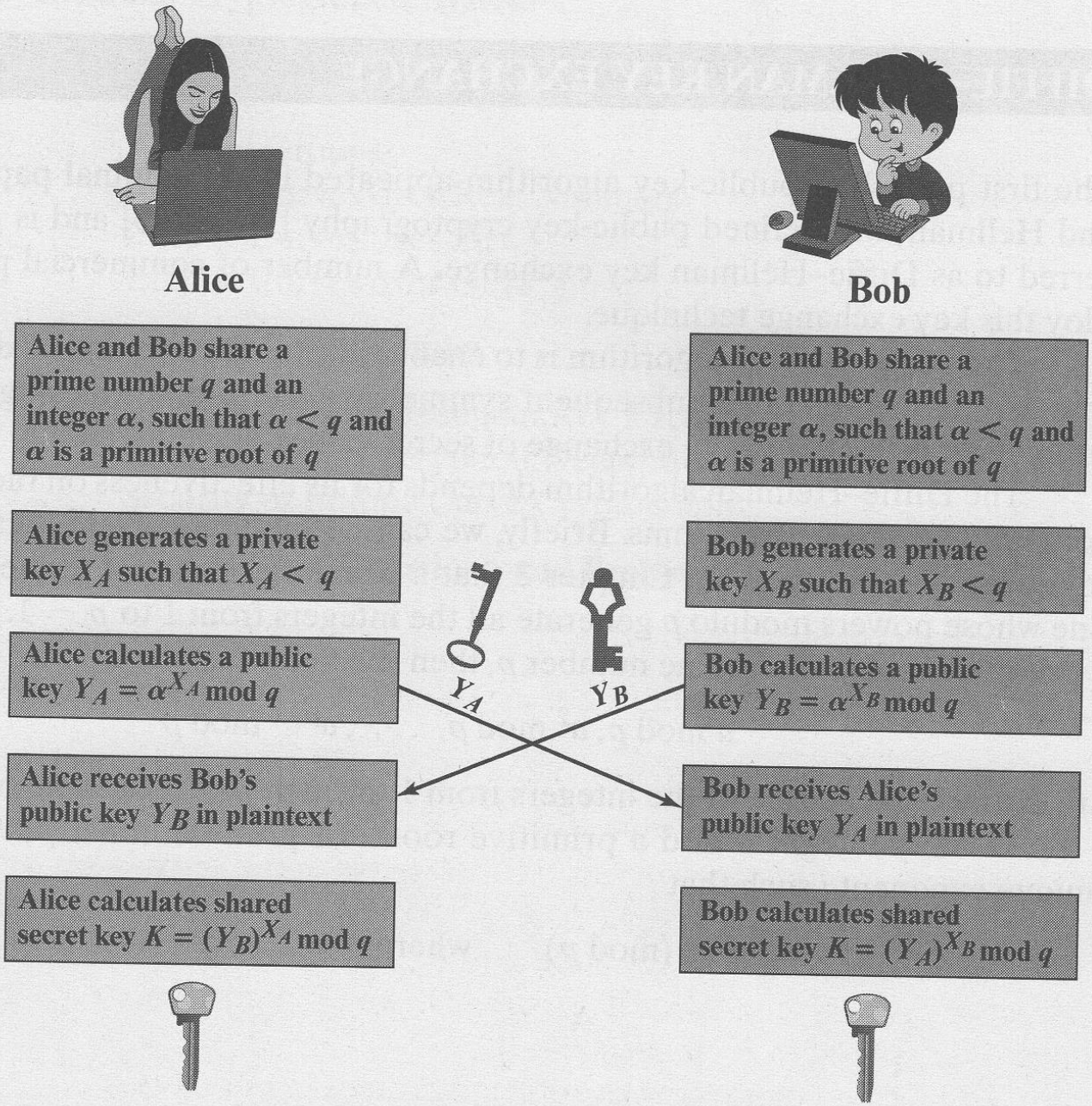


Figure 10.1 The Diffie–Hellman Key Exchange

Diffie-Hellman Example

users A & B who wish to swap keys:

- 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:

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

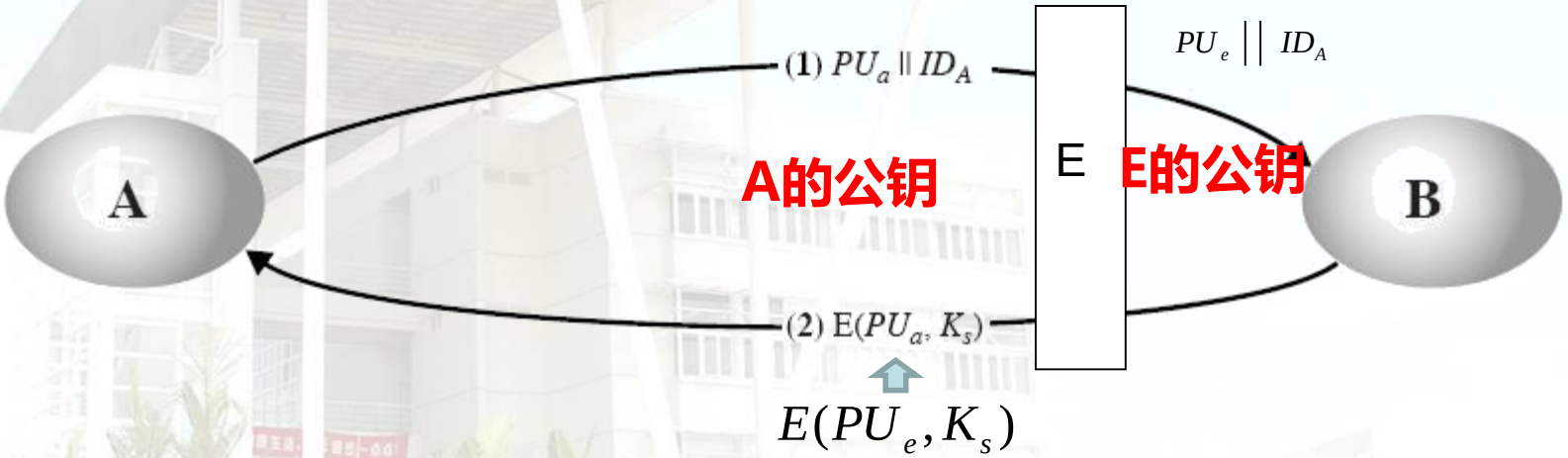
  $y_B = 3^{233} \bmod 353 = 248$ (B)

- compute shared secret as:

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

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

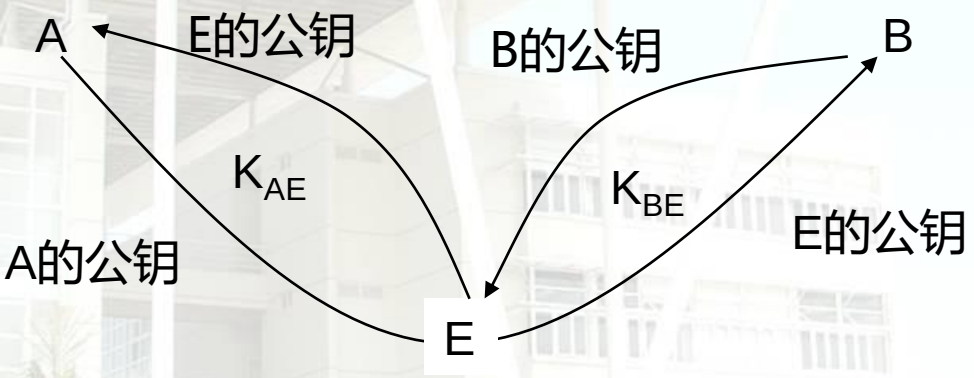
The-man-in-the-middle 中间人攻击



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!!!!!)

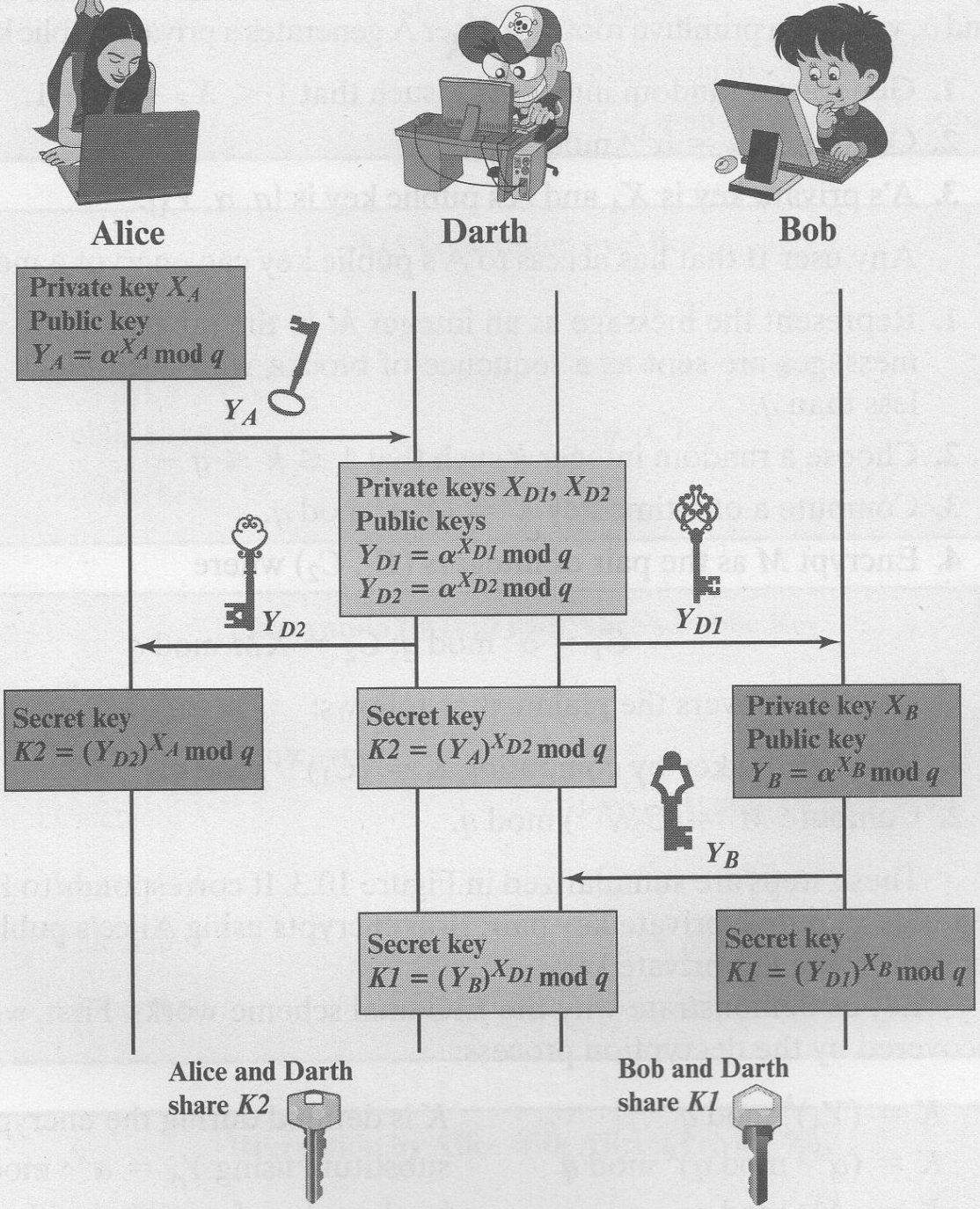


Figure 10.2 Man-in-the-Middle Attack