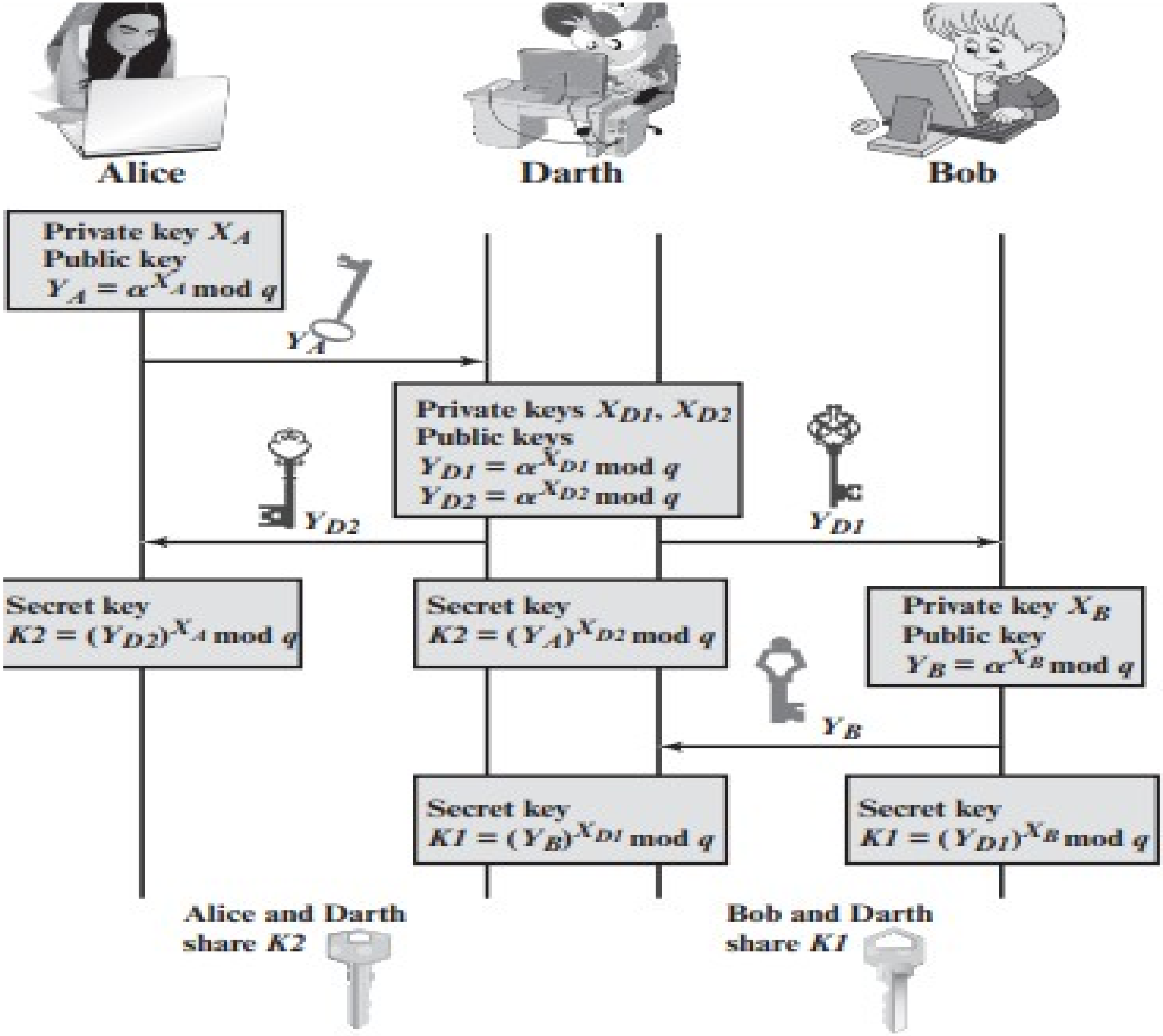
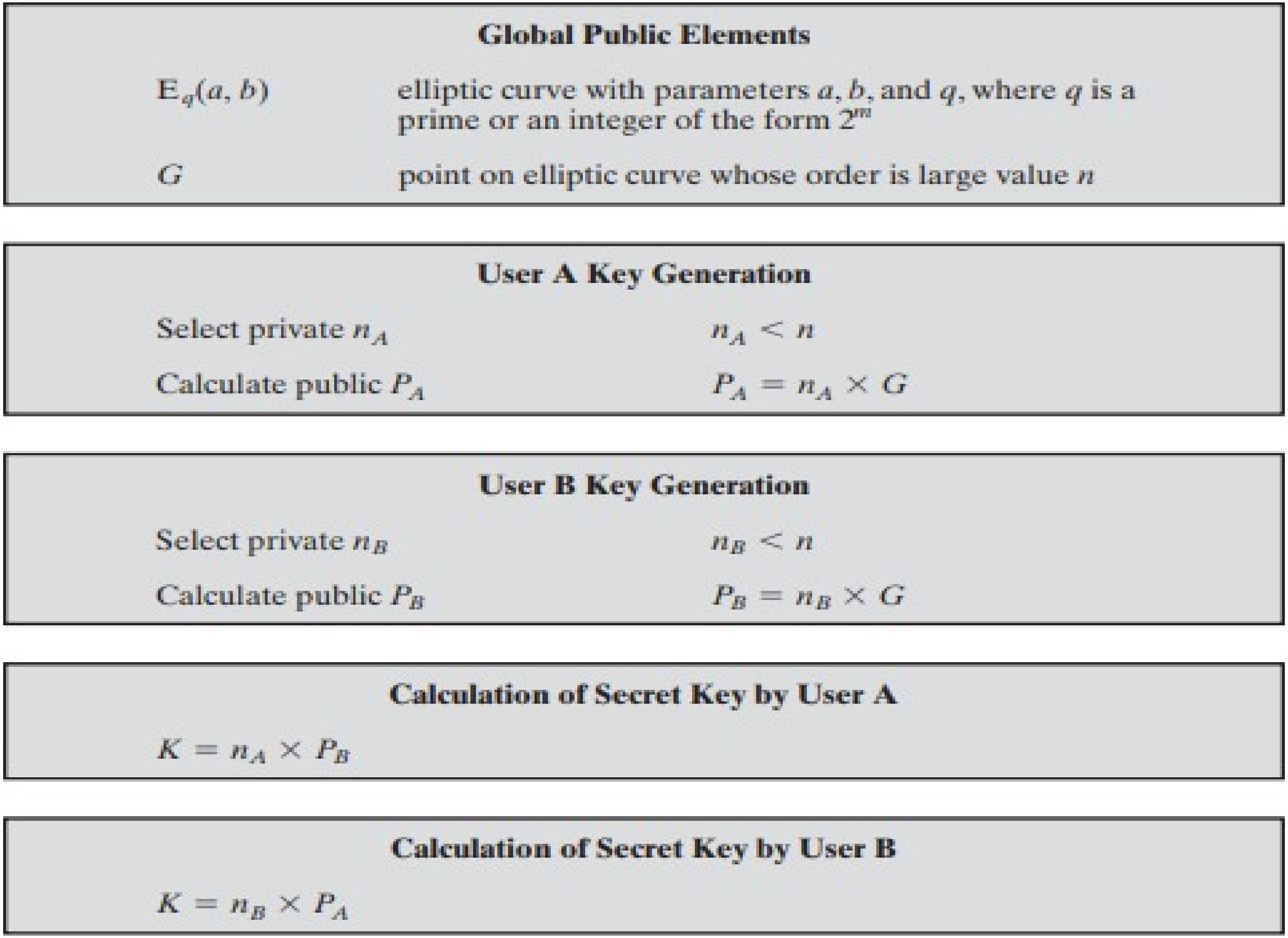

Alice
Darth
Bob
Private key $X_A$
Public key
$Y_A = \alpha^{X_A} \bmod q$
$Y_A$
Private keys $X_{D1}$, $X_{D2}$
Public keys
$Y_{D1} = \alpha^{X_{D1}} \bmod q$
$Y_{D2} = \alpha^{X_{D2}} \bmod q$
$Y_{D2}$
$Y_{D1}$
Secret key
$K2 = (Y_{D2})^{X_A} \bmod q$
Secret key
$K2 = (Y_A)^{X_{D2}} \bmod q$
Private key $X_B$
Public key
$Y_B = \alpha^{X_B} \bmod q$
$Y_B$
Secret key
$K1 = (Y_B)^{X_{D1}} \bmod q$
Secret key
$K1 = (Y_{D1})^{X_B} \bmod q$
Alice and Darth
share $K2$
Bob and Darth
share $K1$

igure 10.2 Man-in-the-Middle Attack



**Global Public Elements**

| | |
|---|---|
| $E_q(a, b)$ | elliptic curve with parameters $a$, $b$, and $q$, where $q$ is a prime or an integer of the form $2^m$ |
| $G$ | point on elliptic curve whose order is large value $n$ |

**User A Key Generation**

| | |
|---|---|
| Select private $n_A$ | $n_A < n$ |
| Calculate public $P_A$ | $P_A = n_A \times G$ |

**User B Key Generation**

| | |
|---|---|
| Select private $n_B$ | $n_B < n$ |
| Calculate public $P_B$ | $P_B = n_B \times G$ |

**Calculation of Secret Key by User A**

$K = n_A \times P_B$

**Calculation of Secret Key by User B**

$K = n_B \times P_A$

Figure 10.7 ECC Diffie–Hellman Key Exchange

- The cryptosystem parameters are E11(1, 6) and G = (2,7). B’s private key is nB = 7.
- Find B’s public key PB.
- A wishes to encrypt the message Pm = (10, 7) and chooses the random value k = 3. Determine the cipher text Cm.