GLOBAL EDITION

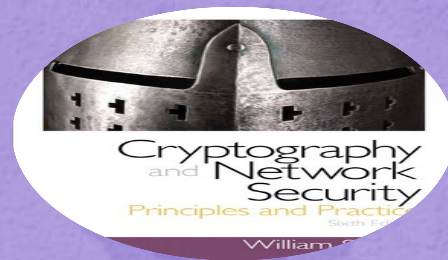
Cryptography and Network Security

Principles and Practice

SEVENTH EDITION

William Stallings

Pearson



Chapter 10

Other Public-Key Cryptosystems

Diffie-Hellman Key Exchange

- First published public-key algorithm
- A number of commercial products employ this key exchange technique
- Purpose is to enable two users to securely exchange a key that can then be used for subsequent symmetric encryption of messages
- The algorithm itself is limited to the exchange of secret values
- Its effectiveness depends on the difficulty of computing discrete logarithms

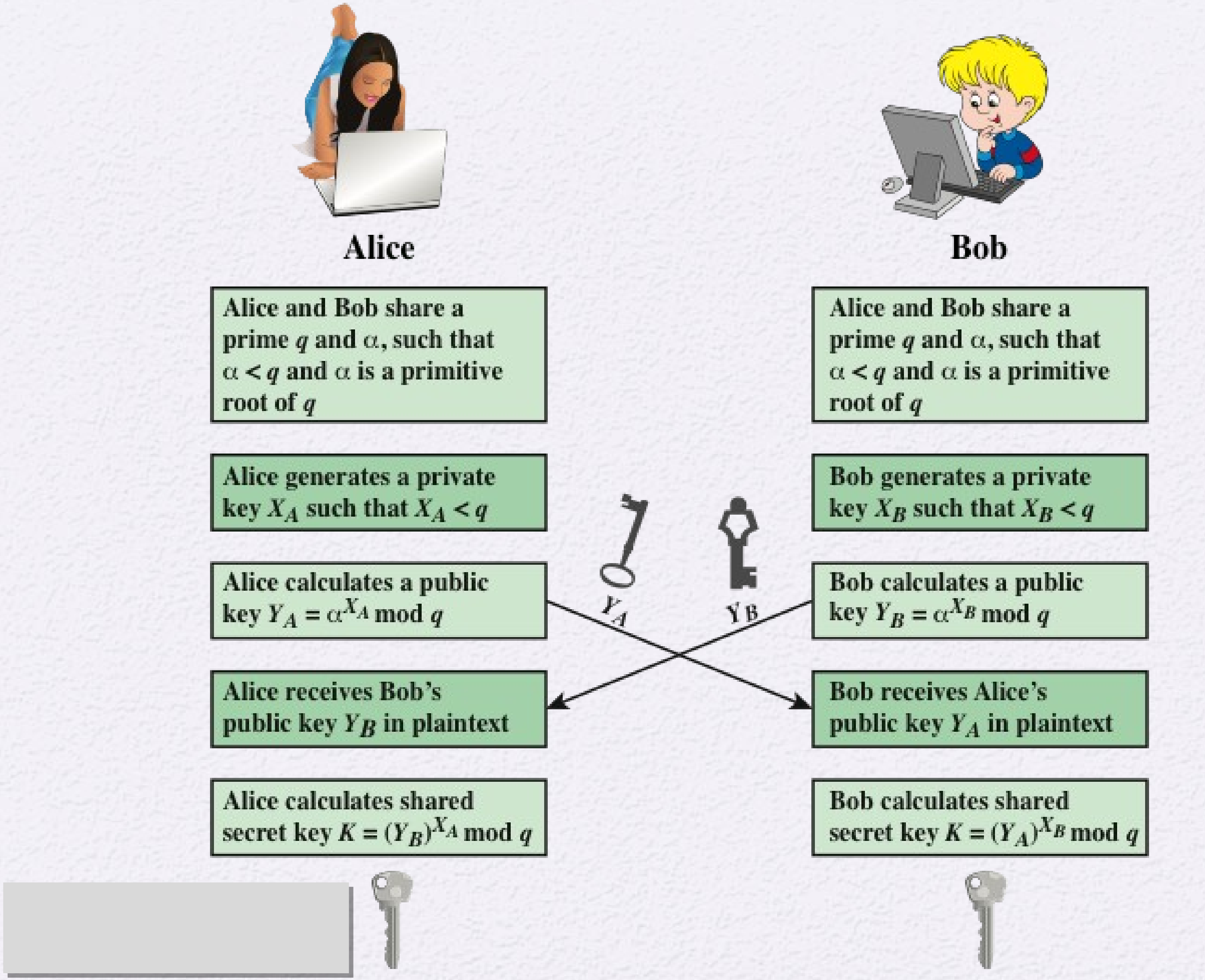


Figure 10.1 Diffie-Hellman Key Exchange

Let

ALICE

$X_A = 4$

BOB

$X_B = 3$

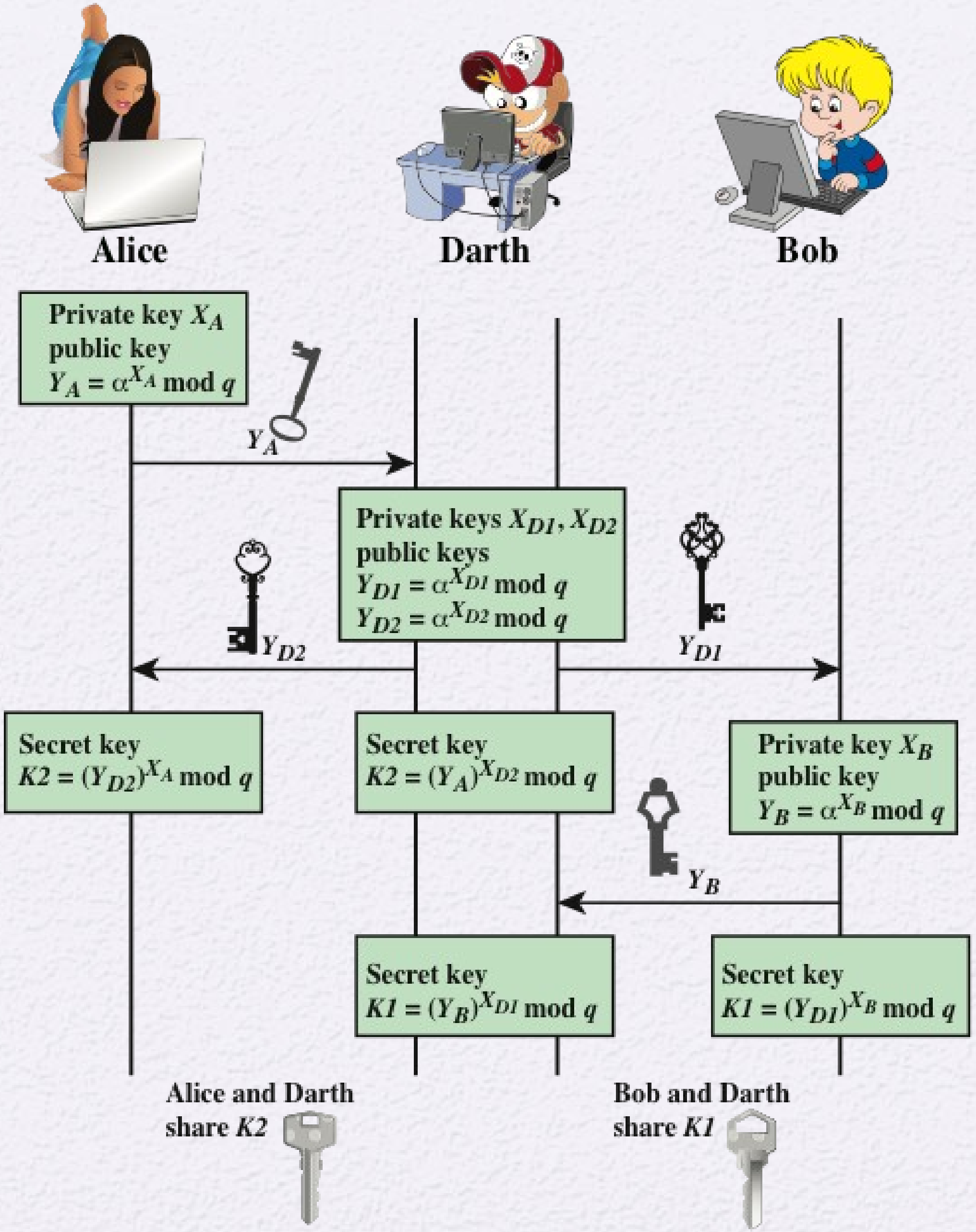


Figure 10.2 Man-in-the-Middle Attack

ElGamal Cryptography

Announced in 1984 by T. Elgamal

Public-key scheme based on discrete logarithms closely related to the Diffie-Hellman technique

Used in the digital signature standard (DSS) and the S/MIME e-mail standard

Global elements are a prime number *q* and *a* which is a primitive root of *q*

Security is based on the difficulty of computing discrete logarithms

Global Public Elements	
q	prime number
α	$\alpha < q$ and α a primitive root of q

Random Number

Key Generation by Alice	
Select private X_A	$\boxed{X_A} < q - 1$
Calculate Y_A	$Y_A = \alpha^{X_A} \bmod q$
Public key	$\{q, \alpha, Y_A\}$
Private key	X_A

Encryption by Bob with Alice's Public Key	
Plaintext:	$M < q$
Select random integer k	$k < q$
Calculate K	$K = (Y_A)^k \bmod q$
Calculate C_1	$C_1 = \alpha^k \bmod q$
Calculate C_2	$C_2 = KM \bmod q$
Ciphertext:	(C_1, C_2)

Decryption by Alice with Alice's Private Key	
Ciphertext:	(C_1, C_2)
Calculate K	$K = (C_1)^{X_A} \bmod q$
Plaintext:	$M = (C_2K^{-1}) \bmod q$

Figure 10.3 The ElGamal Cryptosystem

Let

Alice

Bob sends a message to Alice
"B" (66 in ASCII)

Alice receives (C_1, C_2)