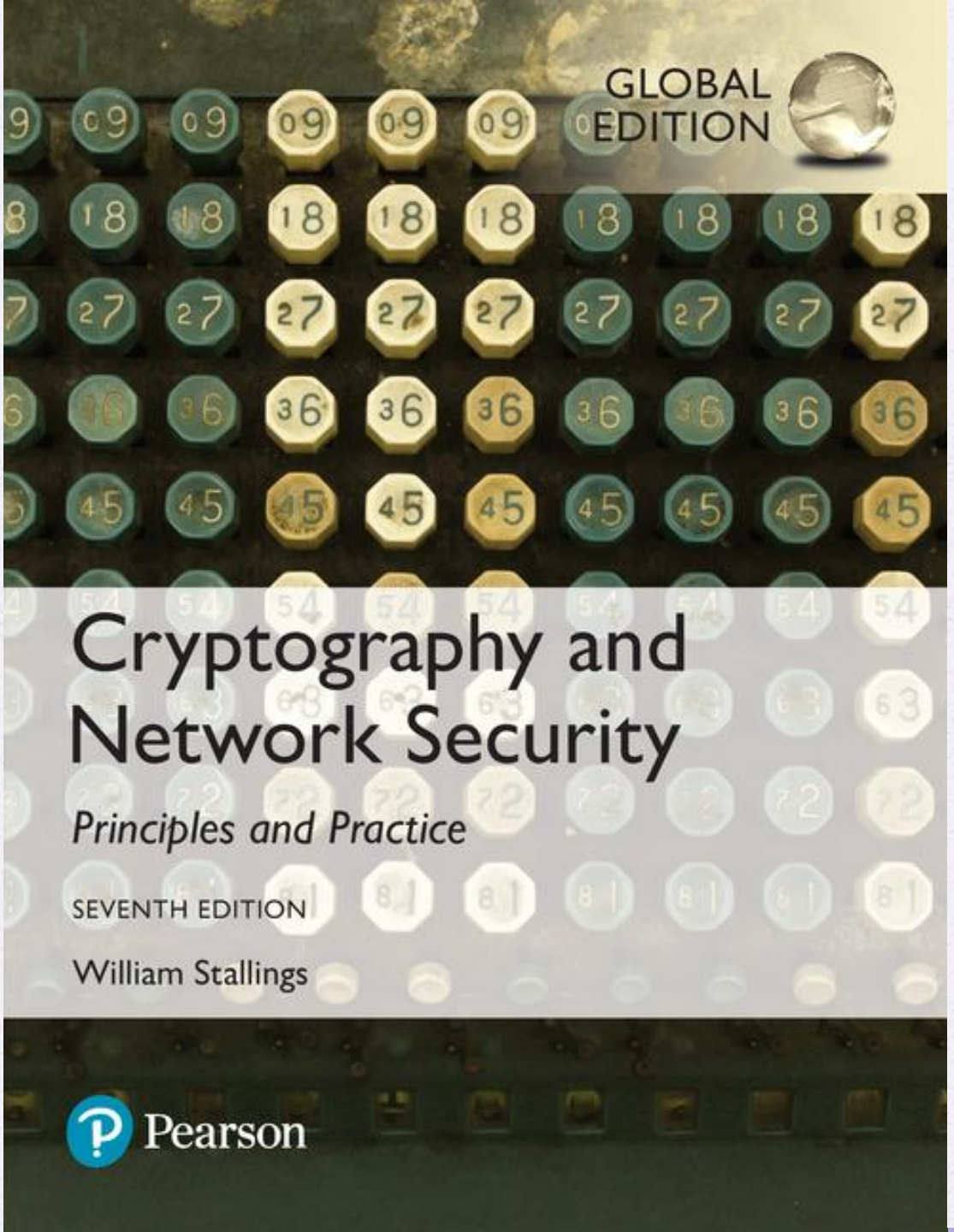
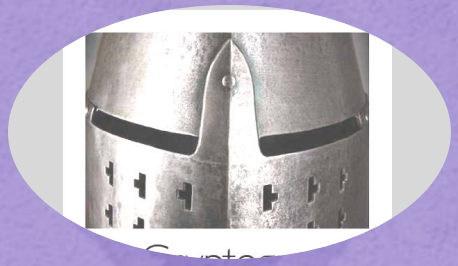

GLOBAL EDITION
Cryptography and Network Security
Principles and Practice
SEVENTH EDITION
William Stallings
Pearson



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

Alice

Bob

Alice	Bob
Alice and Bob share a prime q and α, such that $\alpha < q$ and α is a primitive root of q	Alice and Bob share a prime q and α, such that $\alpha < q$ and α is a primitive root of q
Alice generates a private key X_A such that $X_A < q$	Bob generates a private key X_B such that $X_B < q$
Alice calculates a public key $Y_A = \alpha^{X_A} \bmod q$	Bob calculates a public key $Y_B = \alpha^{X_B} \bmod q$
Alice receives Bob's public key Y_B in plaintext	Bob receives Alice's public key Y_A in plaintext
Alice calculates shared secret key $K = (Y_B)^{X_A} \bmod q$	Bob calculates shared secret key $K = (Y_A)^{X_B} \bmod q$

Figure 10.1 Diffie-Hellman Key Exchange

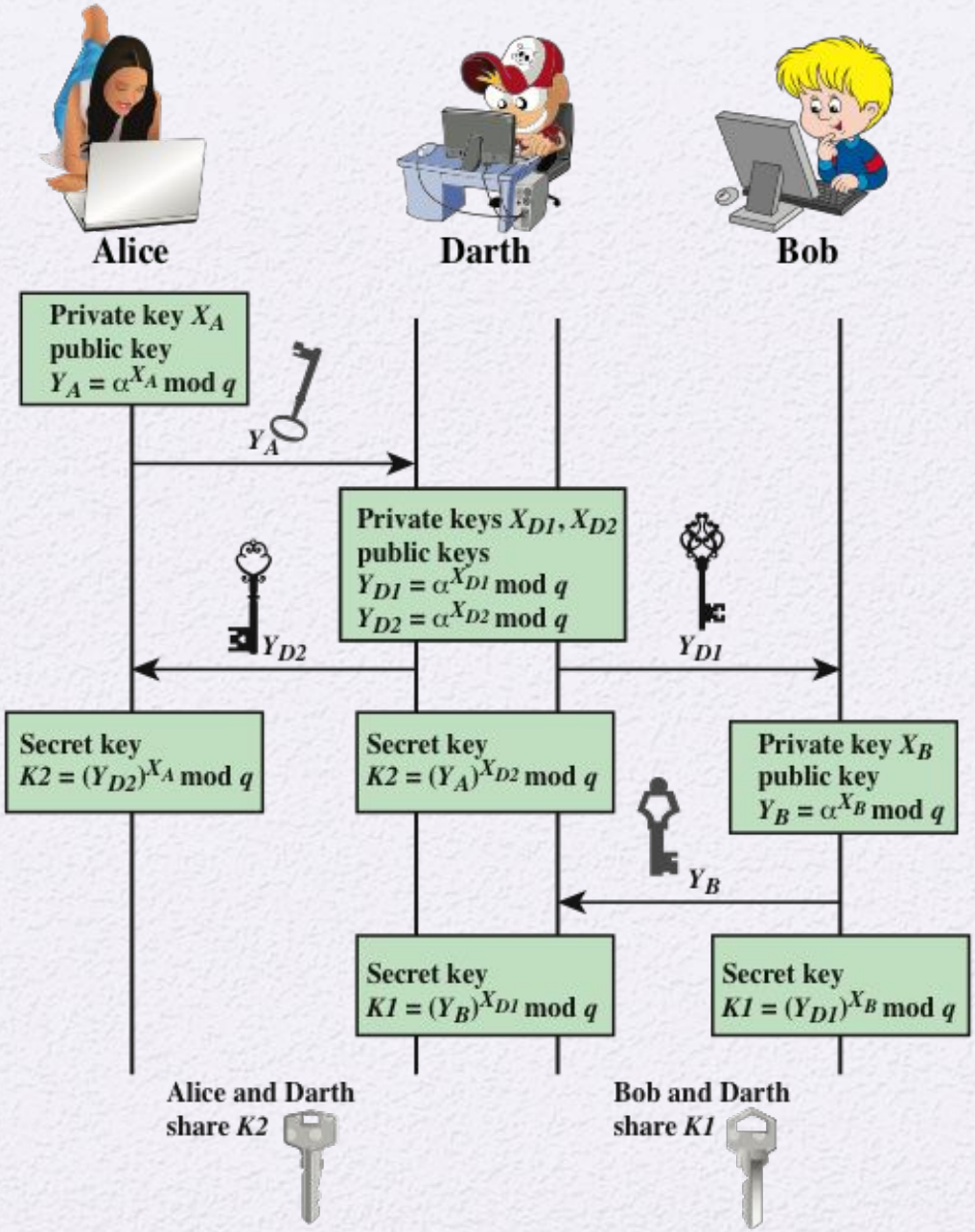


Figure 10.2 Man-in-the-Middle Attack