Cryptography and Network Security

Eighth Edition

by William Stallings

Chapter 10

Other Public-Key Cryptosystems

Diffie-Hellman Key Exchange

- First published public-key algorithm
- **It is a practical method for public <u>exchange of a session secret key</u>; and it is limited to this purpose.**
- It enables two users to securely exchange a key that can then be used for subsequent symmetric encryption of messages
- Its effectiveness depends on the difficulty of computing discrete logarithms.
- It is used in a number of commercial products

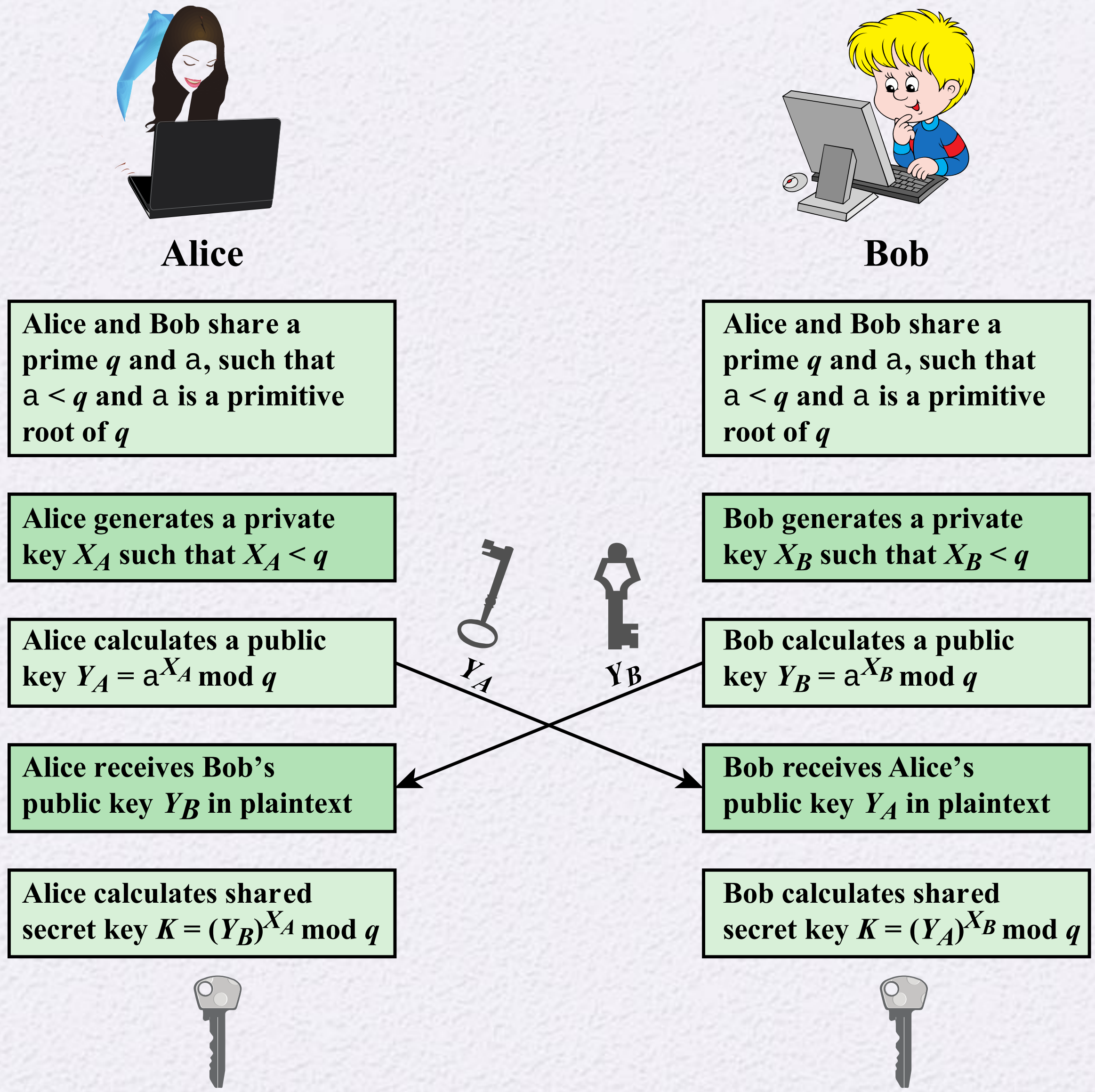

Figure 10.1 Diffie-Hellman Key Exchange

Diffie-Hellman Example

- Suppose Alice and Bob wish to exchange a session secret key:
- They agree on prime q=353 and a=3
- They select random secret keys:
  - Alice chooses x_A=97, Bob chooses x_B=233
- Then, the respective public keys are:
  - $y_A=3^{97} \bmod 353 = 40$ (Alice)
  - $y_B=3^{233} \bmod 353 = 248$ (Bob)
- The shared session key can be computed as:
  - $K_{AB}= y_B^{x_A} \bmod 353 = 248^{97} = 160$ (Alice)
  - $K_{AB}= y_A^{x_B} \bmod 353 = 40^{233} = 160$ (Bob)

Exercise 1

- Two users A and B use the Diffie-Hellman key exchange technique with a common prime **q=17** and a primitive root **a=5.** If A's private key $\mathbf{X_A = 4}$, and B's a private key $\mathbf{X_B=2}$. What is the value of the shared secret key?

Diffie-Hellman Key Exchange protocol is vulnerable to man-in-the-middle attack.

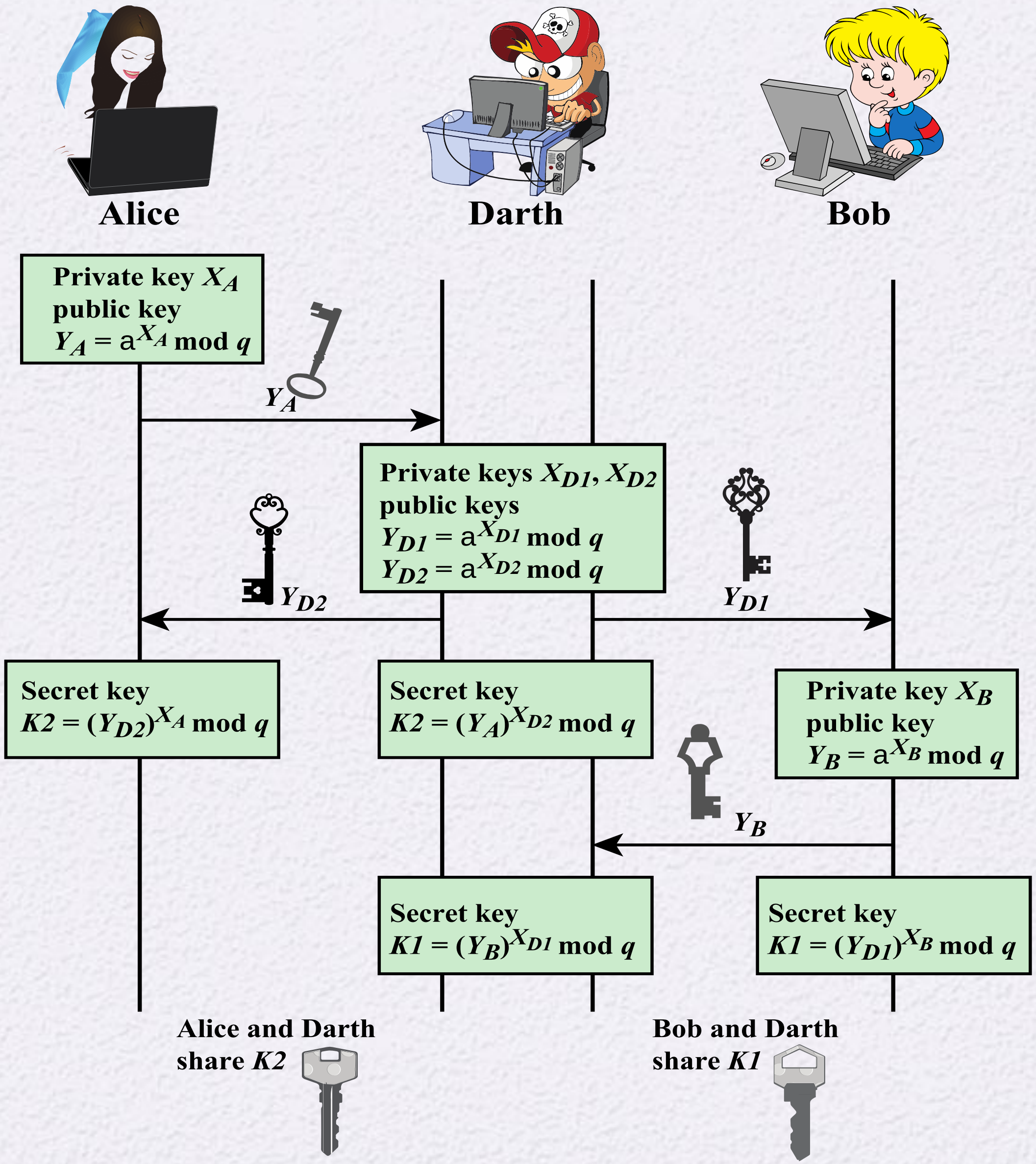

Figure 10.2 Man-in-the-Middle Attack

Diffie-Hellman Man-in-the-Middle Attack

Suppose Alice and Bob wish to exchange keys, and Darth is the adversary. The attack proceeds as follows:

1.Darth prepares for the attack by generating two random private keys X_{D1} and X_{D2} and then computing the corresponding public keys Y_{D1} and Y_{D2}

2. Alice transmits Y_A to Bob.

3. Darth intercepts Y_A and transmits Y_{D1} to Bob. Darth also calculates K2 = (Y_A)^ X_{D2} mod q

4.Bob receives Y_{D1} and calculates K1=(Y_{D1})^ X_B mod q

5.Bob transmits Y_B to Alice.

6.Darth intercepts Y_B and transmits Y_{D2} to Alice. Darth calculates K1=(Y_B)^ X_{D1} mod q

7.Alice receives Y_{D2} and calculates K2=(Y_{D2})^ X_A mod q .

Diffie-Hellman Man-in-the-Middle Attack

At this point, Bob and Alice think that they share a secret key, but instead Bob and Darth share secret key K1 and Alice and Darth share secret key K2. All future communication between Bob and Alice is compromised in the following way:

1. Alice sends an encrypted message M: E($K2$, M).

2. Darth intercepts the encrypted message and decrypts it, to recover M.

3. Darth sends Bob E($K1$, M) or E($K1$, M'), where M' is any message. In the first case, Darth simply wants to eavesdrop on the communication without altering it. In the second case, Darth wants to modify the message going to Bob.

The key exchange protocol is vulnerable to such an attack because it does not authenticate the participants. This vulnerability can be overcome with the use of digital signatures and public-key certificates.

ElGamal Cryptography

- ElGamal Public-key scheme based on discrete logarithms closely related to the Diffie-Hellman technique.
- It is used in the digital signature standard (DSS) and the S/MIME e-mail standard.
- It uses exponentiation in a finite (Galois) with security based difficulty of computing discrete logarithms, as in Diffie-Hellman.
- Global elements are a prime number q and a which is a primitive root of q
- Each user (eg. Alice) generates the keys:
  - Alice chooses a secret key (number): $1 < x_A < q-1$
  - She computes the corresponding public key: $y_A = a^{x_A} \mod q$

ElGamal Cryptography

- If Bob wants to encrypt a message to send it to Alice, he should:
  - represent message M in range 0 <= M <= q-1
    - ✓ longer messages must be sent as blocks
  - chose random integer k with 1 <= k <= q-1
  - compute one-time key $K = y_A^k \bmod q$
  - encrypt M as a pair of integers (C_1,C_2) where
    - $C_1 = a^k \bmod q$; $C_2 = KM \bmod q$
- Alice then recovers message by
  - recovering key K as $K = C_1^{xA} \bmod q$
  - computing M as $M = C_2 K^{-1} \bmod q$
- **a unique k must be used each time**
  - otherwise result is insecure

ElGamal Cryptography

- Using field GF(19) $q=19$ and $a=10$
- Alice computes her key:
  - Alice chooses $x_A=5$ and computes $y_A=10^5 \bmod 19 = 3$
- Bob sends a message $M=17$ as (11,5) by
  - choosing random $k=6$
  - computing $K = y_A^{\ k} \bmod q = 3^6 \bmod 19 = 7$
  - computing $C_1 = a^k \bmod q = 10^6 \bmod 19 = 11$;
  - $C_2 = KM \bmod q = 7.17 \bmod 19 = 5$
- Alice recovers original message by computing:
  - recover $K = C_1^{\ x_A} \bmod q = 11^5 \bmod 19 = 7$
  - compute inverse $K^{-1} = 7^{-1} = 11$
  - recover $M = C_2\ K^{-1} \bmod q = 5.11 \bmod 19 = 17$

Global Public Elements

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

Key Generation by Alice

Select private X_A	$X_A < q - 1$
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:	$M = (C_2 K^{-1}) \bmod q$

Figure 10.3 The ElGamal Cryptosystem

Exercise 2

- Suppose user A who want to send user B an encrypted message M = 8 using ElGamal Message Exchange algorithm with a prime q = 23 and primitive root a=5. If B's public key Y_B=3, and A choses a random integer k=3.
  a) What is the encryption pair (C_1, C_2)?
  b) How does user B recover the message?

Summary

- Define Diffie-Hellman Key Exchange
- Understand the Man-in-the-middle attack

- Present an overview of the Elgamal cryptographic system