GLOBAL EDITION

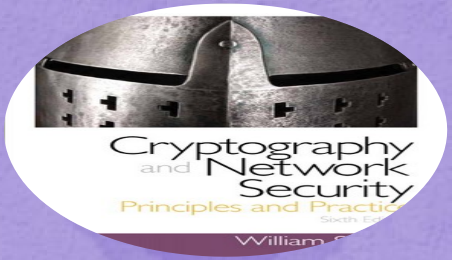
Cryptography and Network Security

Principles and Practice

SEVENTH EDITION

William Stallings

Pearson



Chapter 10

Other Public-Key Cryptosystems

Diffie-Hellman Key Exchange

↳ use to exchange the Keys

- 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

→ reach yk

$q = 7$

$\alpha = 3$

$\rightarrow \alpha^k \bmod q$

$\rightarrow 3^0 \bmod 7 = 1$

$\rightarrow 3^1 \bmod 7 = 3$

$\rightarrow 3^2 \bmod 7 = 2$

$\rightarrow 3^3 \bmod 7 = 6$

$3^4 \bmod 7 = 4$

$3^6 \bmod 7 = 1$

$3^7 \bmod 7 = 3$

α repeat the cycle.

Proof

both the side have same Secret Key.

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 $K = (Y_A)^{X_B} \bmod q$

Y_A $\quad$ Y_B

$k = Y_B^{X_A} \bmod q$

$k = (\alpha^{X_B})^{X_A} \bmod q$

$\rightarrow K = (\alpha^{X_B})^{X_A} \bmod q$

Putting value of X_B

$$\boxed{\begin{aligned} k &= Y_A^{X_B} \bmod q \\ k &= (\alpha^{X_A})^{X_B} \bmod q \end{aligned}}$$

Figure 10.1 Diffie-Hellman Key Exchange

Let $\alpha = 5$, $q = 23$

ALICE

$X_A = 4$ → Private key of Alice

$Y_A = \alpha^{X_A} \bmod q$

$Y_A = 5^4 \bmod 23$

$\boxed{Y_A = 4}$ → Public key of Alice

$\boxed{Y_A = 4}$

find Secret key

$K = (Y_B)^{X_A} \bmod q$

$K = 10^4 \bmod 23$

$\boxed{K = 18}$

BOB

$X_B = 3$
↳ Private key of Bob

$Y_B = \alpha^{X_B} \bmod q$

$Y_B = 5^3 \bmod q/23$

$Y_B = 125 \bmod 23$

$\boxed{Y_B = 10}$

finding Secret key

$K = Y_A^{X_B} \bmod q$

$K = 4^3 \bmod 23$

$\boxed{K = 18}$

Both Are Equal

Symmetric key

Proof

Alice:

$k_2 = (Y_{D2})^{X_A} \bmod q$

$k_2 = (\alpha^{X_{D2}})^{X_A} \bmod q$

Darth:

$k_2 = (Y_A)^{X_{D2}} \bmod q$

Putting value:

$k_2 = (\alpha^{X_A})^{X_{D2}} \bmod q$

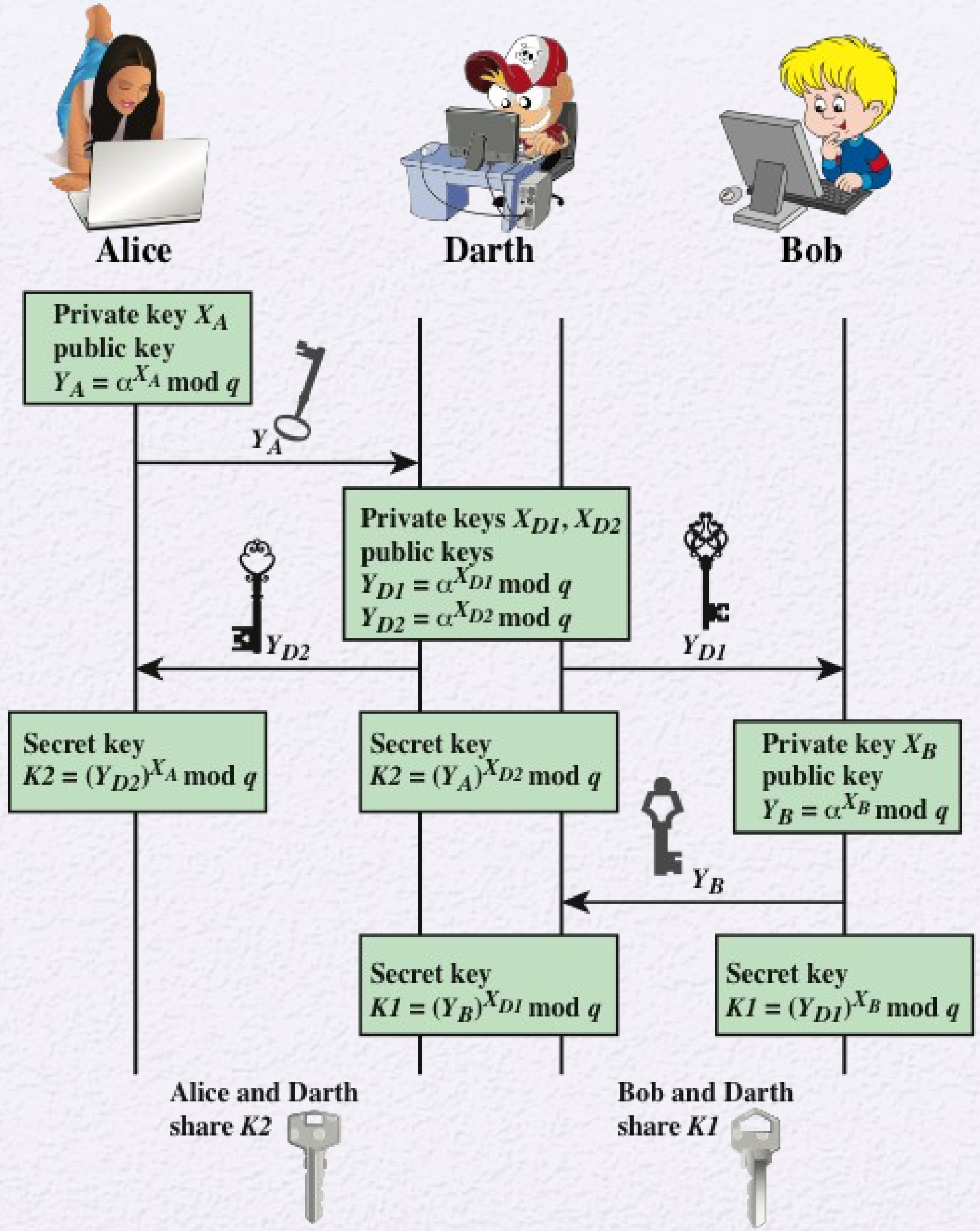


Figure 10.2 Man-in-the-Middle Attack

Bob

$\to k_1 = (Y_{D1})^{X_B} \bmod q$

$k_1 = (\alpha^{X_{D1}})^{X_B} \bmod q$

Darth

$k_1 = (Y_B)^{X_{D1}} \bmod q$

$k_1 = (\alpha^{X_B})^{X_{D1}} \bmod q$

Both are equal

(Key + Msg)
↳ Both In this Algo.

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	$\{q, \alpha, Y_A\}$ → Public portion:
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)

Encryption:

$K = (Y_A)^k \bmod q$

$C_1 = \alpha^k \bmod q$

$C_2 = KM \bmod q$

→ contain k value;

→ contain Msg:

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

Let $q=107$ $\alpha=2$

$X_A < q-1$

$X_A = 67$ #private key Alice

$Y_A = \alpha^{X_A} \bmod q = 2^{67} \bmod 107$

$Y_A = 94$ #public key

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

$M=66$ #Msg

$k=45$ (small k) (RanInte) $k<q$

$K=94^{45} \bmod 107$

$K=5$

$C_1 = \alpha^{k} \bmod q$

$C_1 = 2^{45} \bmod 107$

$C_1 = 28$

$C_2 = K \times M \bmod q$

$C_2 = 5 \times 66 \bmod 107$

$C_2 = 9$

Cipher Text: $(C_1, C_2) = (28, 9)$

Alice receives (C_1, C_2)

Cipher Text: $(C_1, C_2) = (28, 9)$

$K = C_1^{X_A} \bmod q = 28^{67} \bmod 107$

$K=5$

$M = C_2 \times K^{-1} \bmod q$

$M = 9 \times 43 \bmod 107$

$M = 66$

$k \cdot k^{-1} \bmod q = 1$

$5 \cdot ? \bmod q = 1$

$5 \cdot ? \bmod 107 = 1$

? → Select $>q$

>107

$5 \times 43 \bmod 107 = 1$

107×2

214