[Part 3] Integrity, Authenticity, and Key Management

Chapter 15

Key Management

Forouzan, B.A. Cryptography and Network Security (International Edition). United States: McGraw Hill, 2008.

Chapter 15 Objectives

- To explain the need for a *Key-Distribution Center* (KDC).
- To show how a KDC can create a session key between two parties.
- To show how two parties can use a symmetric-key agreement protocol to create a session between themselves without using the services of a KDC.

15.2

Chapter 15 Contents

15.3

Chapter 15 15.1 Introduction

- In previous chapters, we have discussed symmetric-key and asymmetric-key cryptography.
- However, we have not discussed yet on how *secret key* in symmetric-key cryptography, and *public key* in asymmetric-key cryptography are distributed and maintained.

15.4

Chapter 15

15.1 Introduction

- This chapter will touches the *secret key* in symmetric-key cryptography only.
- The discussion will be on:
  - the distribution of symmetric keys using a trusted third party.
  - How two parties can establish a symmetric key between themselves without using a trusted third party.

15.5

Chapter 15

15.1 Introduction

Key Management

- Key management is the way how we manage the cryptographic keys in a cryptosystem.
- This may includes the dealing with the key generation, key exchange, key storage, key use, and key replacement.
- Successful key management is critical to the security of a cryptosystem.

https://en.wikipedia.org/wiki/Key_management

15.6

Chapter 15 Contents

15.7

Chapter 15 15.2 Symmetric-Key Distribution

- Symmetric-key cryptography is more efficient than asymmetric-key cryptography for encrypting large messages.
- Symmetric-key cryptography, however, needs a shared secret key between two parties.
  - For n people, we need: $n(n-1)/2$ shared secrets.
- **Problems**:
  - The number of keys;
  - The distribution of keys is another problem.
- **Solution**: Use a trusted third party.

15.8

Chapter 15

15.2 Symmetric-Key Distribution

Key-Distribution Center (KDC)

- KDC is a practical solution that use a trusted third party.
- To reduce the number of keys, each person establishes a shared secret key with the KDC.

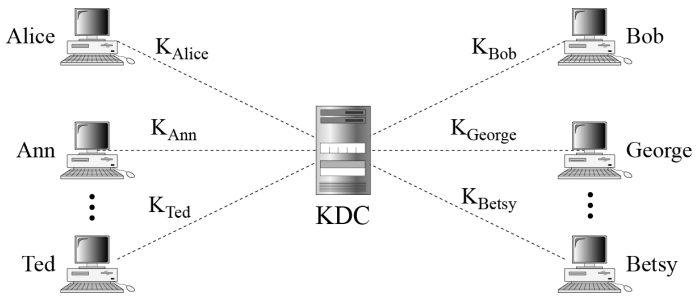


Figure 15.1: Key-distribution center (KDC)

15.9

Chapter 15

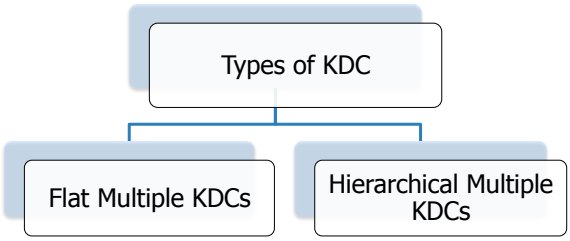
15.2 Symmetric-Key Distribution

- (Figure 15.1)
- A secret key is established between the KDC and each members.
- Alice can sends a confidential message to Bob with the following process:
  - ① Alice sends a request to the KDC stating that she needs a session (temporary) secret key with Bob.
  - ② The KDC informs Bob about Alice's request.
  - ③ If Bob agrees, a session key is created between them.

15.10

Chapter 15 15.2 Symmetric-Key Distribution

- When the number of people using a KDC increases, the system becomes unmanageable and a bottleneck can result.
- **Solution**: Multiple KDCs.



15.11

Chapter 15 15.2 Symmetric-Key Distribution

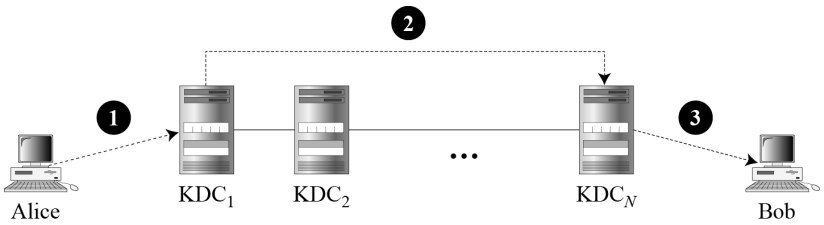


Figure 15.2: Flat multiple KDCs

15.12

Chapter 15 15.2 Symmetric-Key Distribution

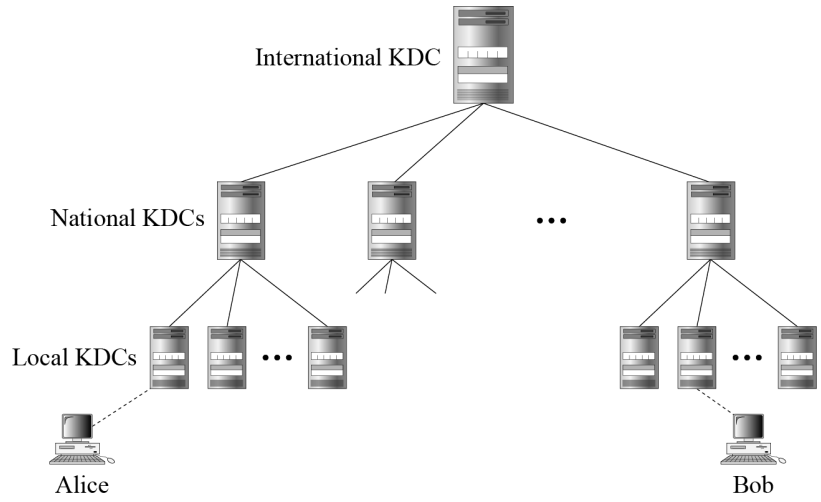


Figure 15.3: Hierarchical multiple KDCs

15.13

Chapter 15 15.2 Symmetric-Key Distribution

Session Keys:

- A KDC creates a secret key for each member.
- This secret key can be used only between the member and the KDC, not between two members.

Note

A session symmetric key between two parties is used only once.

15.14

Chapter 15 Contents

15.15

Chapter 15 15.3 Symmetric-Key Agreement

- Sender and receiver can create a session key between themselves without using a KDC.
- This method of session-key creation is referred to as the *symmetric-key agreement*.
- There are several ways to accomplish this.
- Two common methods are *Diffie-Hellman* and station-to-station.
- However, we shall discuss the *Diffie-Hellman* only.

15.16

Chapter 15

15.3 Symmetric-Key Agreement

Diffie-Hellman (DH)

- In DH protocol, two parties create a symmetric session key without the need of a KDC.
- Before establishing a symmetric-key, the two parties need to choose two numbers :

p	A large prime number on the order of 300 decimal digits (1024 bits)
g	A generator of order $p - 1$ in the group $< Z_{p^*}, \times >$

  - These p and g do not need to be confidential.
  - They can be sent through the Internet; can be public.

15.17

Chapter 15

15.3 Symmetric-Key Agreement

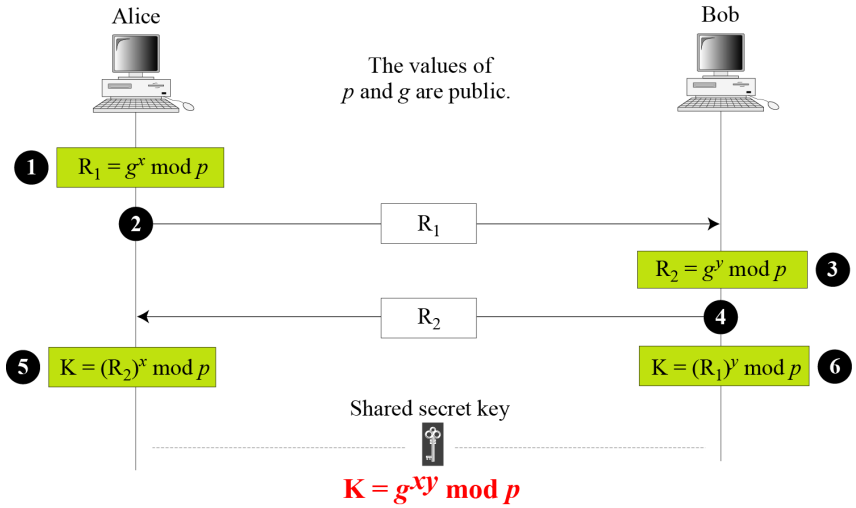


Figure 15.4: Diffie-Hellman method

15.18

Chapter 15 15.3 Symmetric-Key Agreement

- **Figure 15.4** shows the procedure.
- The steps are as follows:

① Alice chooses a large random number x such that $0 \le x \le (p-1)$ and calculates $R_1 = g^x \bmod p$.

② Bob chooses another large random number y such that $0 \le y \le (p-1)$ and calculates $R_2 = g^y \bmod p$.

③ Alice sends R_1 to Bob (but not sends the value of x).

④ Bob sends R_2 to Alice (but not sends the value of y).

⑤ Alice calculate $K = (R_2)^x \bmod p$.

⑥ Bob calculate $K = (R_1)^y \bmod p$.

K is the symmetric key for the session.

Chapter 15 15.3 Symmetric-Key Agreement

- Bob has calculated K as:

$$R_1 = g^x \bmod p$$

$$K = (R_1)^y \bmod p = (g^x \bmod p)^y \bmod p = g^{xy} \bmod p$$

- Alice has calculated K as:

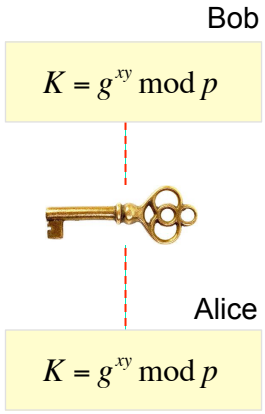
$$R_2 = g^y \bmod p$$

$$K = (R_2)^x \bmod p = (g^y \bmod p)^x \bmod p = g^{xy} \bmod p$$

15.20

Chapter 15 — 15.3 Symmetric-Key Agreement

- Both have reached the same value without Bob knowing the value of x and without Alice knowing the value of y.



15.21

Chapter 15 — 15.3 Symmetric-Key Agreement

Example 15.1: Let us give a trivial example to make the procedure clear.

Our example uses small numbers, but note that in a real situation, the numbers are very large.
Assume that $g = 7$ and $p = 23$.

The steps are as follows:

① Alice chooses $x = 3$ and calculates $R_1 = 7^3 \bmod 23 = 21$.
② Bob chooses $y = 6$ and calculates $R_2 = 7^6 \bmod 23 = 4$.
③ Alice sends the number 21 to Bob.
④ Bob sends the number 4 to Alice.
⑤ Alice calculates the symmetric key $K = 4^3 \bmod 23 = 18$.
⑥ Bob calculates the symmetric key $K = 21^6 \bmod 23 = 18$.

The value of K is the same for both Alice and Bob;
$g^{xy} \bmod p = 7^{18} \bmod 35 = 18$.

Chapter 15 15.3 Symmetric-Key Agreement

Exercise 15.1: Given $p = 97$ and $g = 5$. Assume that Alice and Bob choose the private key as $x = 36$ and $y = 58$ respectively.

a) Calculate Alice public key, R_A.
b) Calculate Bob public key, R_B.
c) Calculate the symmetric key K_A value for Alice.
d) Calculate the symmetric key K_B value for Bob.
e) Do they reach the same value of symmetric key?

Chapter 15 15.3 Symmetric-Key Agreement

Exercise 15.2: Alice and Bob who wish to swap keys agree on $p = 353$ and $g = 3$. Assume that Alice and Bob choose the private key as $x = 97$ and $y = 233$ respectively.

a) Calculate Alice public key, R_A.
b) Calculate Bob public key, R_B.
c) Calculate the symmetric key K_A value for Alice.
d) Calculate the symmetric key K_B value for Bob.

Chapter 15 15.3 Symmetric-Key Agreement

Exercise 15.3: Choose a partner in the class. Assume the prime $p = 97$ and $g = 5$.

- Each person select a random secret key that must less than p.
- Computer your public key.
- Tell your public key to your partner.

- Compute your shared session key.
- Check with your partner whether the keys are the same.

Assoc. Prof. Mazleena Salleh, Cryptography and Network Security, 2014/2015-Semester 2.
https://kellysisco.files.wordpress.com/2014/06/two-people-speech-bubbles1.jpg

15.25

Chapter 15 15.3 Symmetric-Key Agreement

Example 15.2: Let us give a more realistic example.

We used a program to create a random integer of 512 bits (the ideal is 1024 bits).

The integer p is a 159-digit number.

We also choose g, x, and y as shown below:

p	764624298563493572182493765955030507476338096726949748923573772860925235666660755423637423309661180033338106194730130950414738700999178043654785807987581
g	2
x	557
y	273

Chapter 15 — 15.3 Symmetric-Key Agreement

(Continued)

The following shows the values of R_1, R_2, and K.

$\mathbf{R_1}$	844920284205665505216172947491035094143433698520012660862863631067673619959280828586700802131859290945140217500319973312945836083821943065966020157955354
$\mathbf{R_2}$	435262838709200379470747114895581627636389116262115557975123379218566310011435718208390040181876486841753831165342691630263421106721508589625520128859414 3
$\mathbf{K}$	155638000664522290596225827523270765273218046944423678520320400146406500887936651204257426776608327911017153038674561252213151610976584200120408643361774 0

Chapter 15 — 15.3 Symmetric-Key Agreement

Analysis of *Diffie-Hellman*:

- The DH concept is simple but elegant.
- The secret key between Alice and Bob is made of three parts: g, x, and y.
- However, $1/3$ of the key is public: g.
- The other $2/3$ of the key must be added by Alice and Bob.

Note

Although the key in Alice's hand (g, y, and x) and the key in Bob's hand (g, x, and y), these two keys are the same because $g^{xy} = g^{yx}$

Although the two keys are the same, Alice cannot find the value of y used by Bob because the calculation is done in modulo p.

Chapter 15 — 15.3 Symmetric-Key Agreement

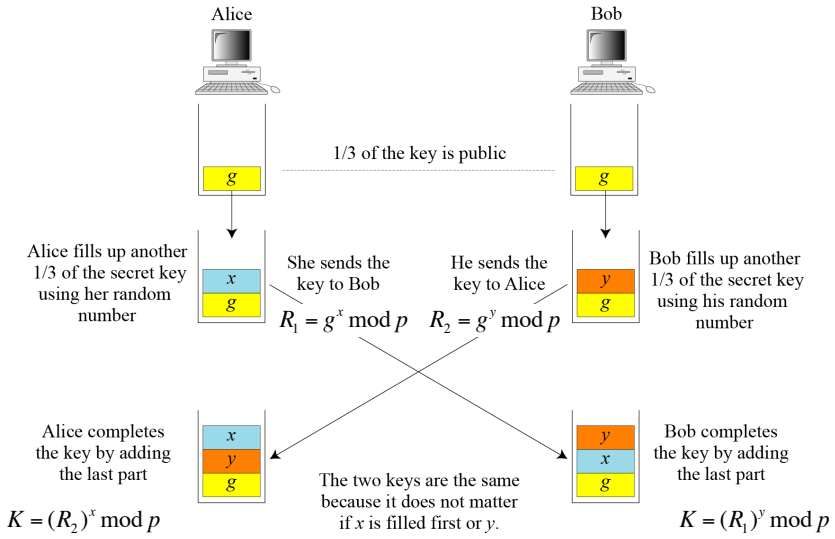


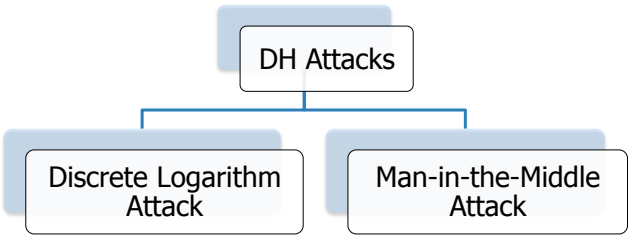
Figure 15.5: Diffie-Hellman idea

15.29

Chapter 15 — 15.3 Symmetric-Key Agreement

Security of *Diffie-Hellman*:

- The DH key exchange is susceptible to two attacks:



- Eve can intercept R_1 and R_2.
- If the x and y found from R_1 and R_2, the symmetric key K can be calculated.
- Eve does not have to find the value of x and y.
- Eve can fool Alice and Bob by creating two keys; one between herself and Alice, one between herself and Bob. (Figure 15.6)

Chapter 15

15.3 Symmetric-Key Agreement

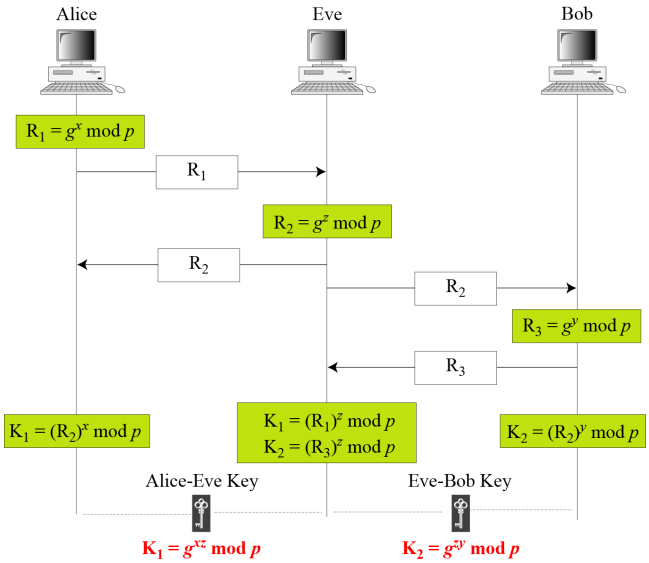


Figure 15.6: Man-in-the-middle attack

15.31

Chapter 15

Contents

15.32

Chapter 15

15.4 Summary

- Symmetric-key cryptography needs a shared secret key between two parties.
  - *N* people need *N(N – 1)/2* keys.
  - The problem are the number of keys and the distribution of the keys.
- A practical solution is the use of a trusted third party, referred to as a *Key-Distribution Center* (KDC).
  - Create a session key temporarily between Alice and Bob.
  - Their keys are used to authenticate themselves to the center.

15.33

Chapter 15

15.4 Summary

- Alice and Bob can create a session key between themselves without using KDC referred to as the *Symmetric-Key Agreement.*
  - One method discussed: *Diffie-Hellman (DH)*.
  - However, DH is susceptible to the man-in-the-middle attack.

15.34

Chapter 15 Exercises

Exercise 15.4:

a) What is the main duties of a KDC?

b) Define a session key and show how a KDC can create a session key between Alice and Bob.

c) Define the *Diffie-Hellman* protocol and its purpose.

d) Define man-in-the-middle attack.

Forouzan,B.A. Cryptography and Network Security (International Edition). Singapore: McGraw-Hill, 2008. (page 463) 15.35

Chapter 15 Exercises

Exercise 15.5: In the *Diffie-Hellman* protocol, $g = 7$, $p = 23$, $x = 3$, and $y = 5$.

a) What is the value of R_1 and R_2?

b) What is the value of the symmetric key?

Forouzan,B.A. Cryptography and Network Security (International Edition). Singapore: McGraw-Hill, 2008. (page 463)

Chapter 15 Exercises

Exercise 15.6: In the *Diffie-Hellman* protocol, what happen if x and y have the same value, that is, Alice and Bob have accidently chosen the same number? Are the R_1 and R_2 the same? Do the session keys calculated by Alice and Bob have the same value?

Use an example to prove your claims.

Forouzan,B.A. Cryptography and Network Security (International Edition). Singapore: McGraw-Hill, 2008. (page 464)