DISTRIBUTED SYSTEMS
Principles and Paradigms
Second Edition
ANDREW S. TANENBAUM
MAARTEN VAN STEEN

Chapter 9
Security

1

Security Threats, Policies, and Mechanisms

Types of security threats to consider:

- Interception
- Interruption
- Modification
- Fabrication

2

Example: The Globus Security Architecture (1)

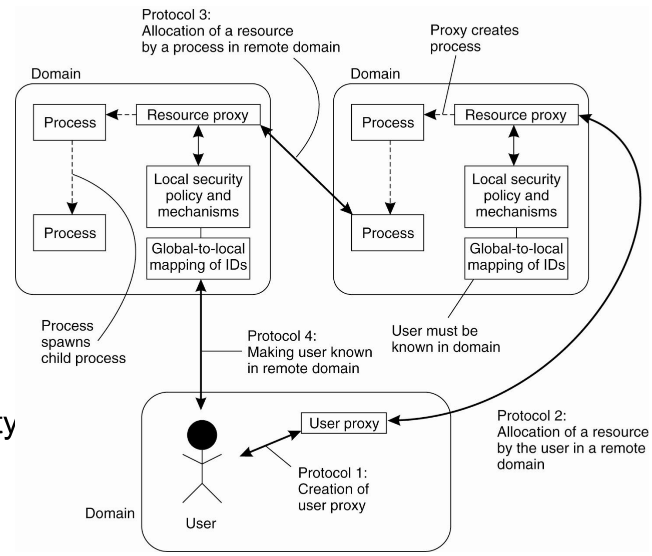

Figure 9-1. The Globus security architecture.

3

Example: The Globus Security Architecture (2)

1. The environment consists of multiple administrative domains.
2. Local operations are subject to a local domain security policy only.
3. Global operations require the initiator to be known in each domain where the operation is carried out.

4

Example: The Globus Security Architecture (3)

4. Operations between entities in different domains require mutual authentication.
5. Global authentication replaces local authentication.
6. Controlling access to resources is subject to local security only.
7. Users can delegate rights to processes.
8. A group of processes in the same domain can share credentials.

5

Focus of Control (1)

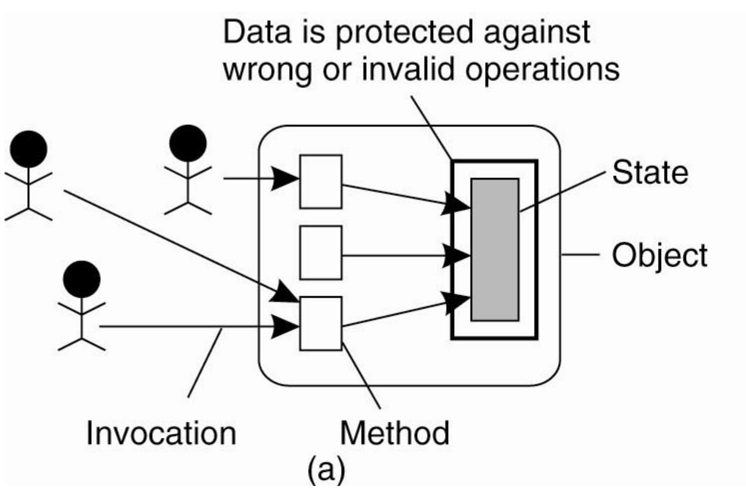

Figure 9-2. Three approaches for protection against security threats. (a) Protection against invalid operations

6

Focus of Control (2)

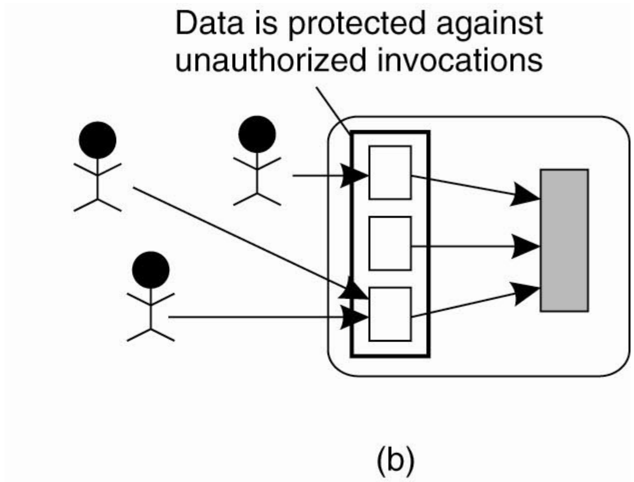

Figure 9-2. Three approaches for protection against security threats. (b) Protection against unauthorized invocations.

7

Focus of Control (3)

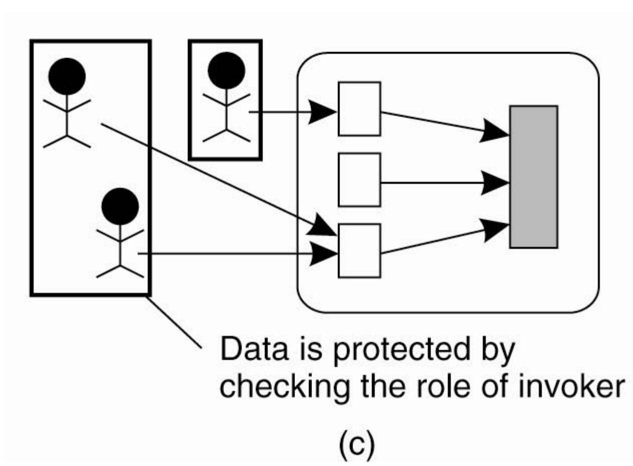

Figure 9-2. Three approaches for protection against security threats. (c) Protection against unauthorized users.

8

Layering of Security Mechanisms (1)

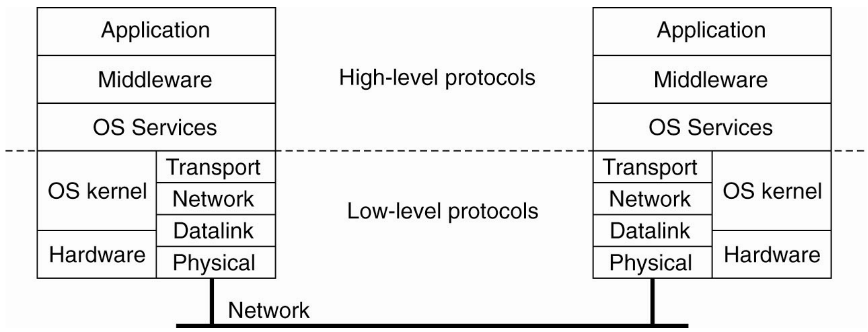

Figure 9-3. The logical organization of a distributed system into several layers.

9

Layering of Security Mechanisms (2)

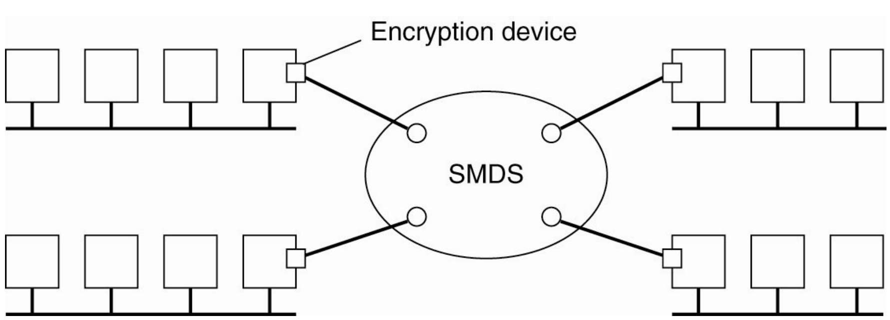

Figure 9-4. Several sites connected through a wide-area backbone service.

10

Distribution of Security Mechanisms

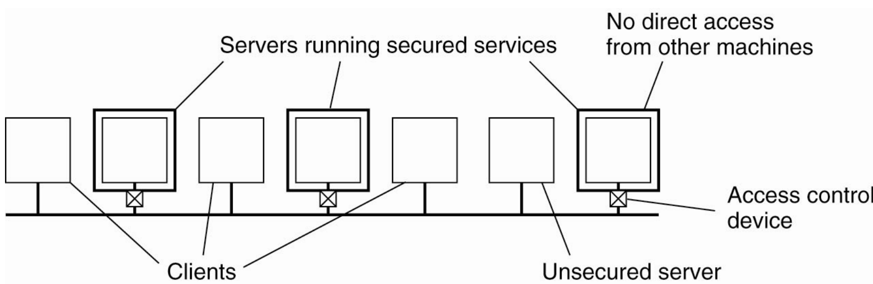

Figure 9-5. The principle of RISSC as applied to secure distributed systems.

11

Cryptography (1)

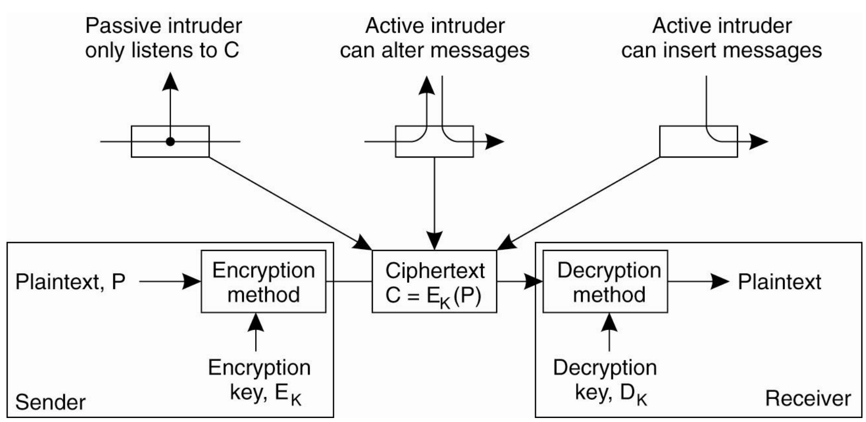

Figure 9-6. Intruders and eavesdroppers in communication.

12

Cryptography (2)

Notation	Description
$K_{A,B}$	Secret key shared by A and B
K_A^+	Public key of A
K_A^-	Private key of A

Figure 9-7. Notation used in this chapter.

13

Symmetric Cryptosystems: DES (1)

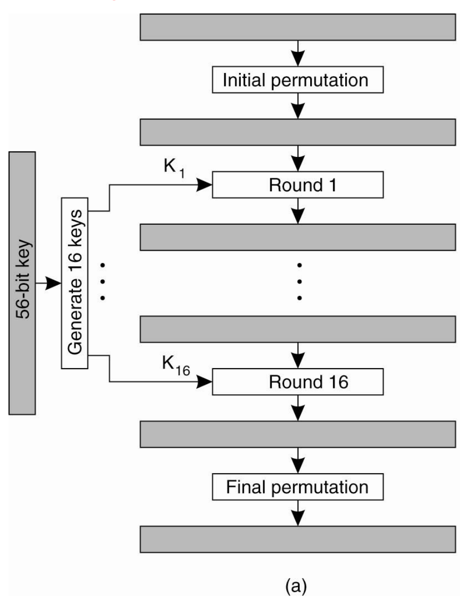

Figure 9-8. (a) The principle of DES.

14

Symmetric Cryptosystems: DES (2)

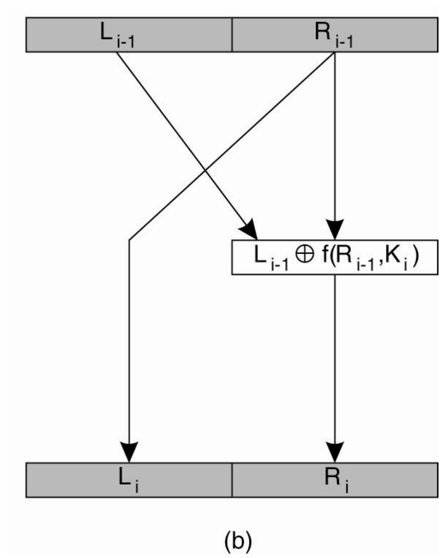

Figure 9-8. (b) Outline of one encryption round.

15

Symmetric Cryptosystems: DES (3)

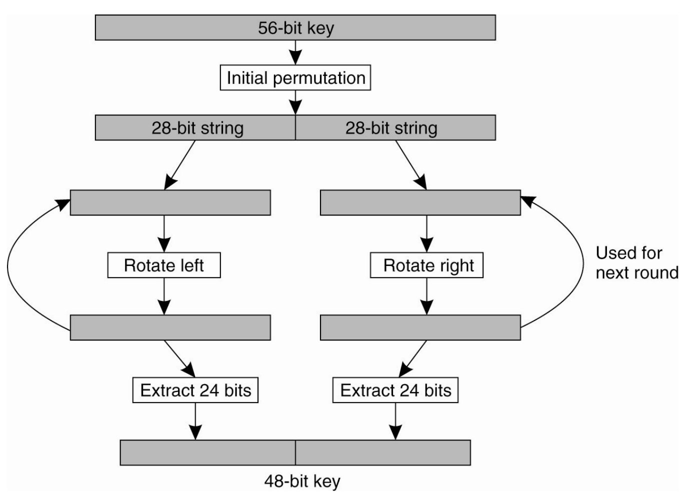

Figure 9-9. Details of per-round key generation in DES.

16

Public-Key Cryptosystems: RSA

Generating the private and public keys requires four steps:

- Choose two very large prime numbers, p and q.
- Compute $n = p \times q$ and $z = (p - 1) \times (q - 1)$.
- Choose a number d that is relatively prime to z.
- Compute the number e such that $e \times d = 1 \bmod z$.

17

Hash Functions: MD5 (1)

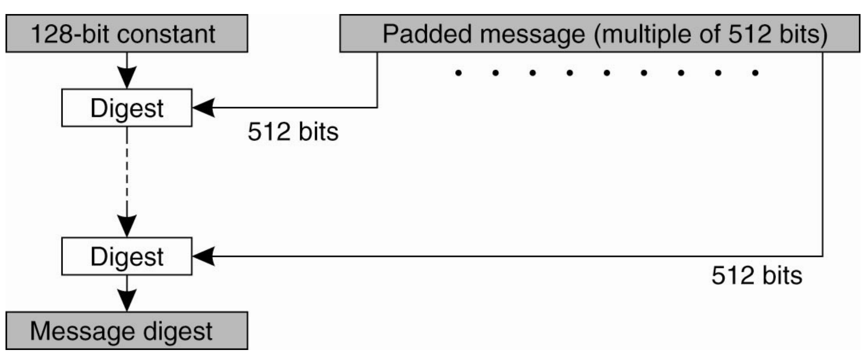

Figure 9-10. The structure of MD5.

18

Hash Functions: MD5 (2)

Iterations 1–8	Iterations 9–16
$p \leftarrow (p + F(q,r,s) + b_0 + C_1) \lll 7$	$p \leftarrow (p + F(q,r,s) + b_8 + C_9) \lll 7$
$s \leftarrow (s + F(p,q,r) + b_1 + C_2) \lll 12$	$s \leftarrow (s + F(p,q,r) + b_9 + C_{10}) \lll 12$
$r \leftarrow (r + F(s,p,q) + b_2 + C_3) \lll 17$	$r \leftarrow (r + F(s,p,q) + b_{10} + C_{11}) \lll 17$
$q \leftarrow (q + F(r,s,p) + b_3 + C_4) \lll 22$	$q \leftarrow (q + F(r,s,p) + b_{11} + C_{12}) \lll 22$
$p \leftarrow (p + F(q,r,s) + b_4 + C_5) \lll 7$	$p \leftarrow (p + F(q,r,s) + b_{12} + C_{13}) \lll 7$
$s \leftarrow (s + F(p,q,r) + b_5 + C_6) \lll 12$	$s \leftarrow (s + F(p,q,r) + b_{13} + C_{14}) \lll 12$
$r \leftarrow (r + F(s,p,q) + b_6 + C_7) \lll 17$	$r \leftarrow (r + F(s,p,q) + b_{14} + C_{15}) \lll 17$
$q \leftarrow (q + F(r,s,p) + b_7 + C_8) \lll 22$	$q \leftarrow (q + F(r,s,p) + b_{15} + C_{16}) \lll 22$

Figure 9-11. The 16 iterations during the first round in a phase in MD5.

19

Digital Signatures (1)

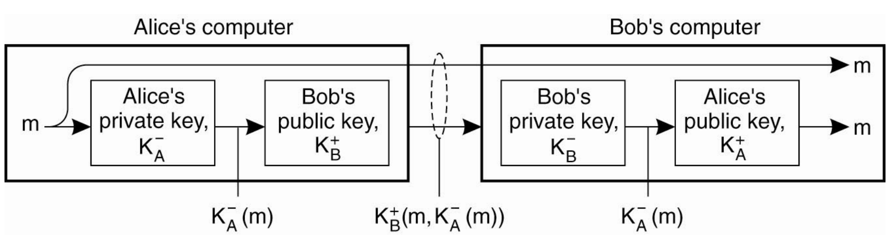

Figure 9-20. Digital signing a message using public-key cryptography.

20

Digital Signatures (2)

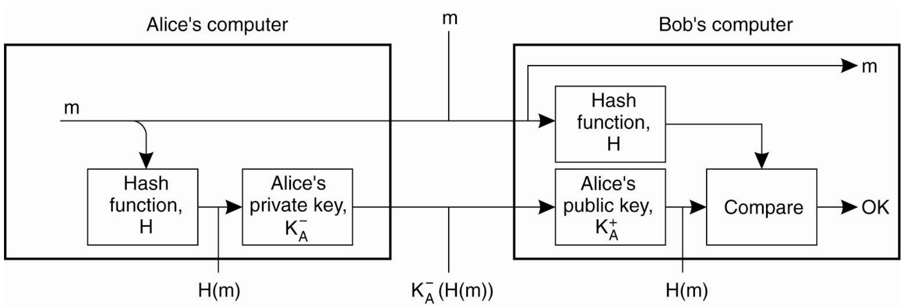

Figure 9-21. Digitally signing a message using a message digest.

21

Key Establishment

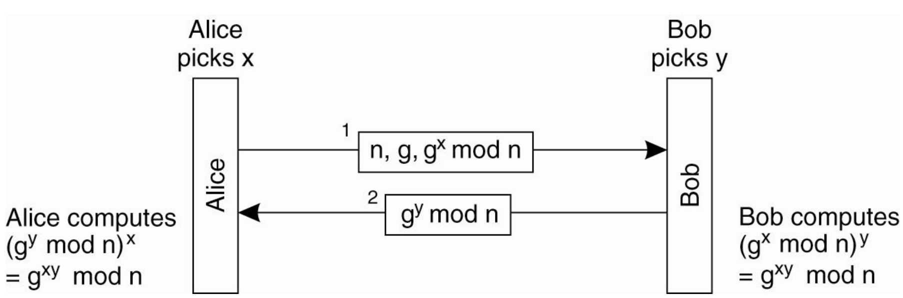

Figure 9-33. The principle of Diffie-Hellman key exchange.

22

Key Distribution (1)

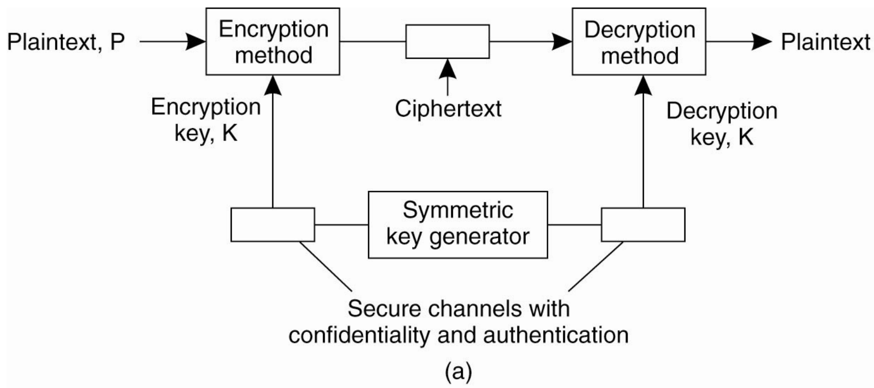

Figure 9-34. (a) Secret-key distribution. [see also Menezes et al. (1996)].

23

Key Distribution (2)

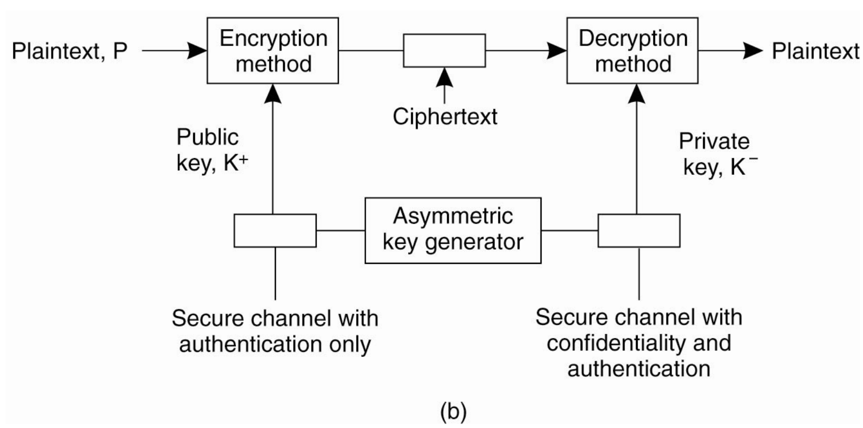

Figure 9-34. (b) Public-key distribution [see also Menezes et al. (1996)].

24

Authentication Based on a Shared Secret Key (1)

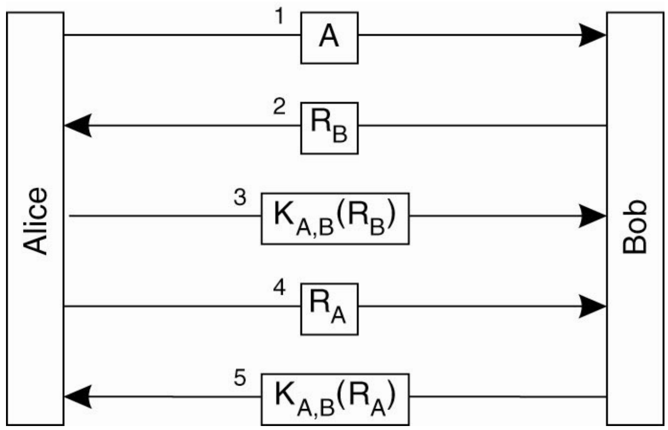

Figure 9-12. Authentication based on a shared secret key.

25

Authentication Based on a Shared Secret Key (2)

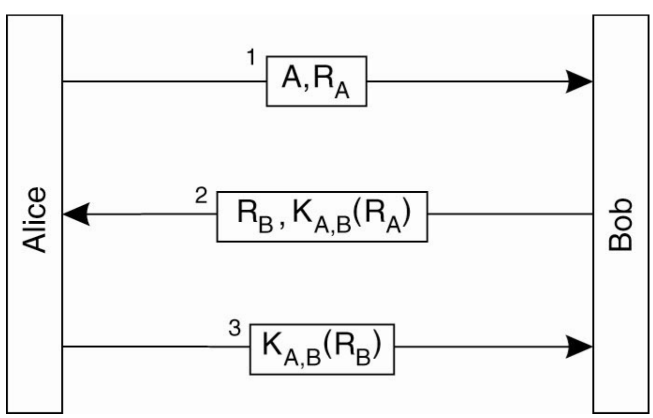

Figure 9-13. Authentication based on a shared secret key, but using three instead of five messages.

26

Authentication Based on a Shared Secret Key (3)

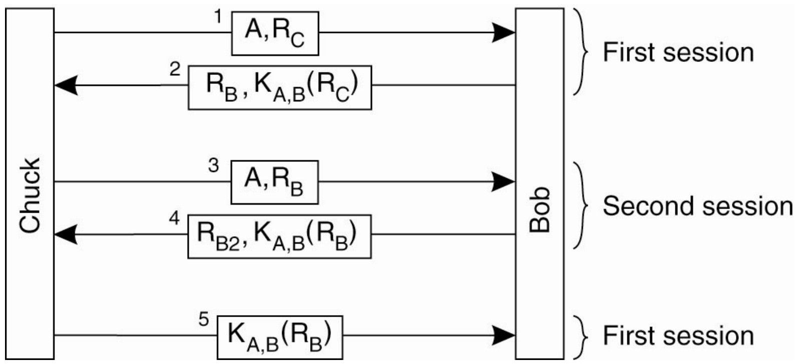

Figure 9-14. The reflection attack.

27

Authentication Using a Key Distribution Center (1)

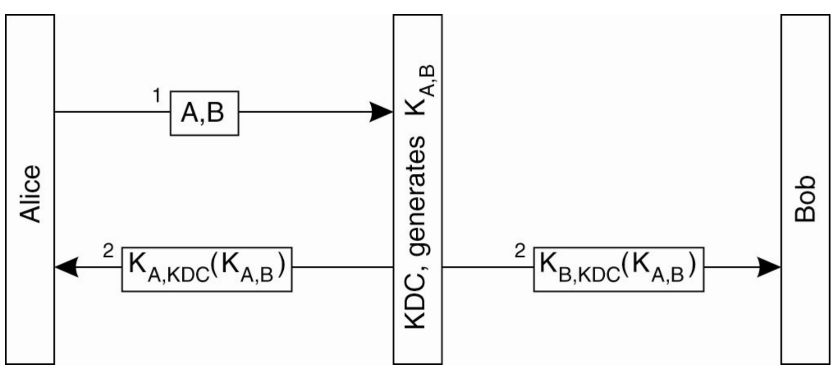

Figure 9-15. The principle of using a KDC.

28

Authentication Using a Key Distribution Center (2)

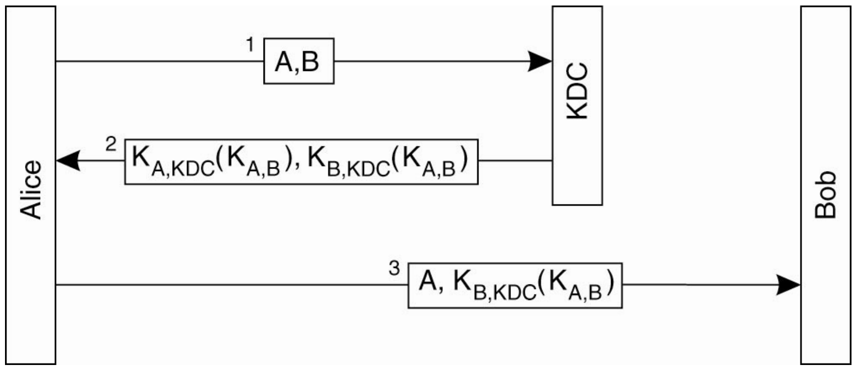

Figure 9-16. Using a ticket and letting Alice set up a connection to Bob.

29

Authentication Using a Key Distribution Center (3)

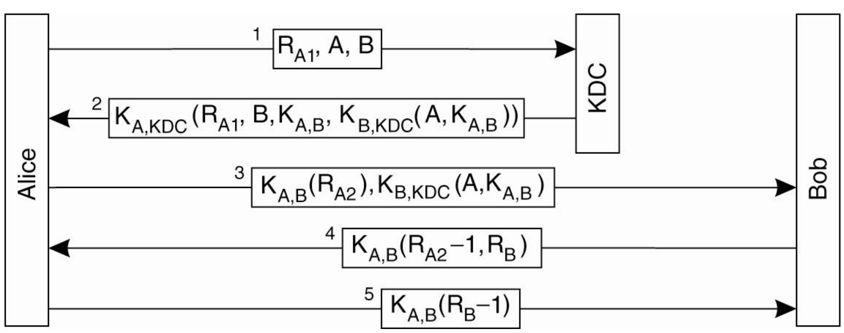

Figure 9-17. The Needham-Schroeder authentication protocol.

30

Authentication Using a Key Distribution Center (4)

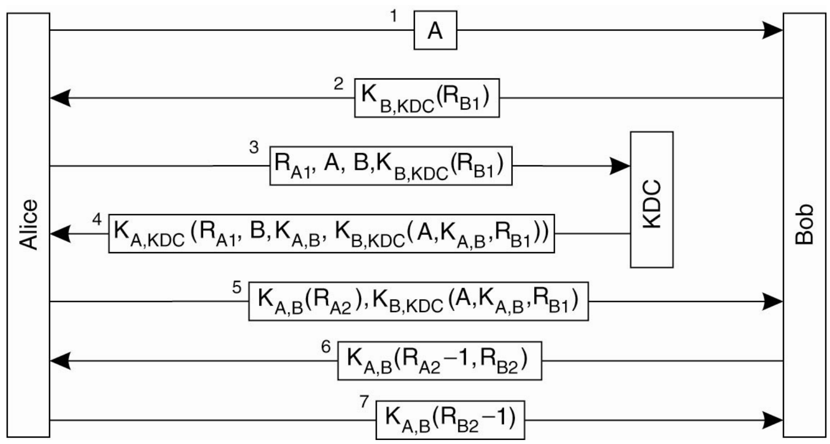

Figure 9-18. Protection against malicious reuse of a previously generated session key in the Needham-Schroeder protocol.

31

Authentication Using a Key Distribution Center (5)

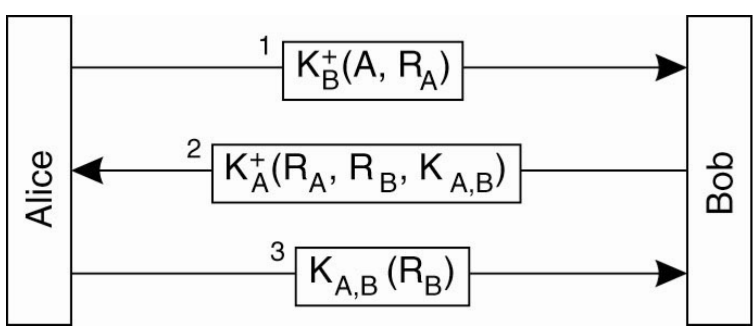

Figure 9-19. Mutual authentication in a public-key cryptosystem.

32

Example: Kerberos (1)

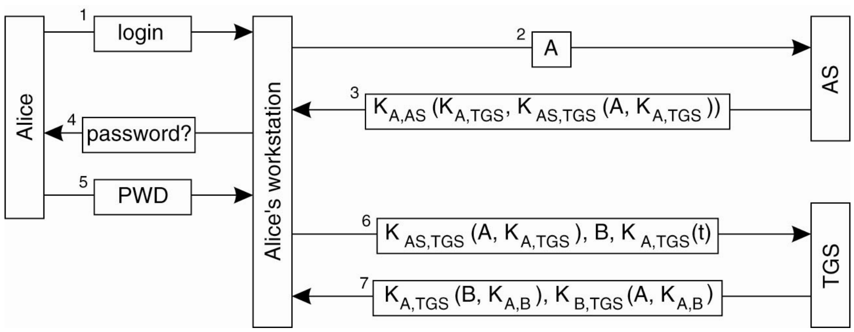

Figure 9-23. Authentication in Kerberos.

34

Example: Kerberos (2)

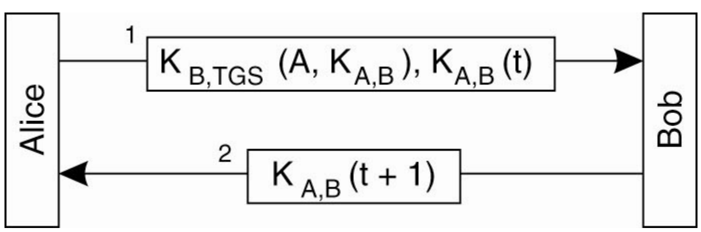

Figure 9-24. Setting up a secure channel in Kerberos.

35