Chapter 30

Message Security, User Authentication, and Key Management

30.1 Message Security

Privacy

Authentication

Integrity

Nonrepudiation

Figure 30.1 Message security

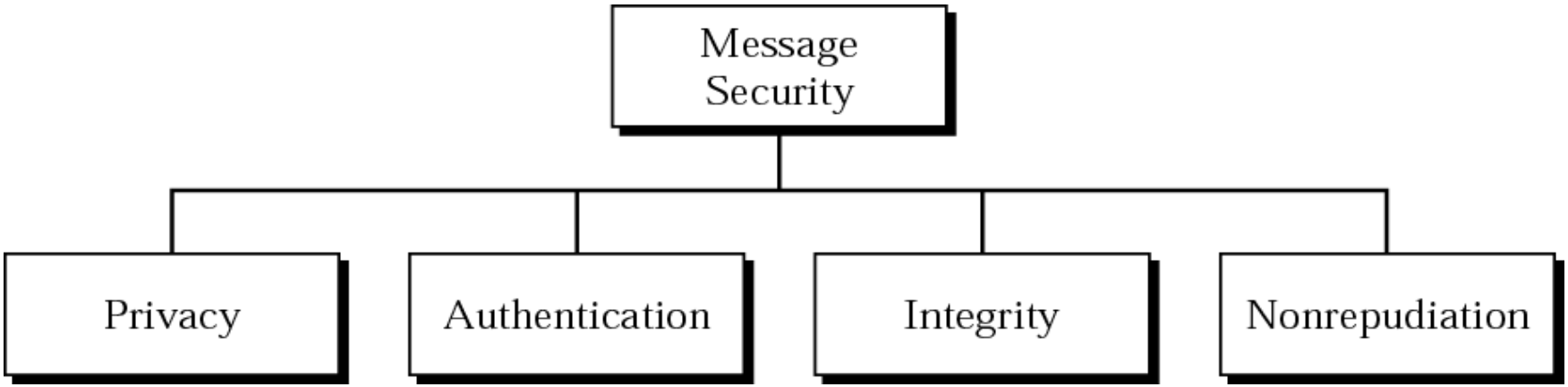


Figure 30.2 Privacy using symmetric-key encryption

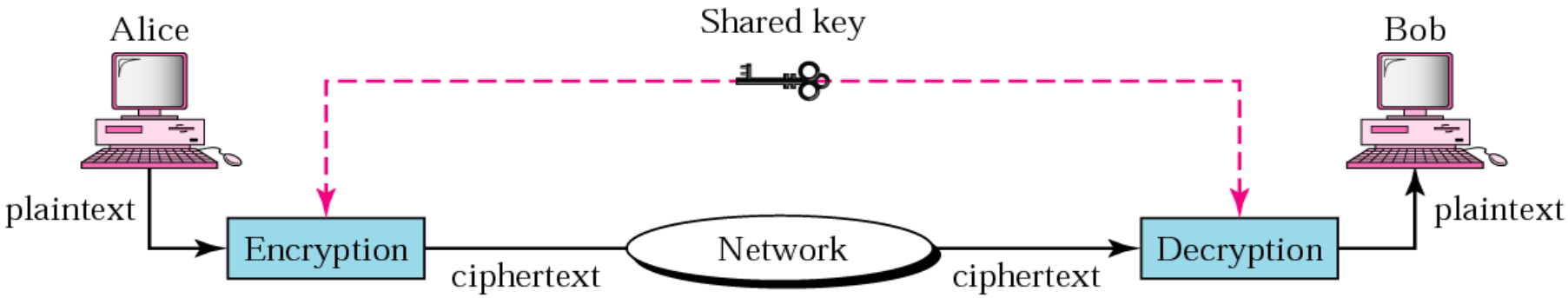
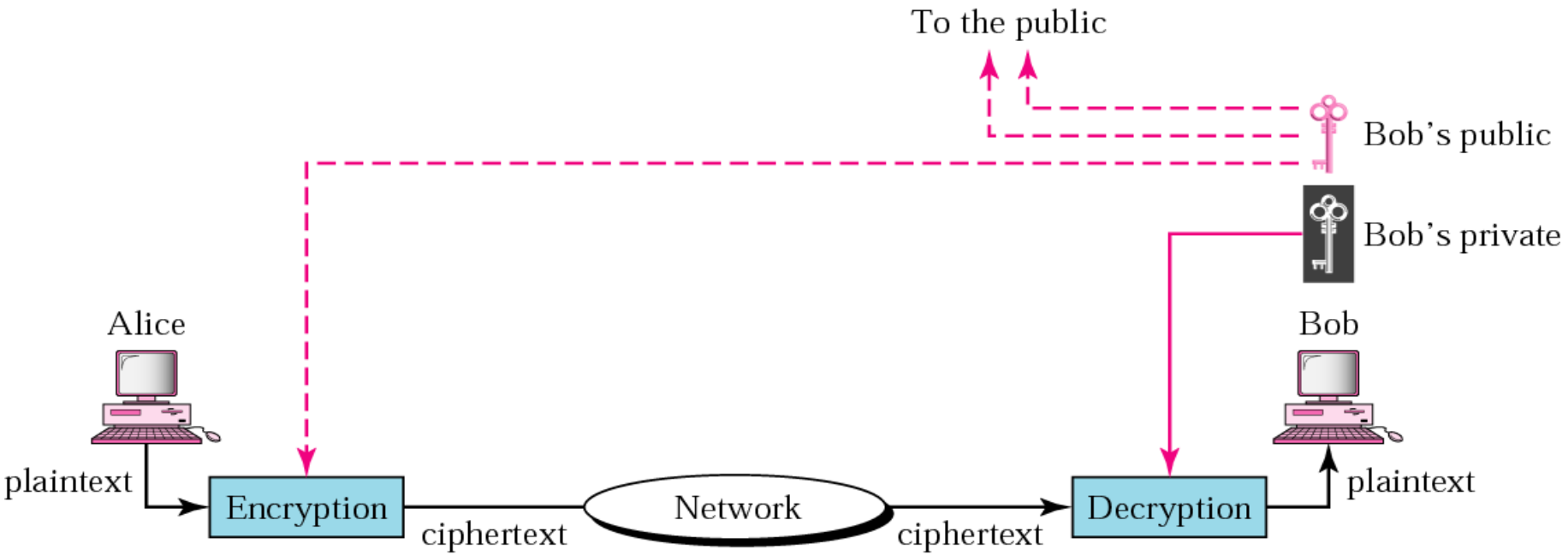


Figure 30.3 Privacy using public-key encryption

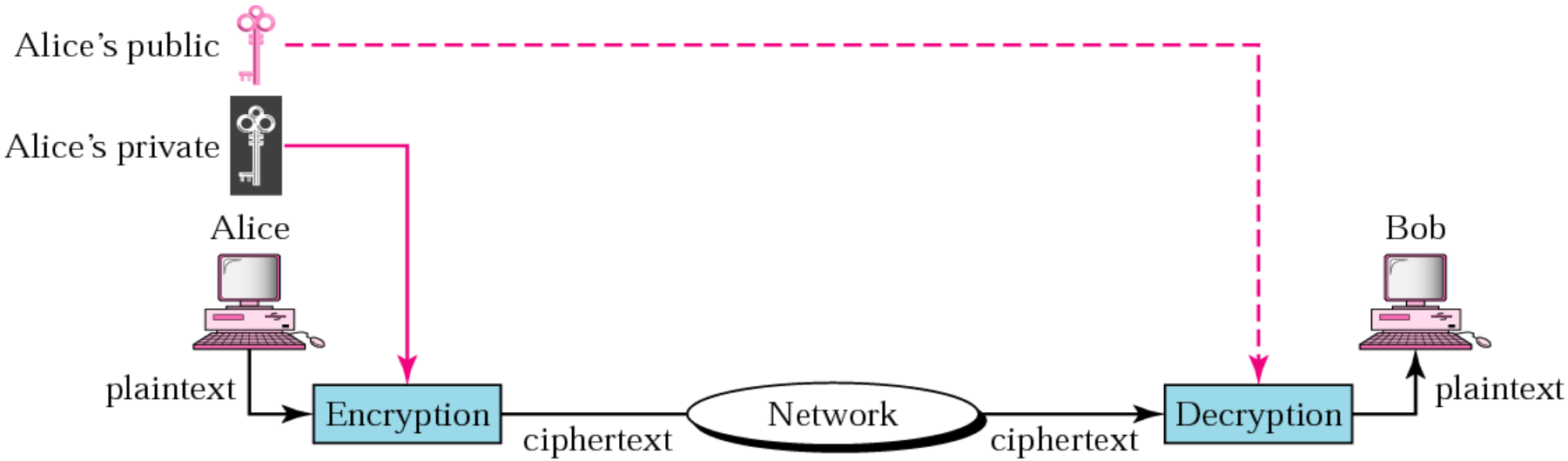


30.2 Digital Signature

Signing the Whole Document

Signing the Digest

Figure 30.4 Signing the whole document



Note:

Digital signature does not provide privacy. If there is a need for privacy, another layer of encryption/decryption must be applied.

Figure 30.5 Signing the digest

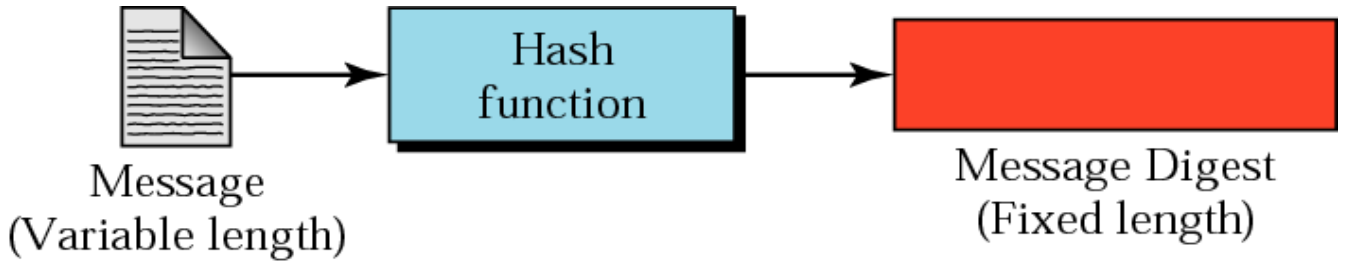


Figure 30.6 Sender site

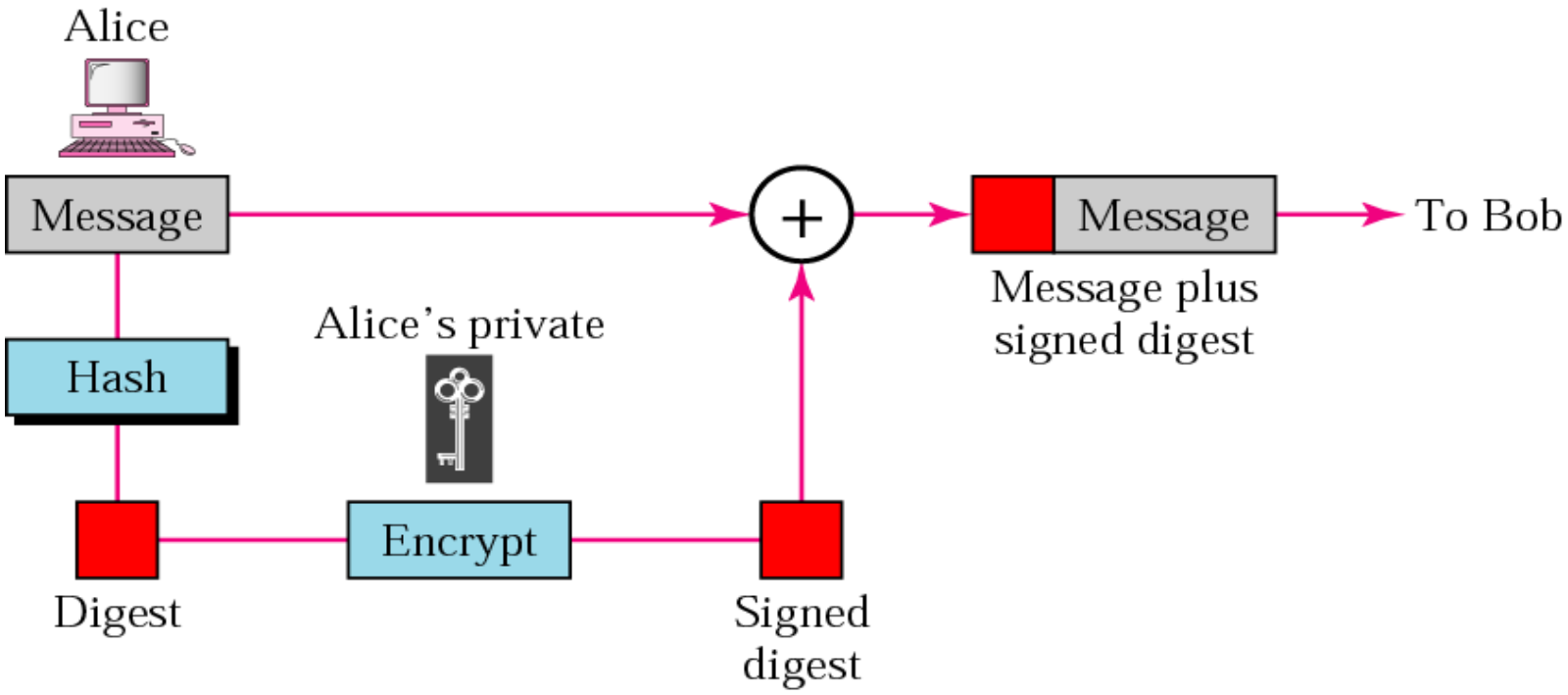
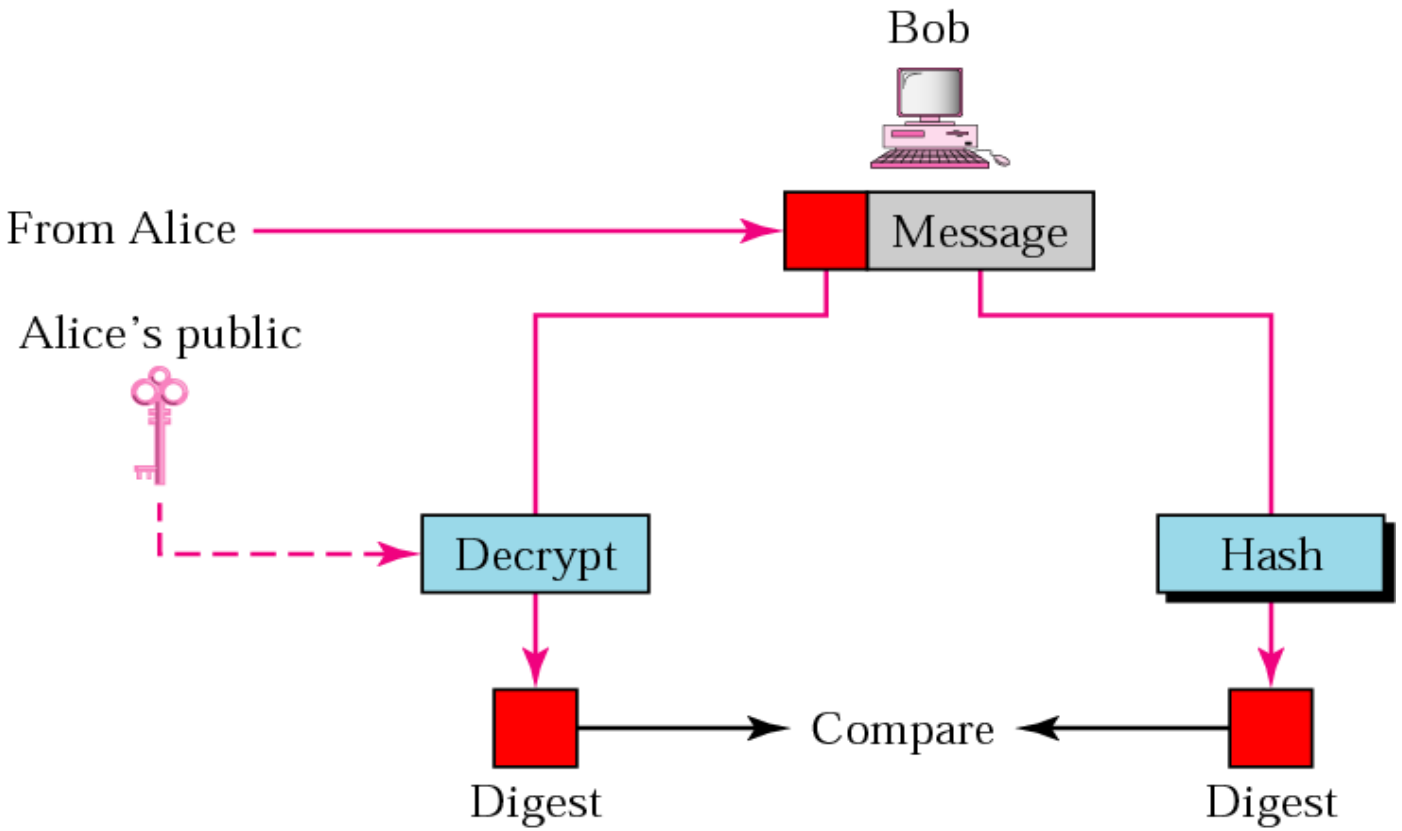


Figure 30.7 Receiver site



30.3 User Authentication

With Symmetric Key

With Public Key

Figure 30.8 Using a symmetric key only

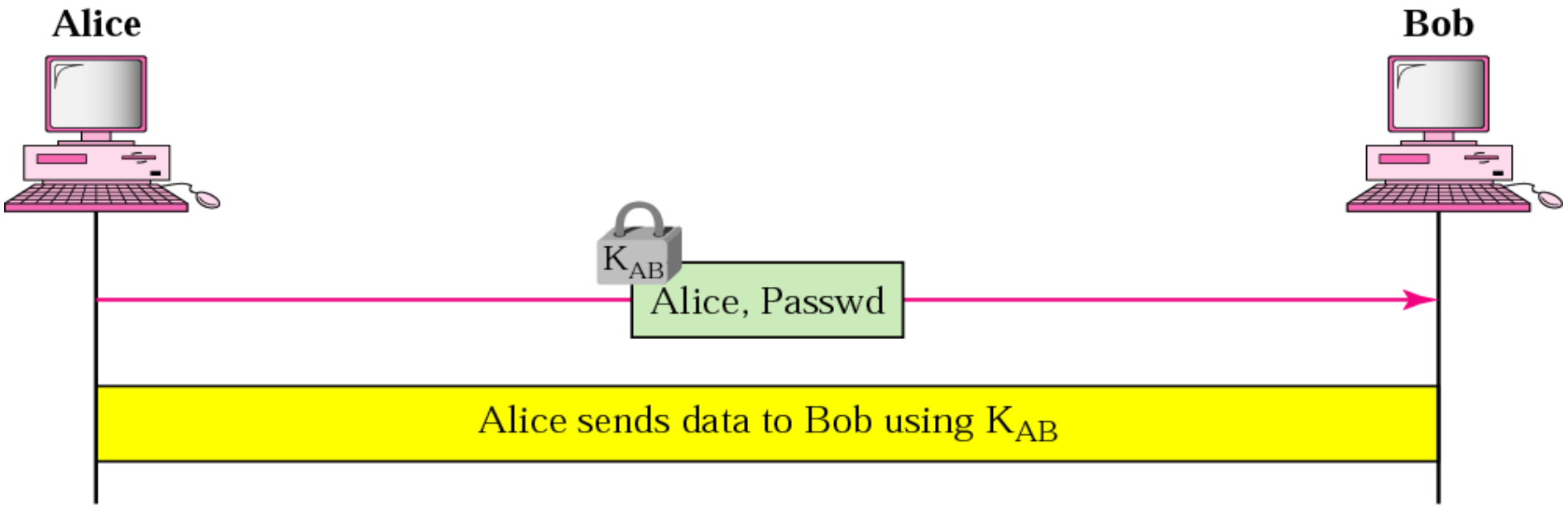


Figure 30.9 Using a nonce

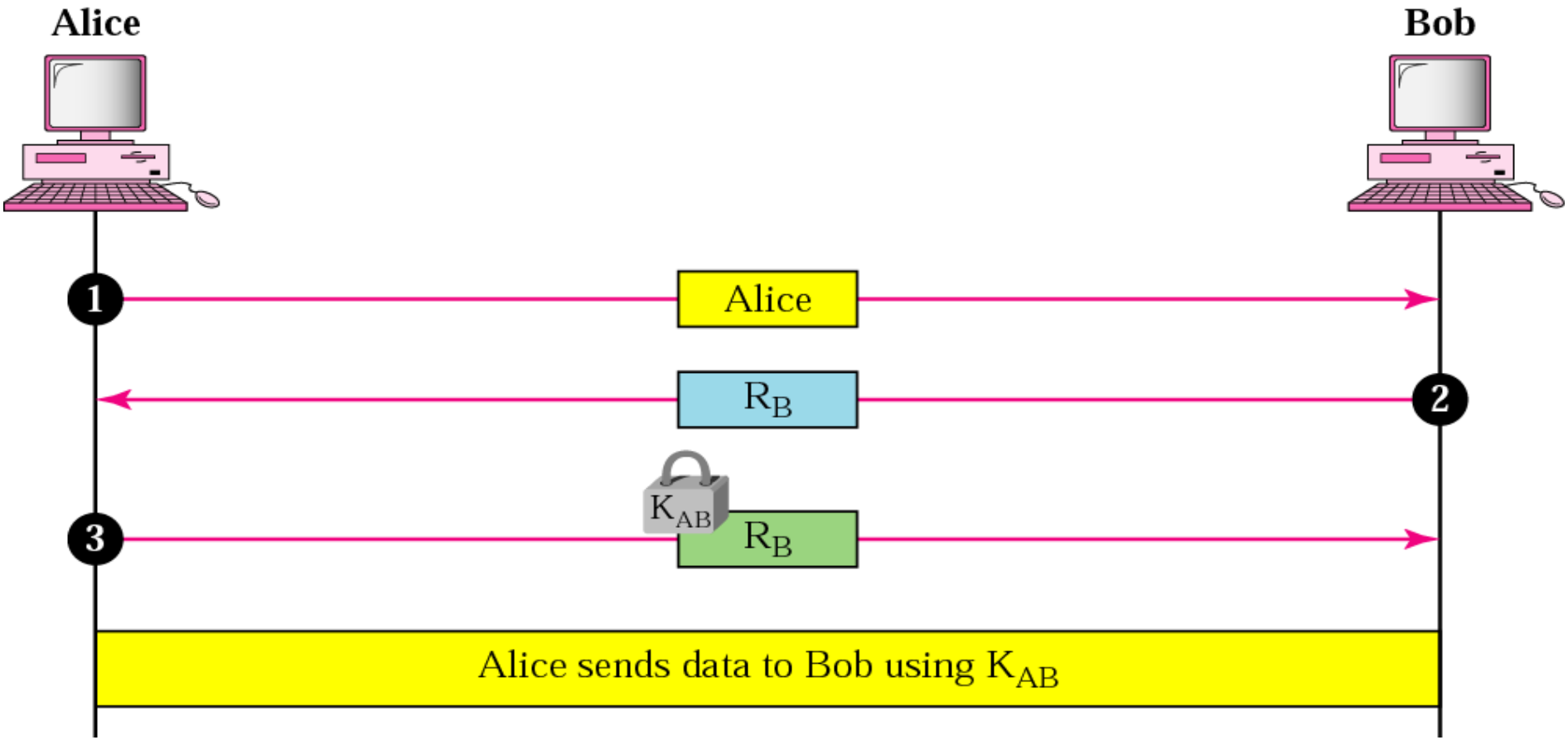
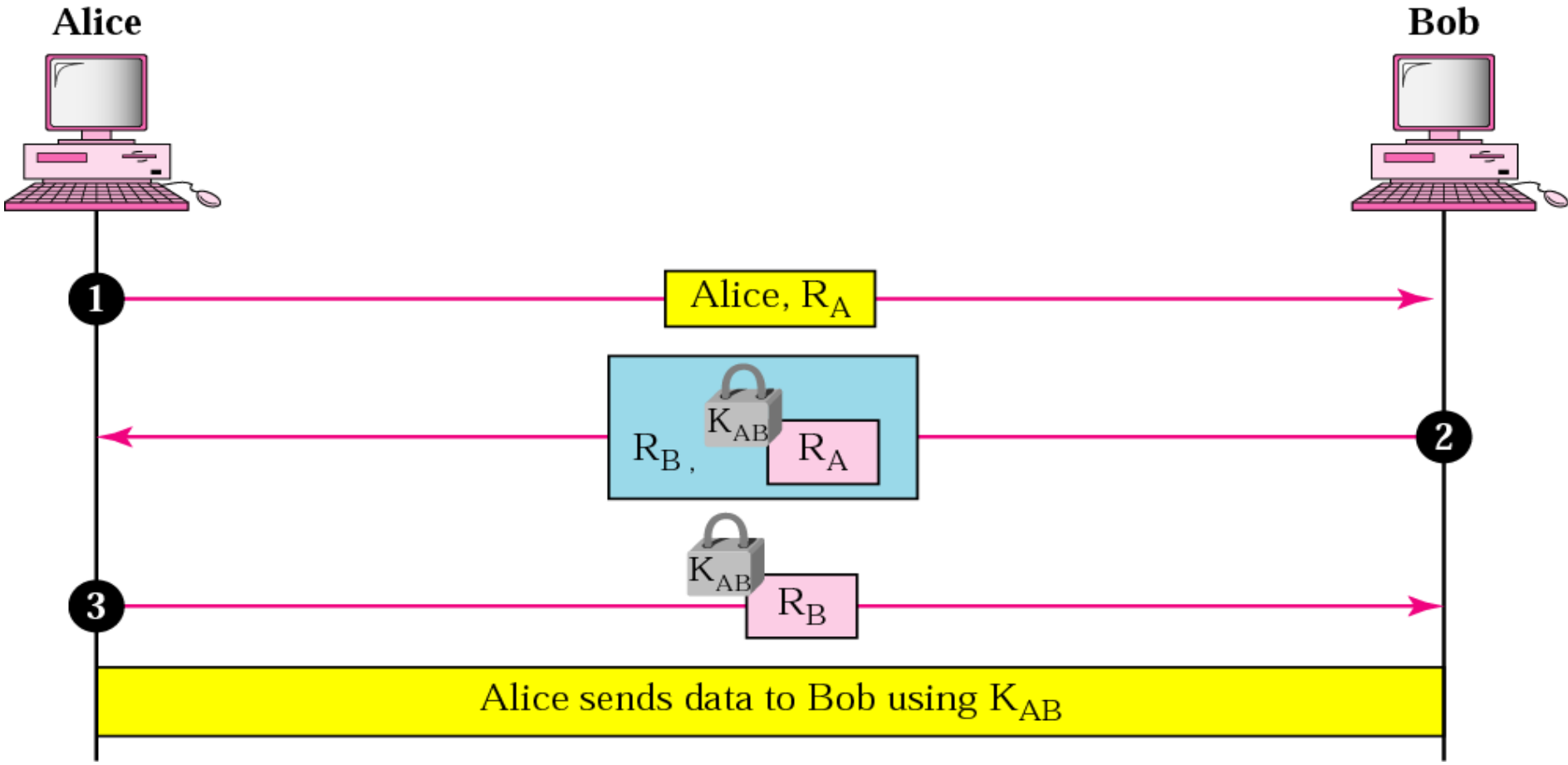


Figure 30.10 Bidirectional authentication



30.4 Key Management

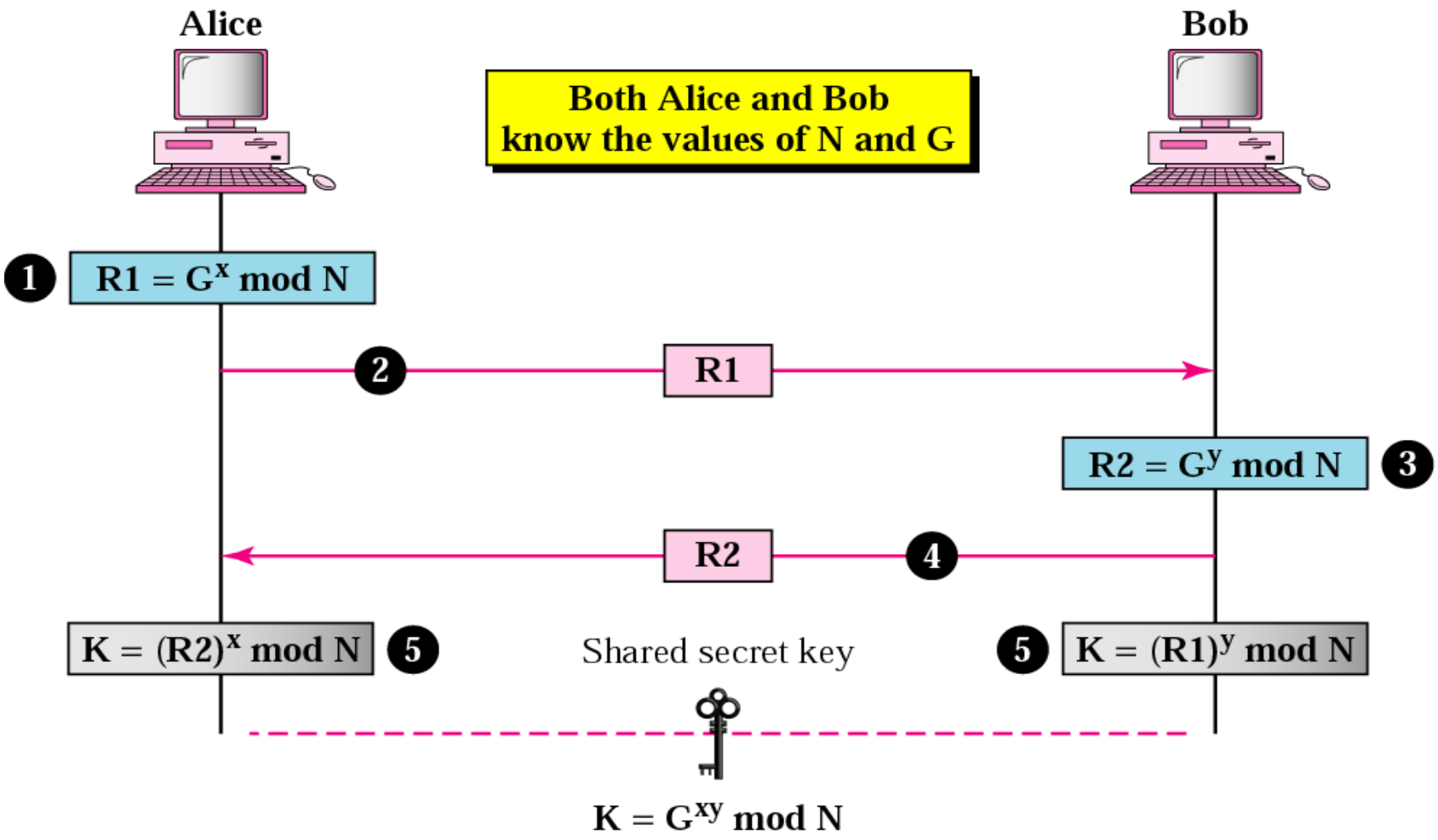
Symmetric-Key Distribution

Public-Key Certification

Note:

A symmetric key between two parties is useful if it is used only once; it must be created for one session and destroyed when the session is over.

Figure 30.11 Diffie-Hellman method



Note:

The symmetric (shared) key in the Diffie-Hellman protocol is $K = G^{xy} \bmod N$.

Example 2

Assume G = 7 and N = 23. The steps are as follows:

1. Alice chooses x = 3 and calculates R1 = 7^3 mod 23 = 21.
2. Alice sends the number 21 to Bob.
3. Bob chooses y = 6 and calculates R2 = 7^6 mod 23 = 4.
4. Bob sends the number 4 to Alice.
5. Alice calculates the symmetric key K = 4^3 mod 23 = 18.
6. Bob calculates the symmetric key K = 21^6 mod 23 = 18.

The value of K is the same for both Alice and Bob;
G^{xy} mod N = 7^{18} mod 23 = 18.

Figure 30.12 Man-in-the-middle attack

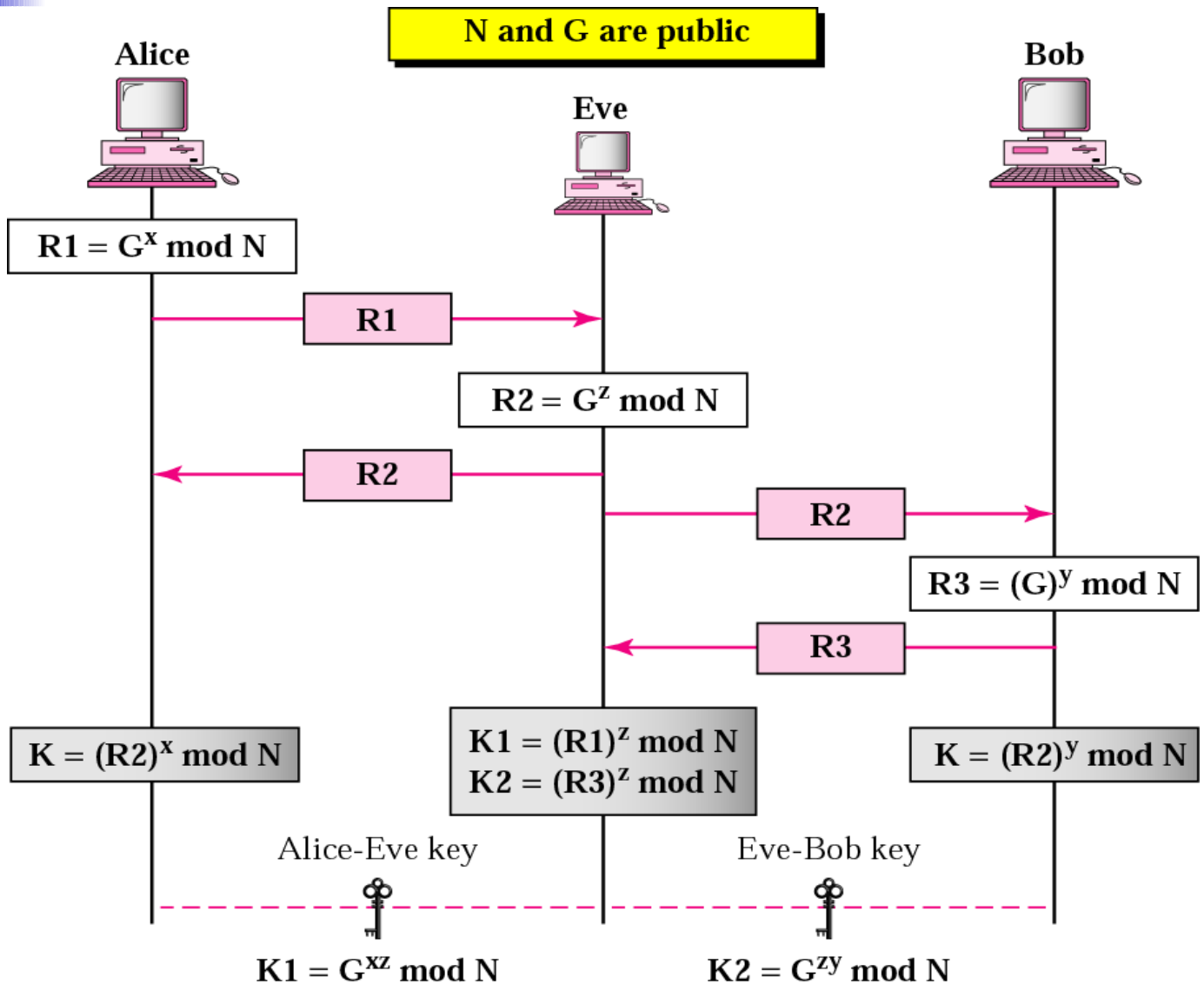


Figure 30.13 First approach using KDC

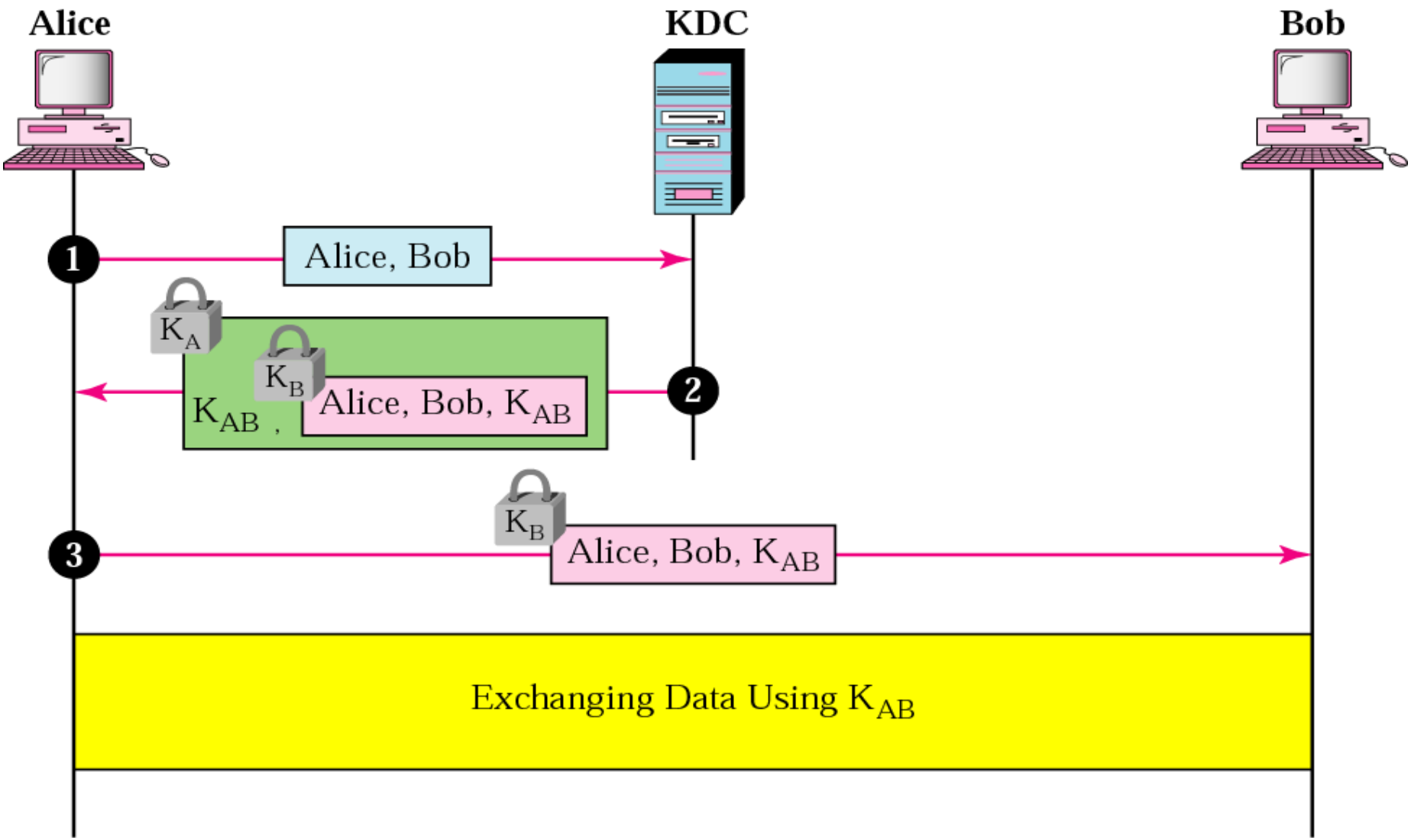


Figure 30.14 Needham-Schroeder protocol

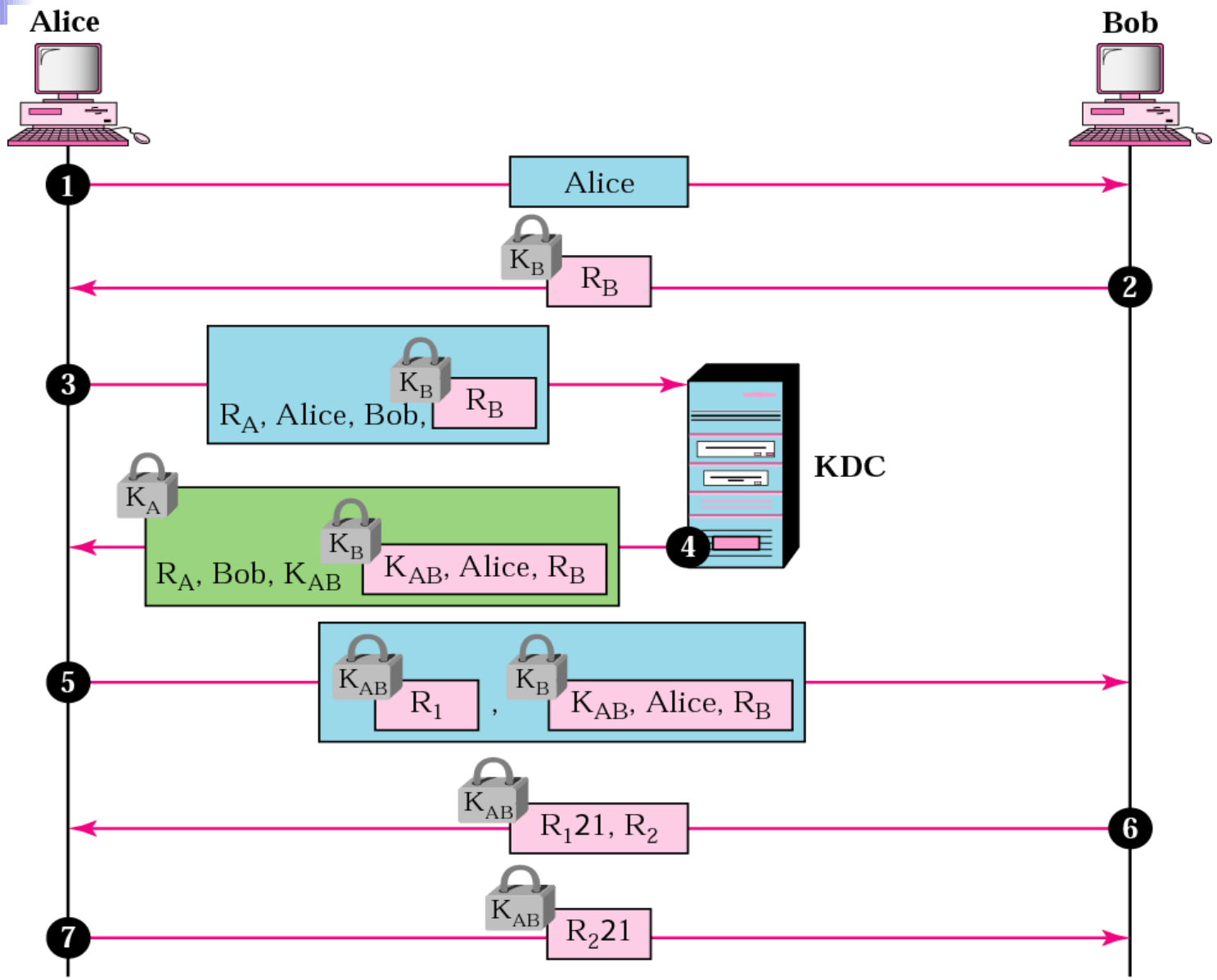
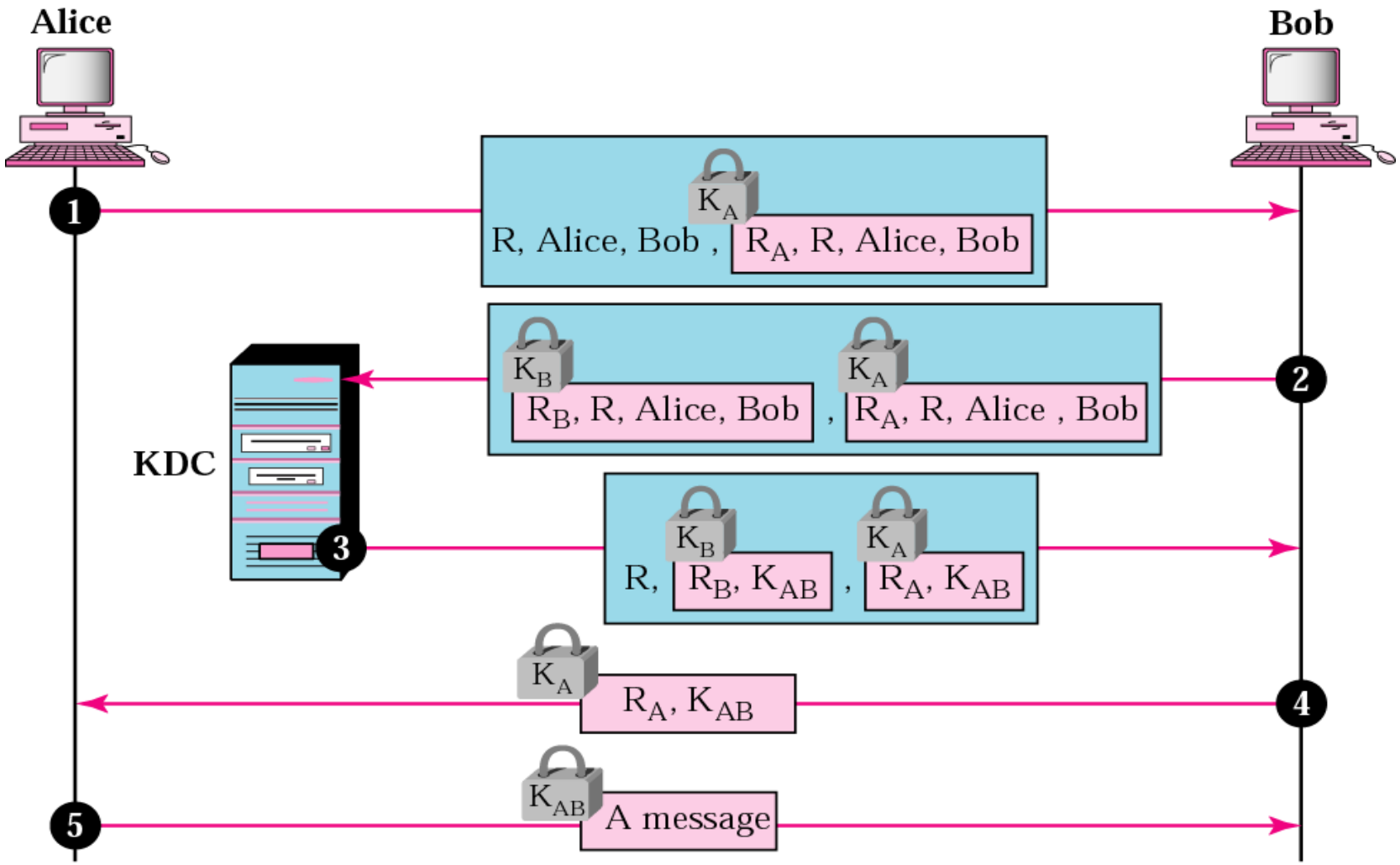


Figure 30.15 Otway-Rees protocol



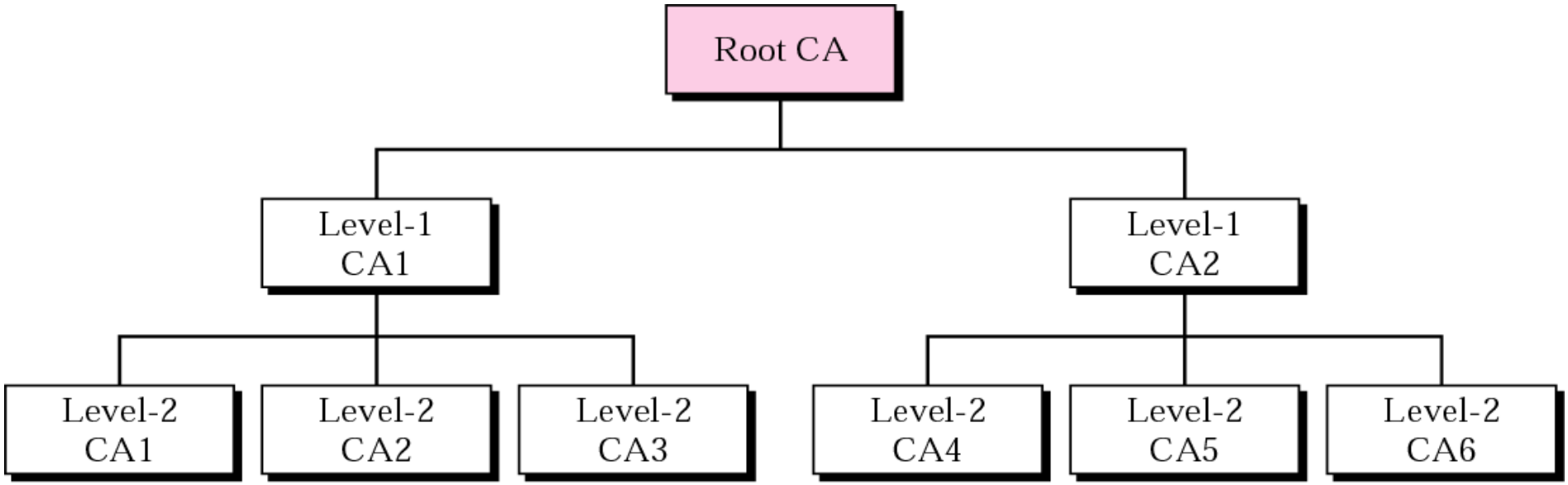
Note:

In public-key cryptography, everyone has access to everyone's public key.

Table 30.1 X.500 fields

Field	*Explanation*
Version	Version number of X.509
Serial number	The unique identifier used by the CA
Signature	The certificate signature
Issuer	The name of the CA defined by X.509
Validity period	Start and end period that certificate is valid
Subject name	The entity whose public key is being certified
Public key	The subject public key and the algorithms that use it

Figure 30.16 PKI hierarchy



30.5 Kerberos

Servers

Operation

Using Different Servers

Version 5

Realms

Figure 30.17 Kerberos servers

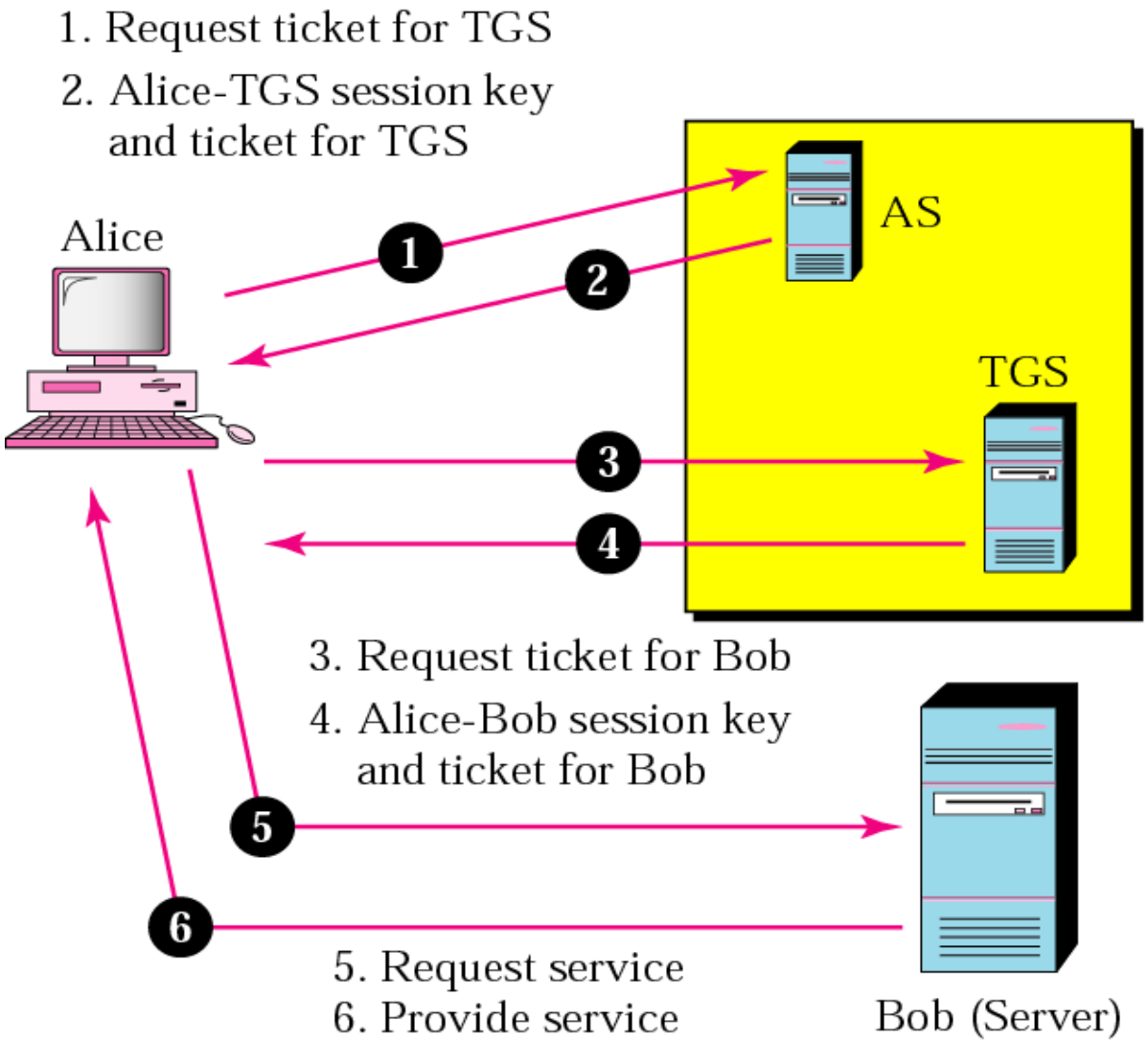


Figure 30.18 *Kerberos example*