Data Communications and Networking Fourth Edition

Forouzan

Chapter 30

Cryptography

30-1 INTRODUCTION

Let us introduce the issues involved in cryptography. First, we need to define some terms; then we give some taxonomies.

Topics discussed in this section:

Definitions

Two Categories

Figure 30.1 *Cryptography components*

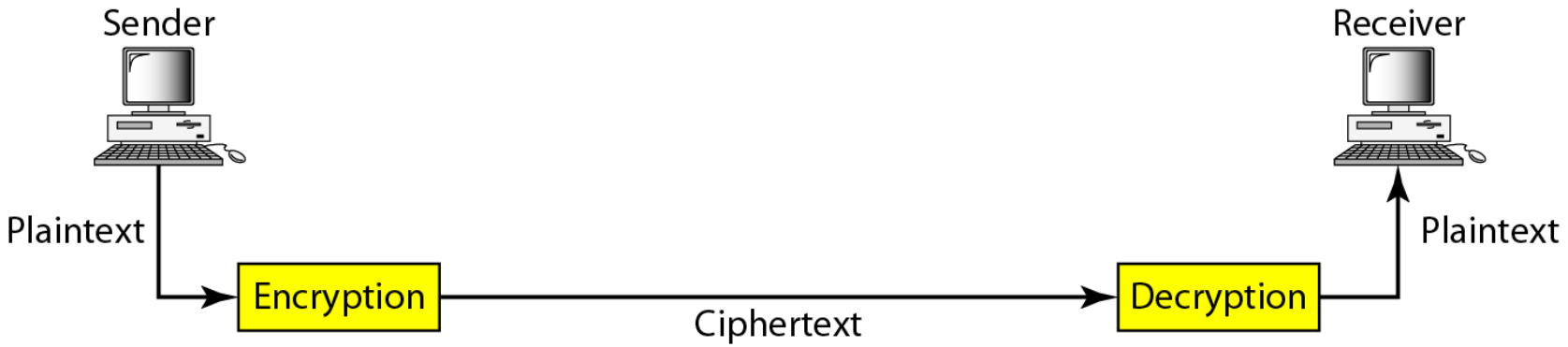


Figure 30.2 *Categories of cryptography*

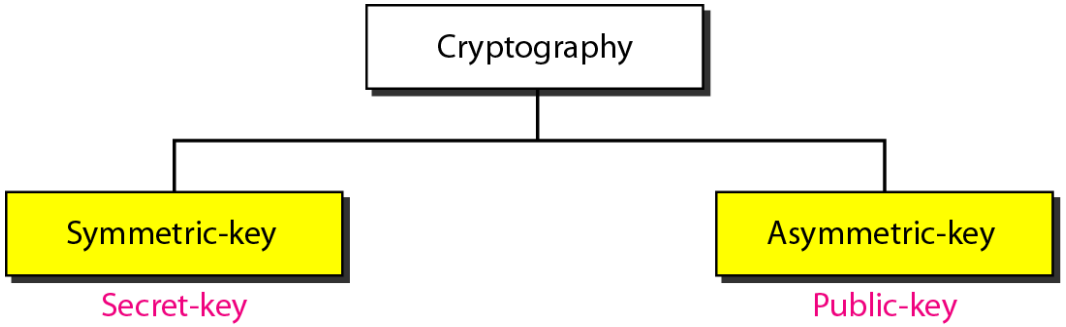
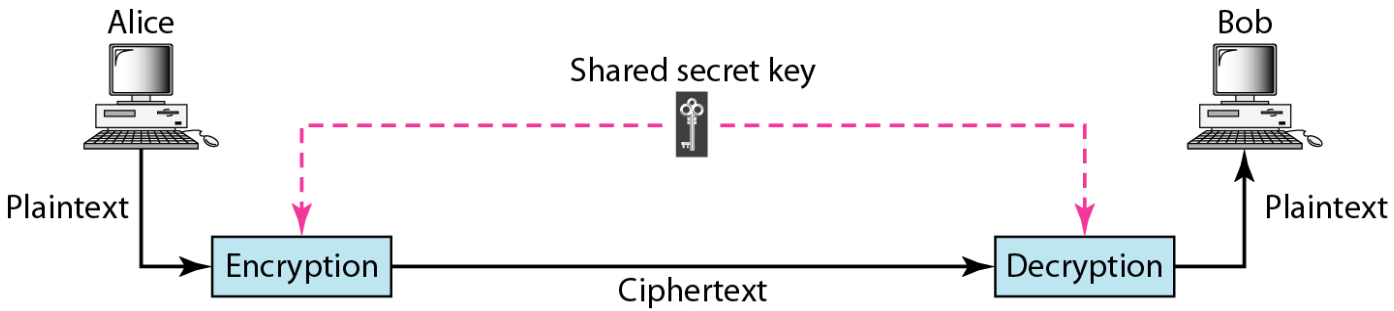


Figure 30.3 *Symmetric-key cryptography*



Note

In symmetric-key cryptography, the same key is used by the sender (for encryption) and the receiver (for decryption). The key is shared.

Figure 30.4 *Asymmetric-key cryptography*

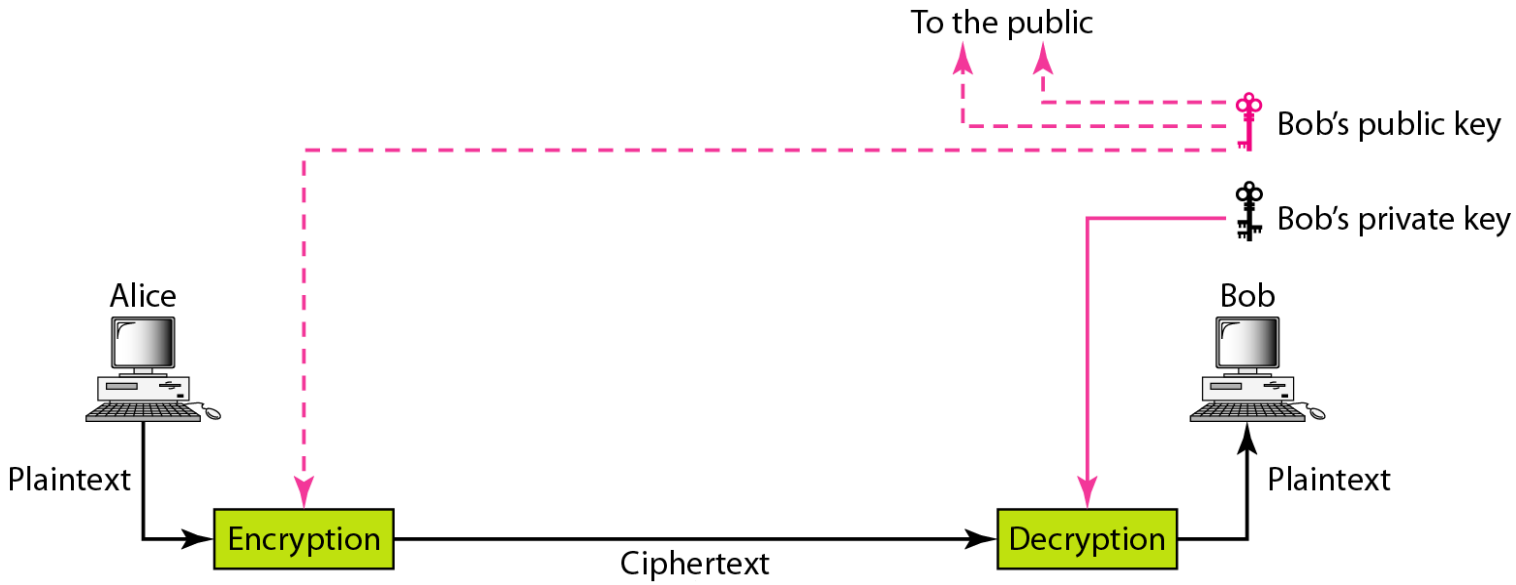
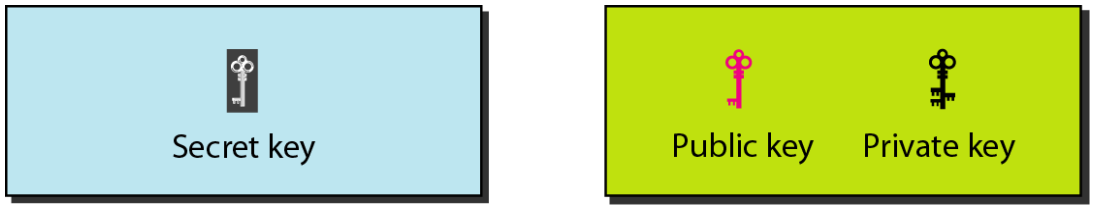


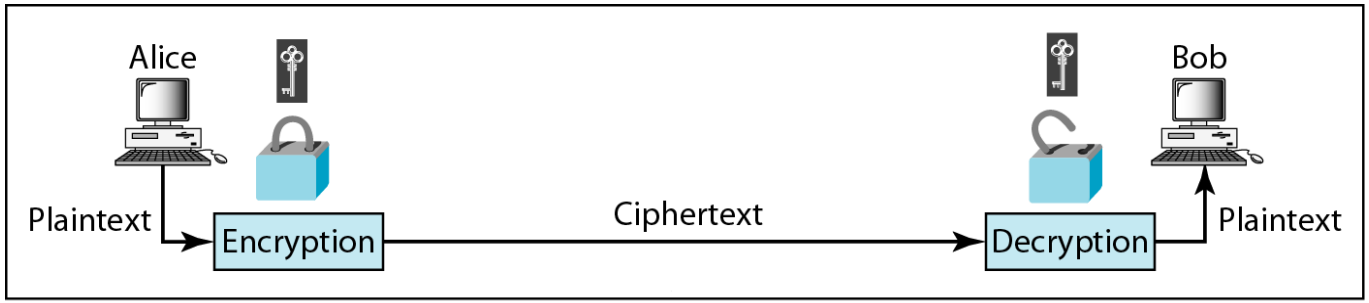
Figure 30.5 *Keys used in cryptography*



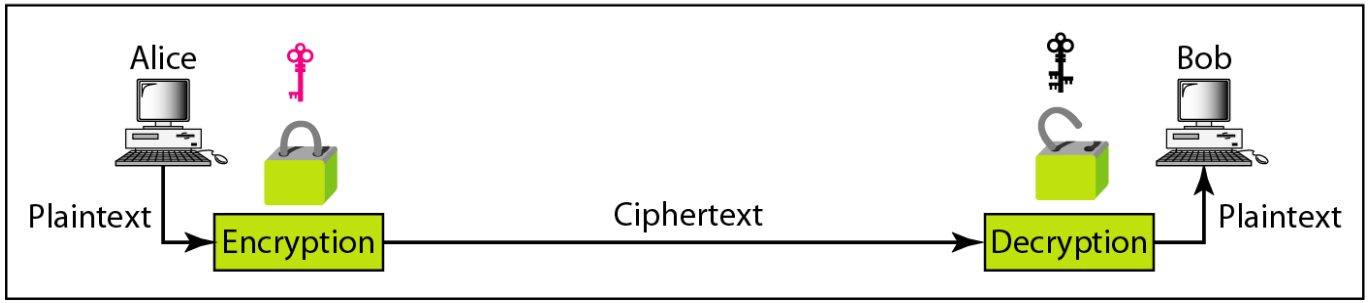
Symmetric-key cryptography

Asymmetric-key cryptography

Figure 30.6 *Comparison between two categories of cryptography*



a. Symmetric-key cryptography



b. Asymmetric-key cryptography

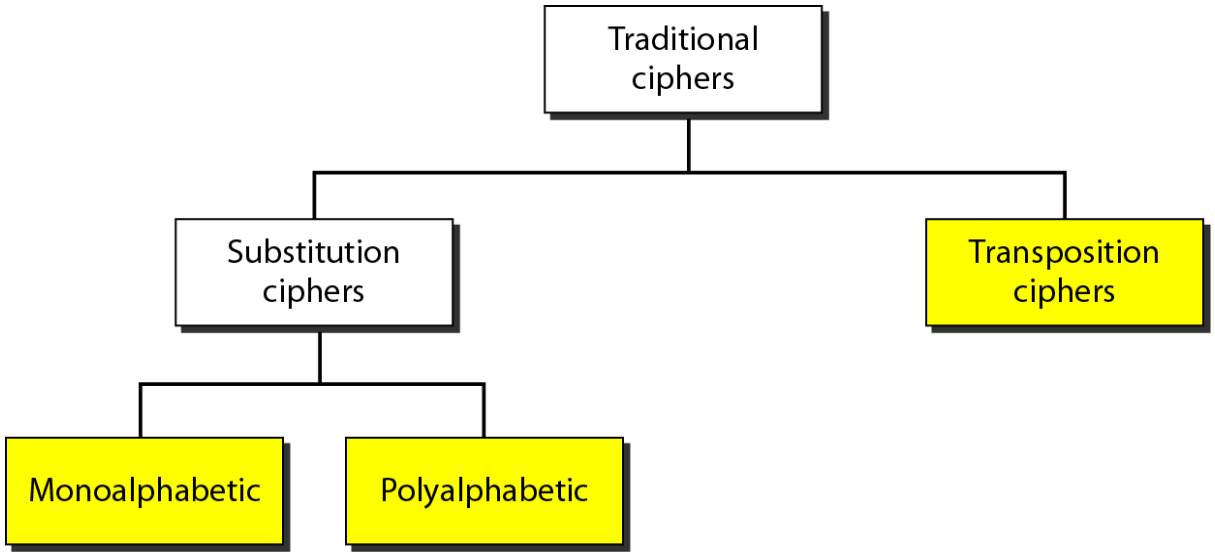
30-2 SYMMETRIC-KEY CRYPTOGRAPHY

Symmetric-key cryptography started thousands of years ago when people needed to exchange secrets (for example, in a war). We still mainly use symmetric-key cryptography in our network security.

Topics discussed in this section:

Traditional Ciphers
Simple Modern Ciphers
Modern Round Ciphers
Mode of Operation

Figure 30.7 *Traditional ciphers*



Note

A substitution cipher replaces one symbol with another.

Example 30.1

The following shows a plaintext and its corresponding ciphertext. Is the cipher monoalphabetic?

Plaintext: HELLO
Ciphertext: KHOOR

Solution

The cipher is probably monoalphabetic because both occurrences of L's are encrypted as O's.

Example 30.2

The following shows a plaintext and its corresponding ciphertext. Is the cipher monoalphabetic?

Plaintext: HELLO
Ciphertext: ABNZF

Solution

The cipher is not monoalphabetic because each occurrence of L is encrypted by a different character. The first L is encrypted as N; the second as Z.

Note

The shift cipher is sometimes referred to as the Caesar cipher.

Example 30.3

Use the shift cipher with key = 15 to encrypt the message "HELLO."

Solution

We encrypt one character at a time. Each character is shifted 15 characters down. Letter H is encrypted to W. Letter E is encrypted to T. The first L is encrypted to A. The second L is also encrypted to A. And O is encrypted to D. The cipher text is WTAAD.

Example 30.4

Use the shift cipher with key = 15 to decrypt the message "WTAAD."

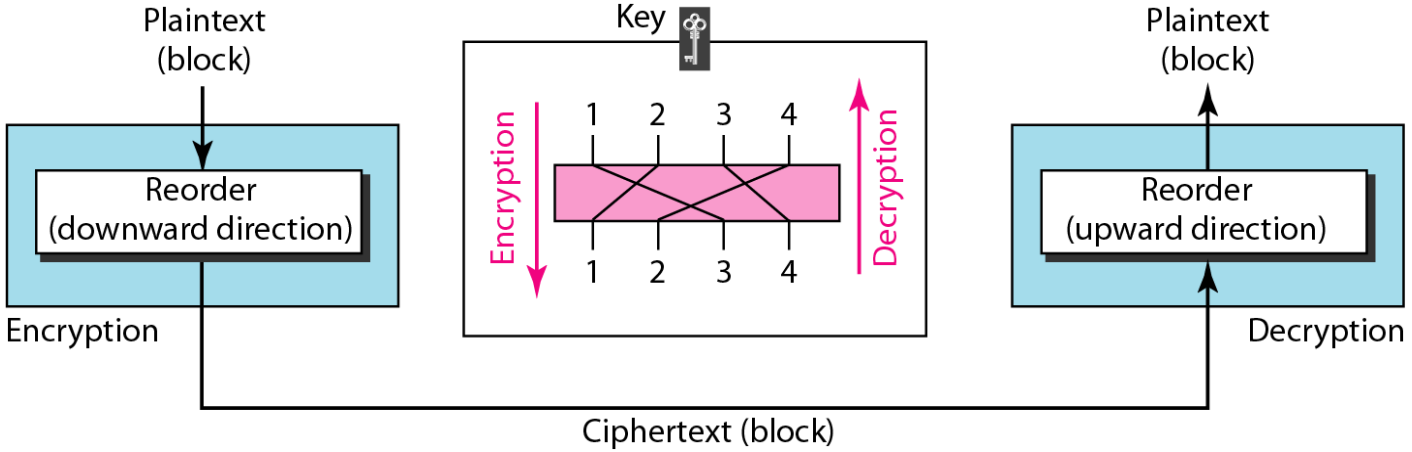
Solution

We decrypt one character at a time. Each character is shifted 15 characters up. Letter W is decrypted to H. Letter T is decrypted to E. The first A is decrypted to L. The second A is decrypted to L. And, finally, D is decrypted to O. The plaintext is HELLO.

Note

A transposition cipher reorders (permutes) symbols in a block of symbols.

Figure 30.8 *Transposition cipher*



Example 30.5

Encrypt the message "HELLO MY DEAR," using the key shown in Figure 30.8.

Solution

We first remove the spaces in the message. We then divide the text into blocks of four characters. We add a bogus character Z at the end of the third block. The result is HELL OMYD EARZ. We create a three-block ciphertext ELHLMDOYAZER.

Example 30.6

Using Example 30.5, decrypt the message "ELHLMDOYAZER".

Solution

The result is HELL OMYD EARZ. After removing the bogus character and combining the characters, we get the original message "HELLO MY DEAR."

Figure 30.9 *XOR cipher*

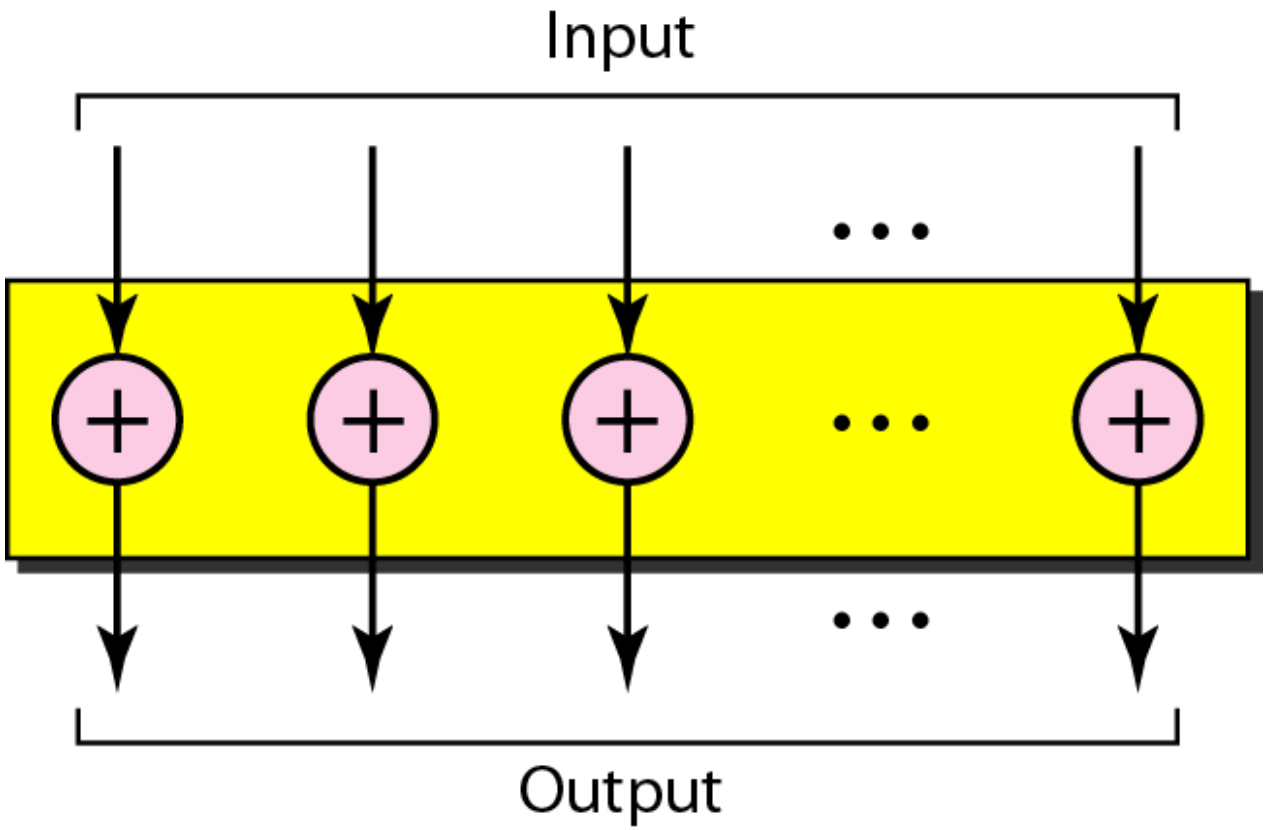


Figure 30.10 *Rotation cipher*

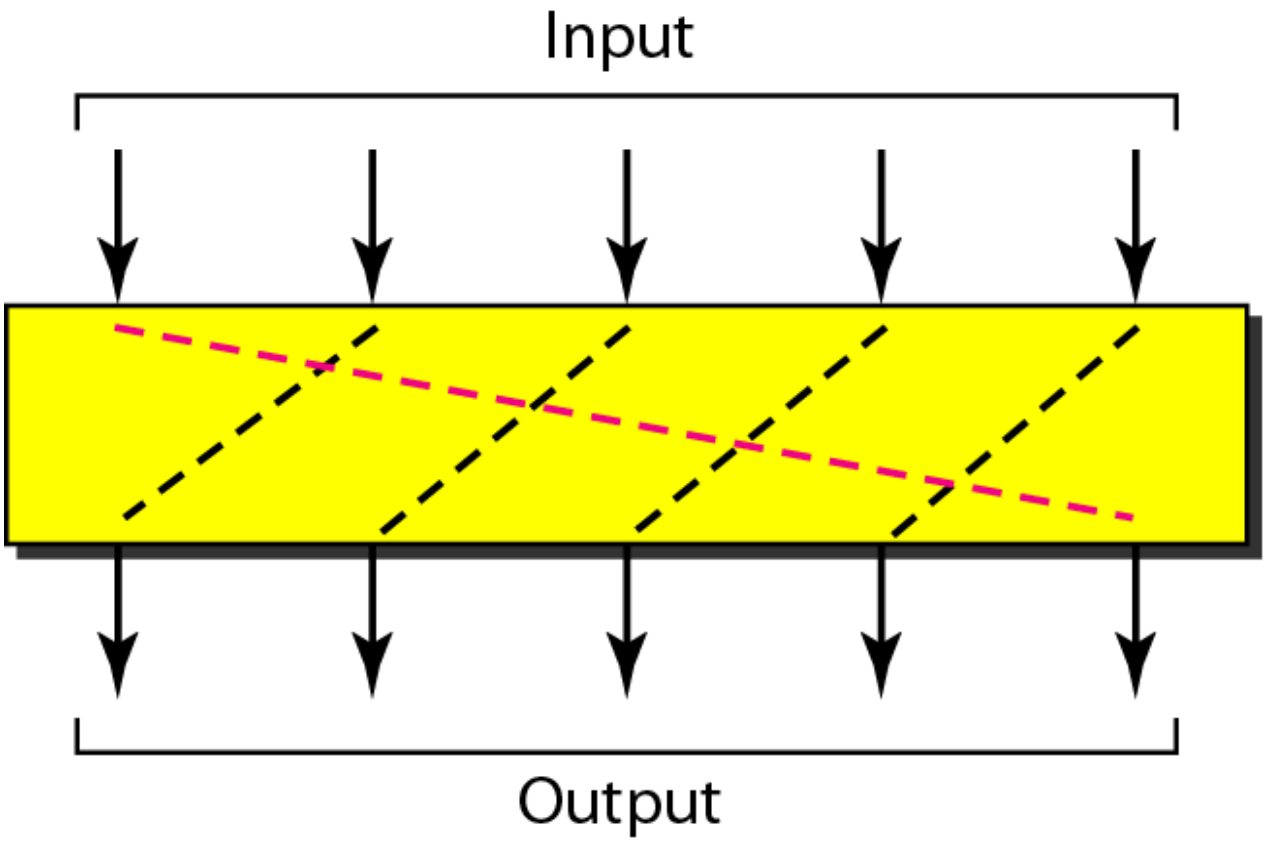


Figure 30.11 *S-box*

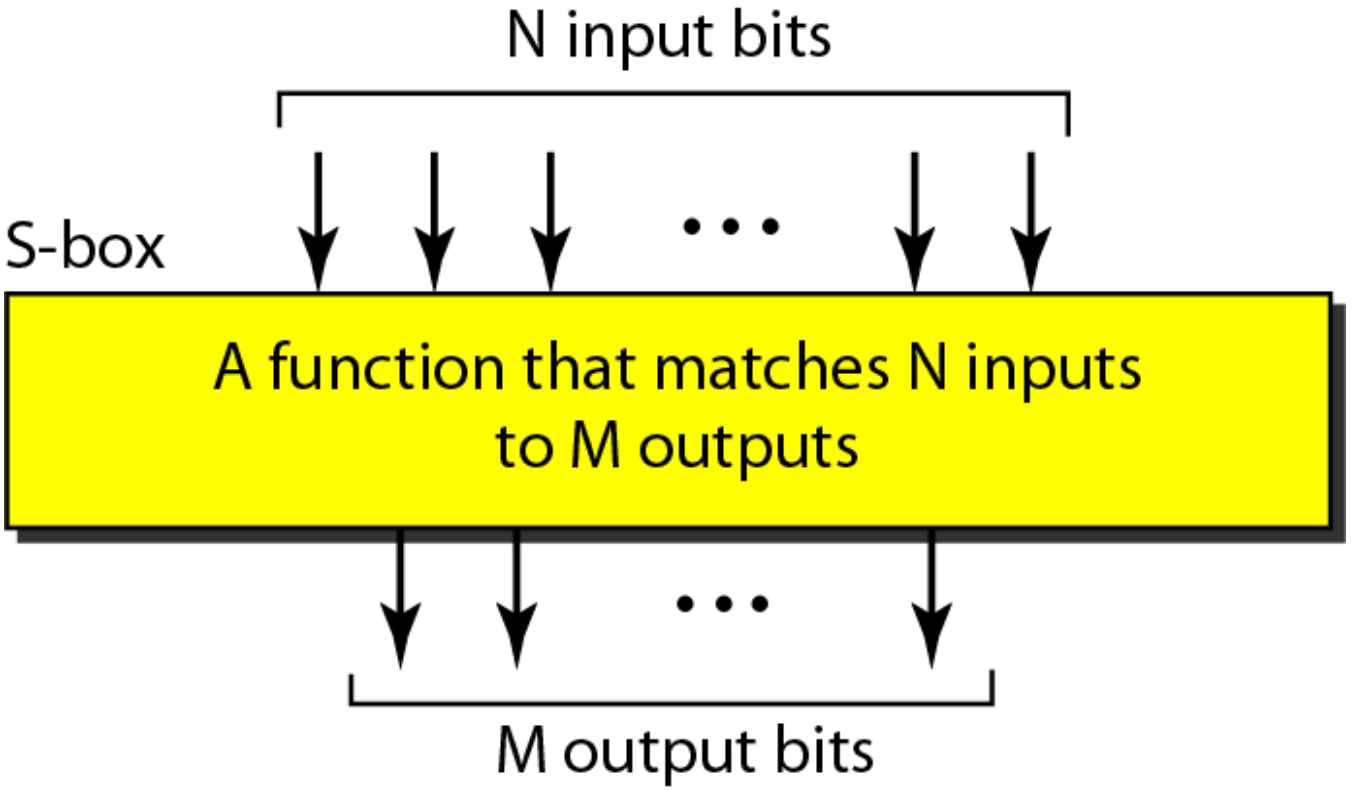
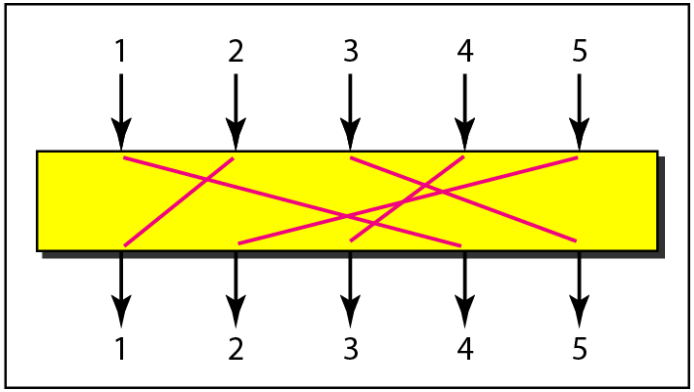
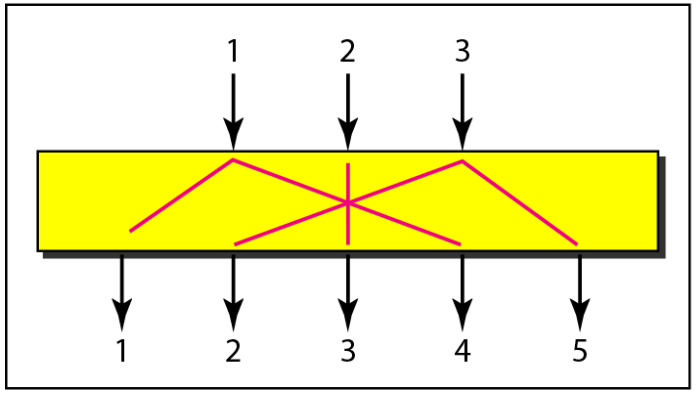


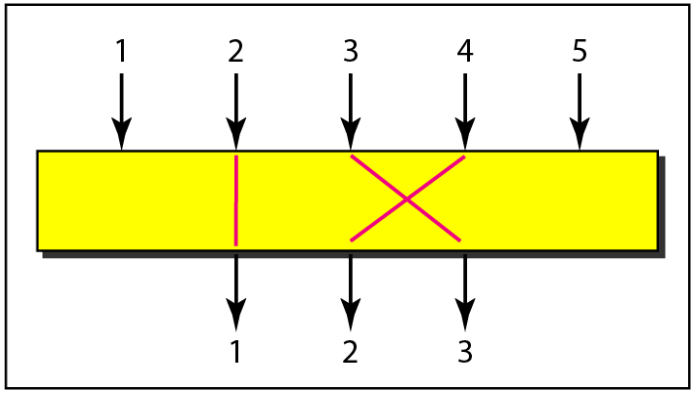
Figure 30.12 *P-boxes: straight, expansion, and compression*



a. Straight



b. Expansion



c. Compression

Figure 30.13 *DES*

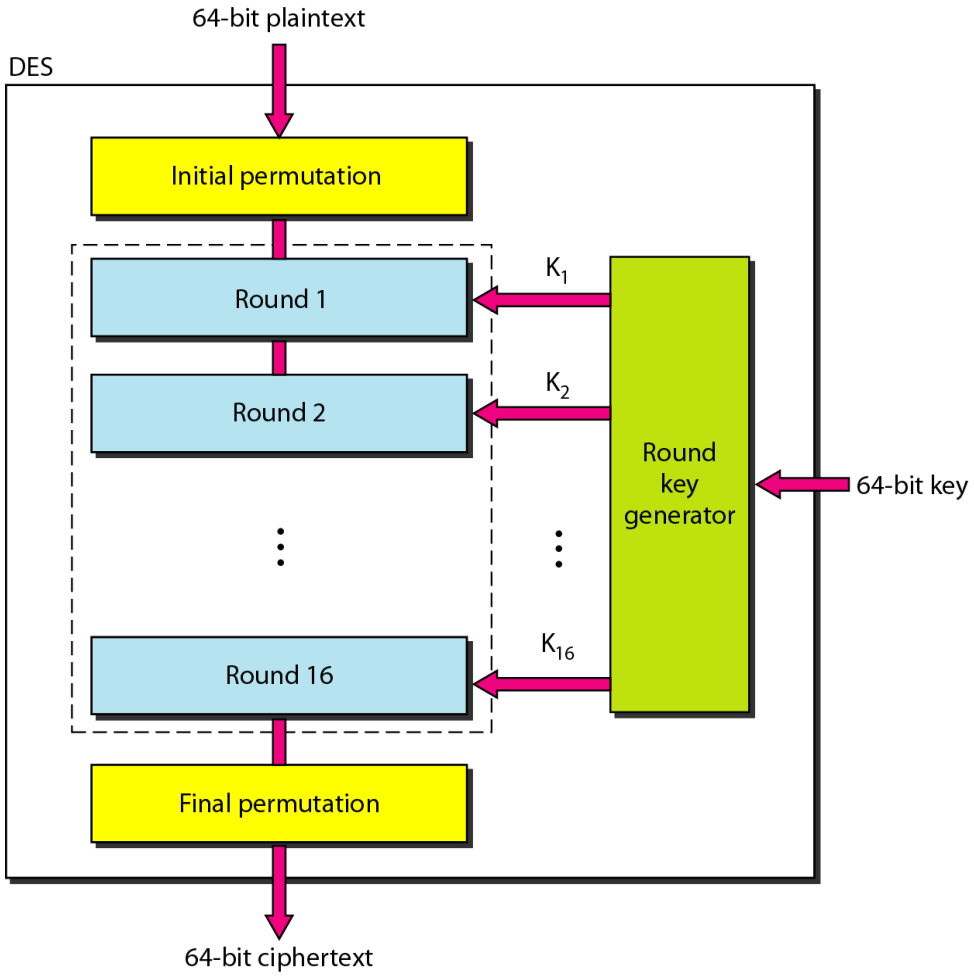


Figure 30.14 *One round in DES ciphers*

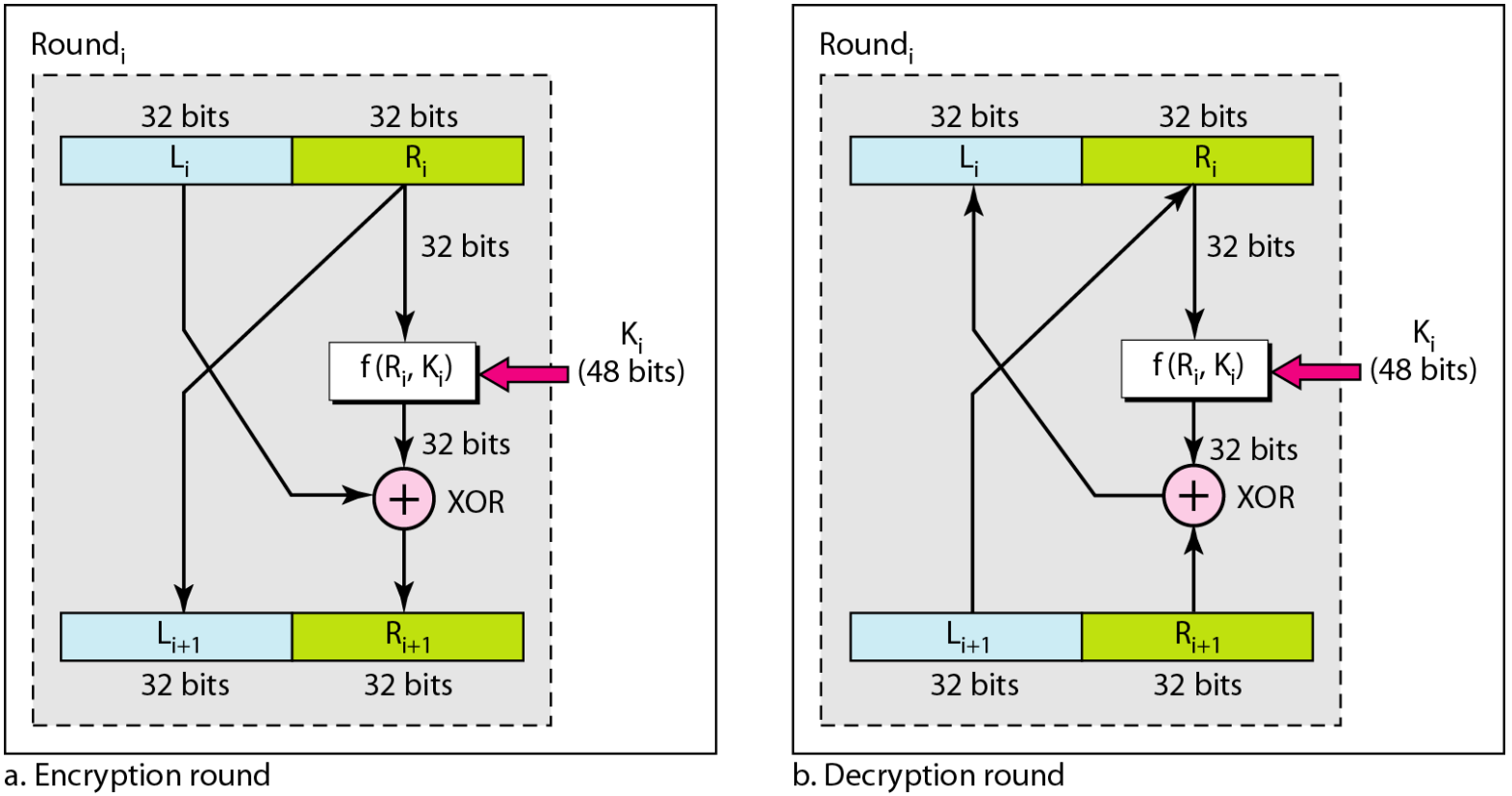
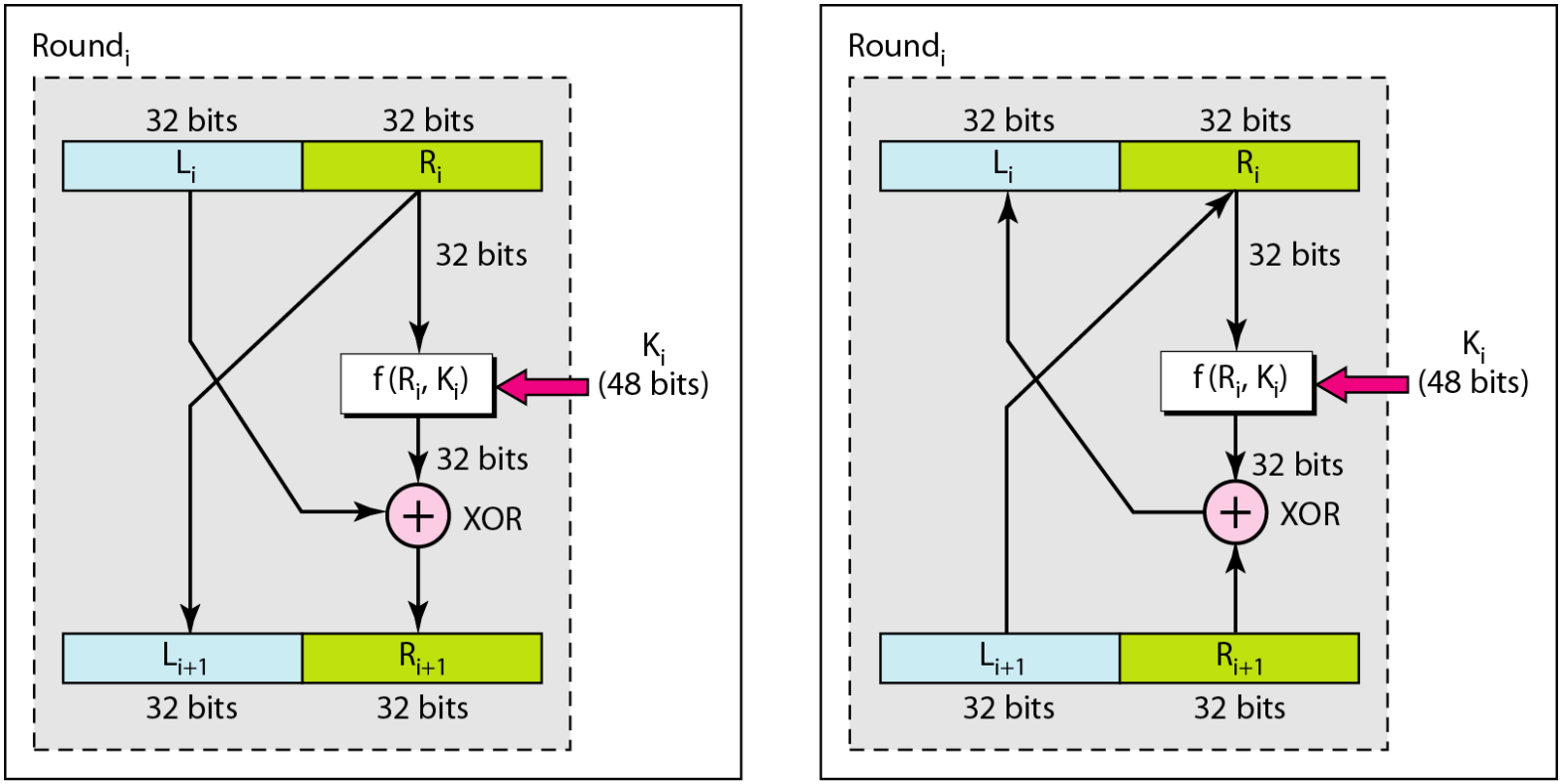


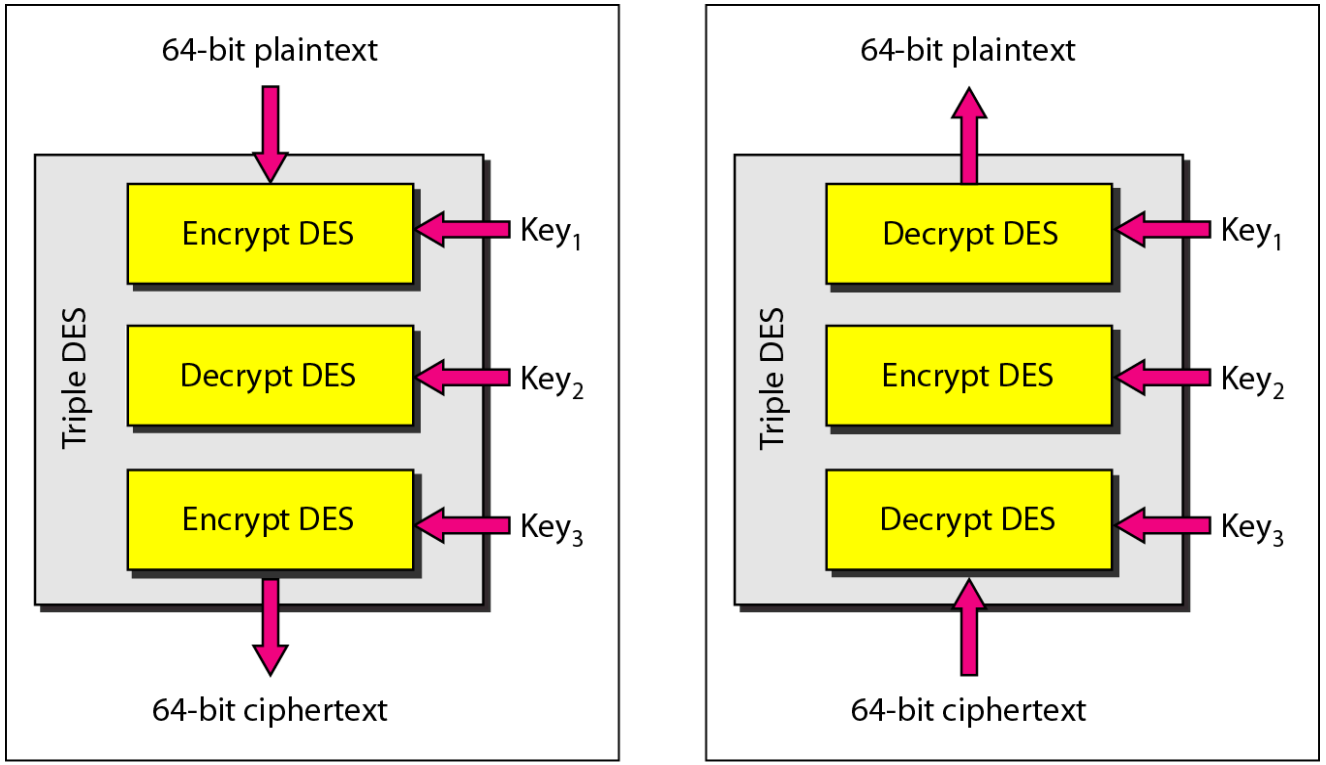
Figure 30.15 *DES function*



a. Encryption round

b. Decryption round

Figure 30.16 *Triple DES*



a. Encryption Triple DES

b. Decryption Triple DES

Table 30.1 *AES configuration*

Size of Data Block	*Number of Rounds*	*Key Size*
128 bits	10	128 bits
	12	192 bits
	14	256 bits

Note

AES has three different configurations with respect to the number of rounds and key size.

Figure 30.17 *AES*

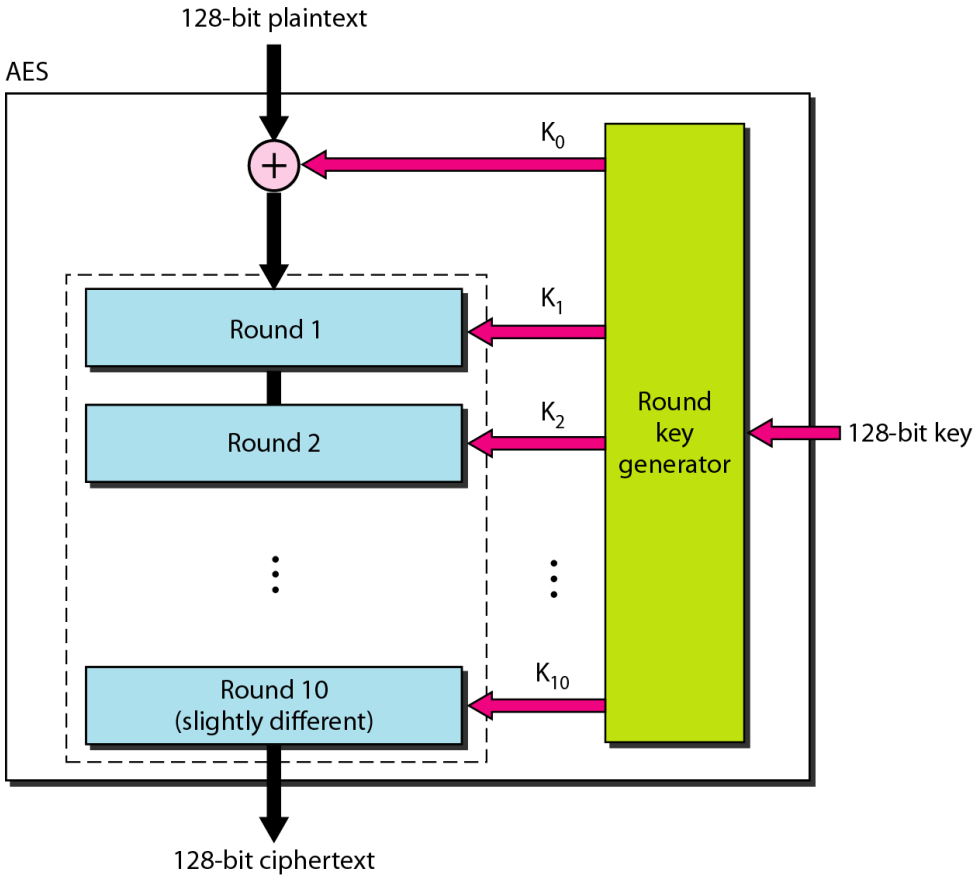


Figure 30.18 *Structure of each round*

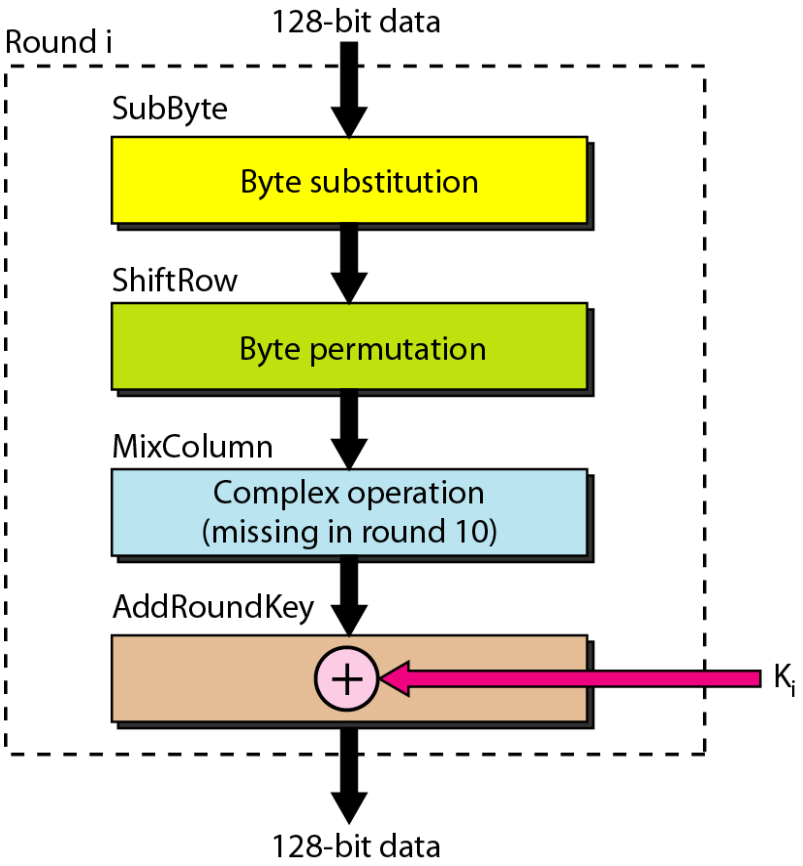


Figure 30.19 *Modes of operation for block ciphers*

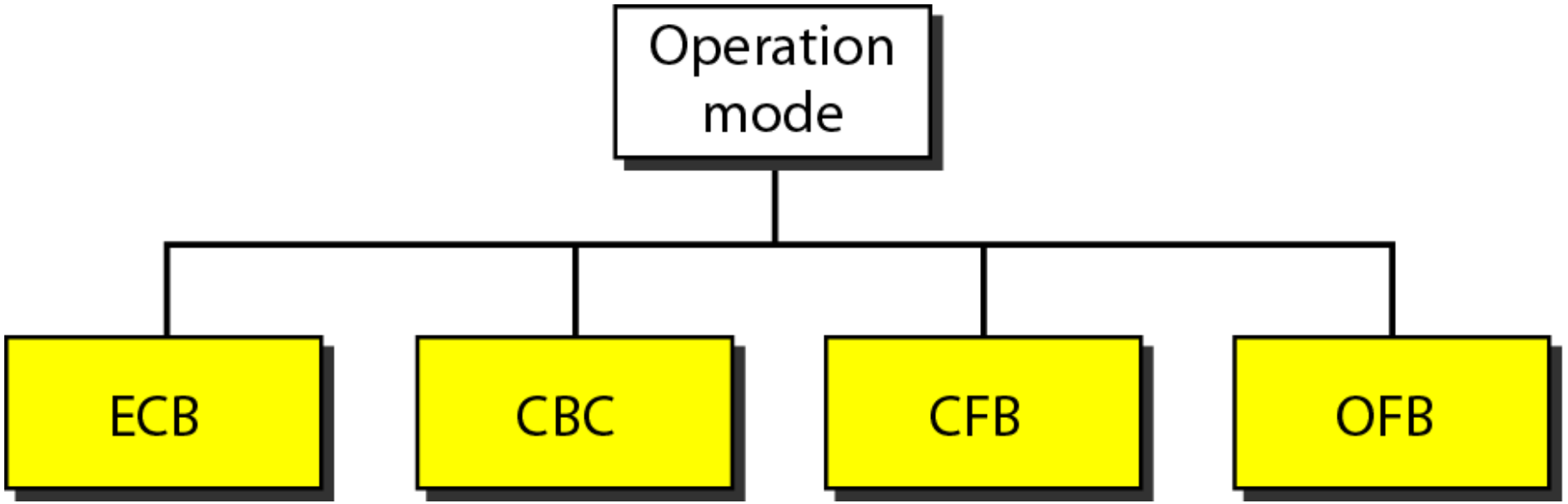


Figure 30.20 *ECB mode*

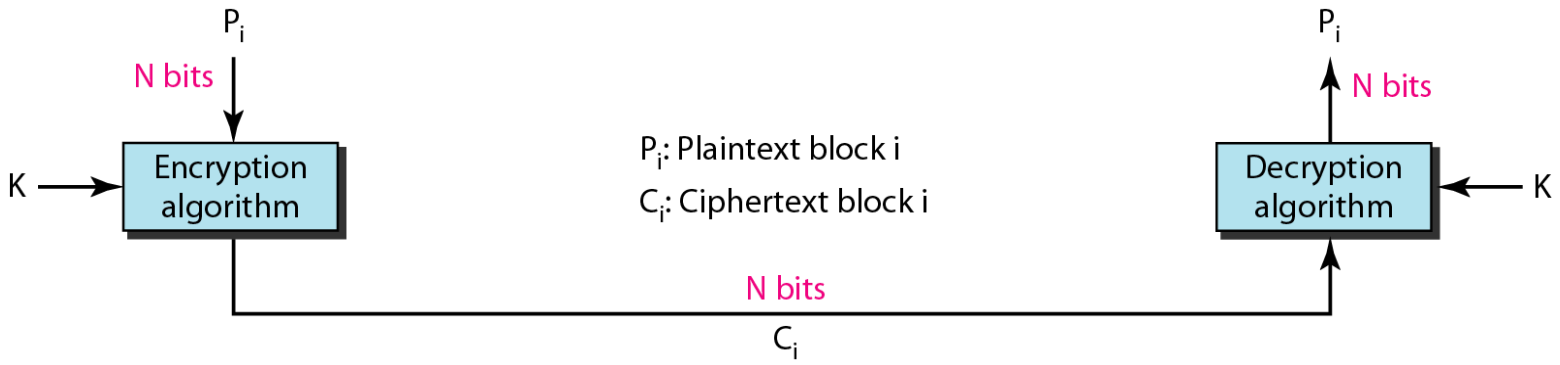


Figure 30.21 *CBC mode*

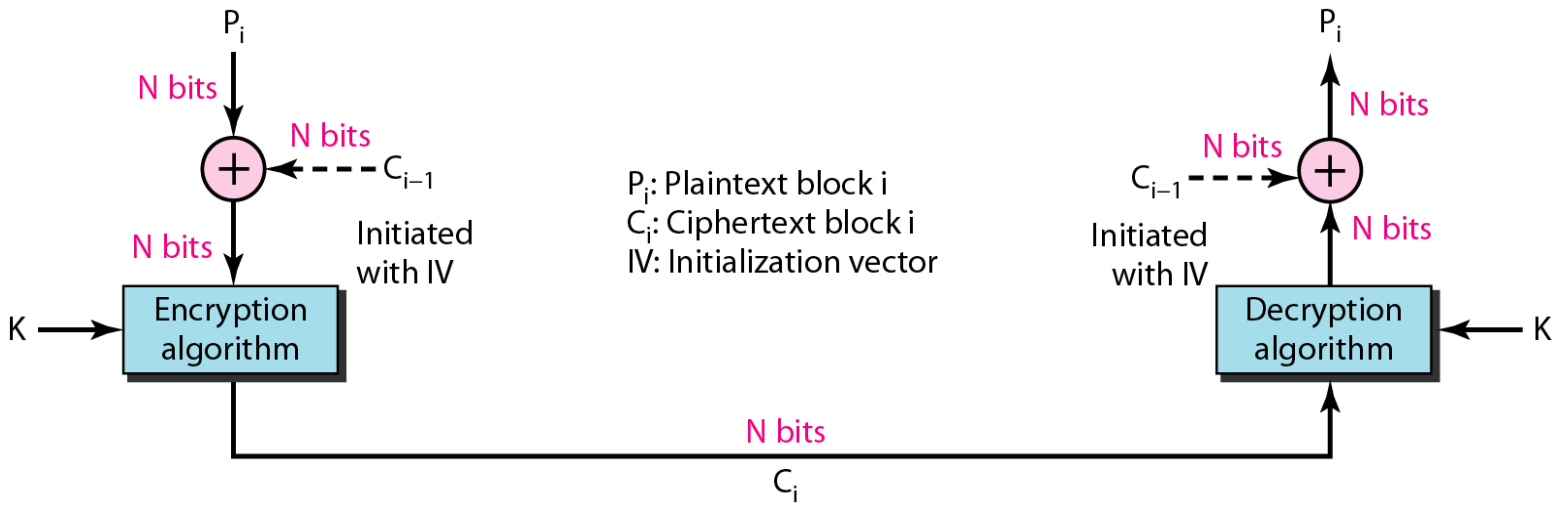


Figure 30.22 *CFB mode*

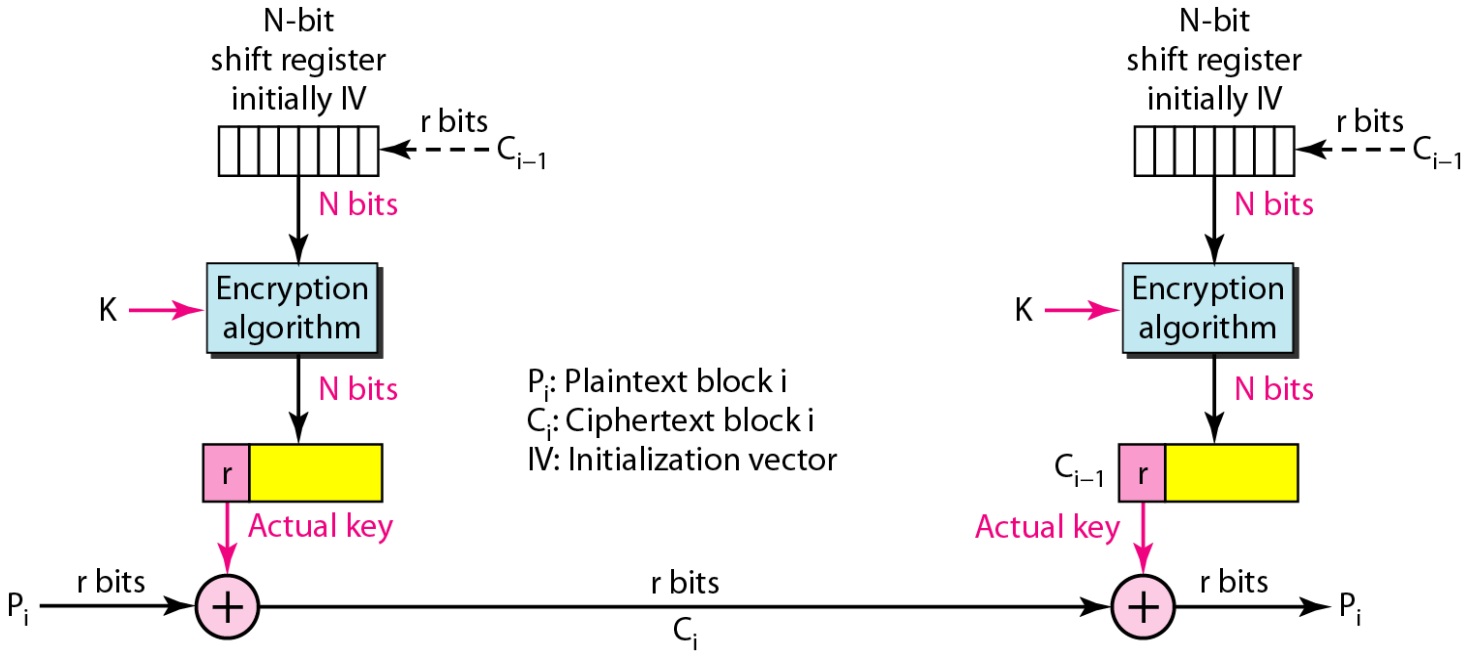
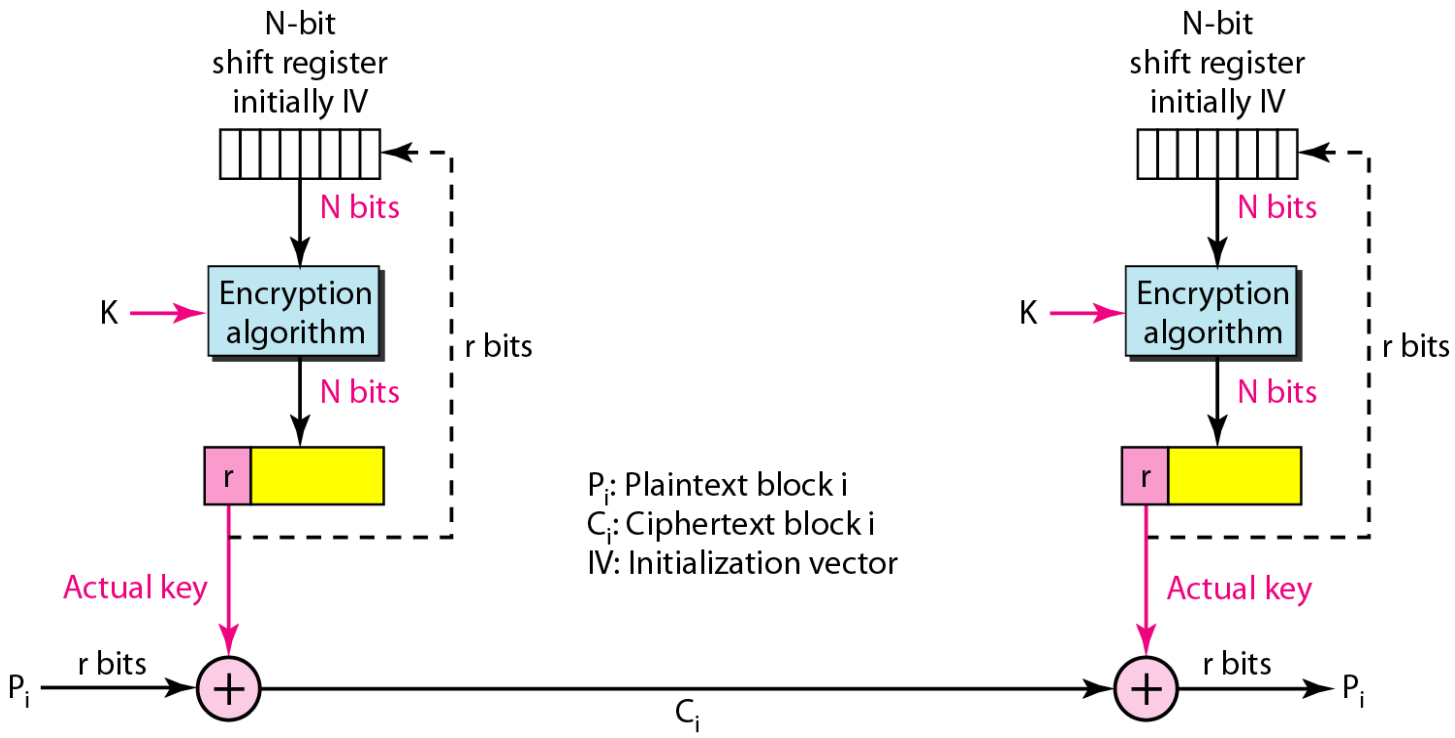


Figure 30.23 *OFB mode*



30-3 ASYMMETRIC-KEY CRYPTOGRAPHY

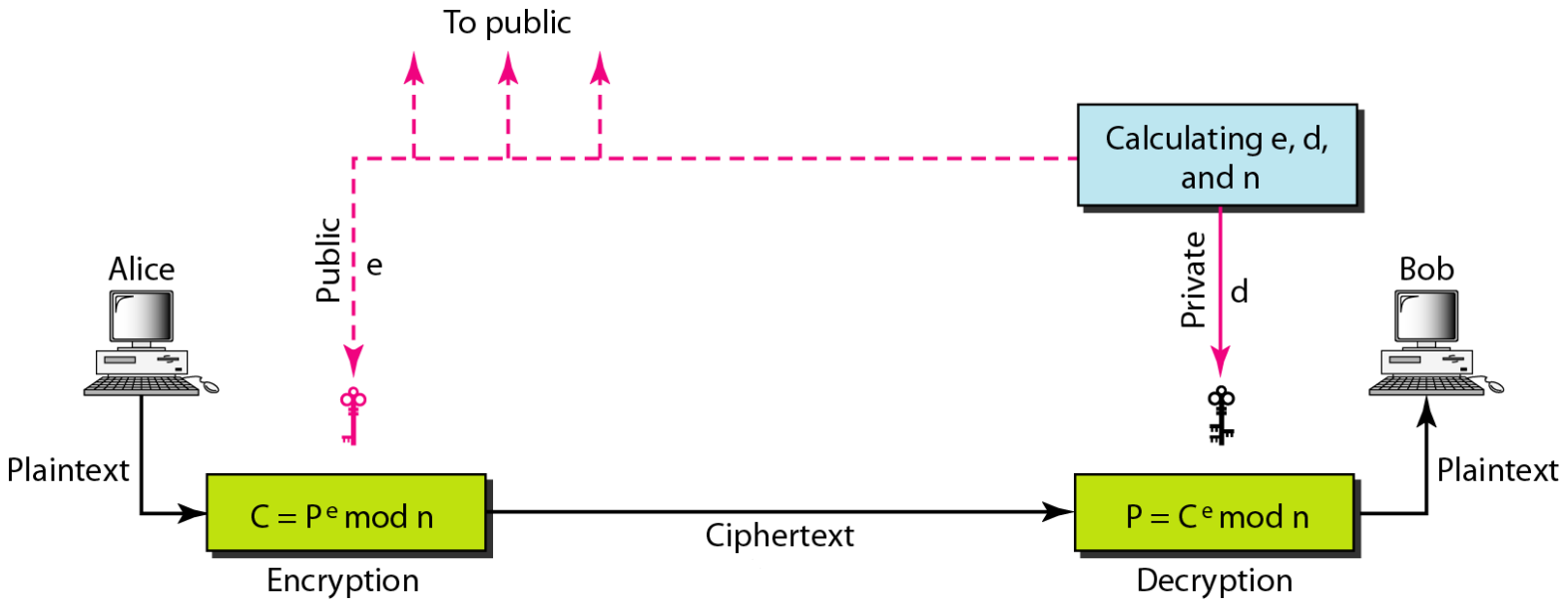
An asymmetric-key (or public-key) cipher uses two keys: one private and one public. We discuss two algorithms: RSA and Diffie-Hellman.

Topics discussed in this section:

RSA

Diffie-Hellman

Figure 30.24 *RSA*



Note

In RSA, *e* and *n* are announced to the public; *d* and Φ are kept secret.

Example 30.7

Bob chooses 7 and 11 as p and q and calculates $n = 7 \cdot 11 = 77$. The value of $\Phi = (7 - 1)\ (11 - 1)$ or 60. Now he chooses two keys, e and d. If he chooses e to be 13, then d is 37. Now imagine Alice sends the plaintext 5 to Bob. She uses the public key 13 to encrypt 5.

Plaintext: 5

$C = 5^{13} = 26 \bmod 77$

Ciphertext: 26

Example 30.7 (continued)

Bob receives the ciphertext 26 and uses the private key 37 to decipher the ciphertext:

Ciphertext: 26

$P = 26^{37} = 5 \bmod 77$

Plaintext: 5

The plaintext 5 sent by Alice is received as plaintext 5 by Bob.

Example 30.8

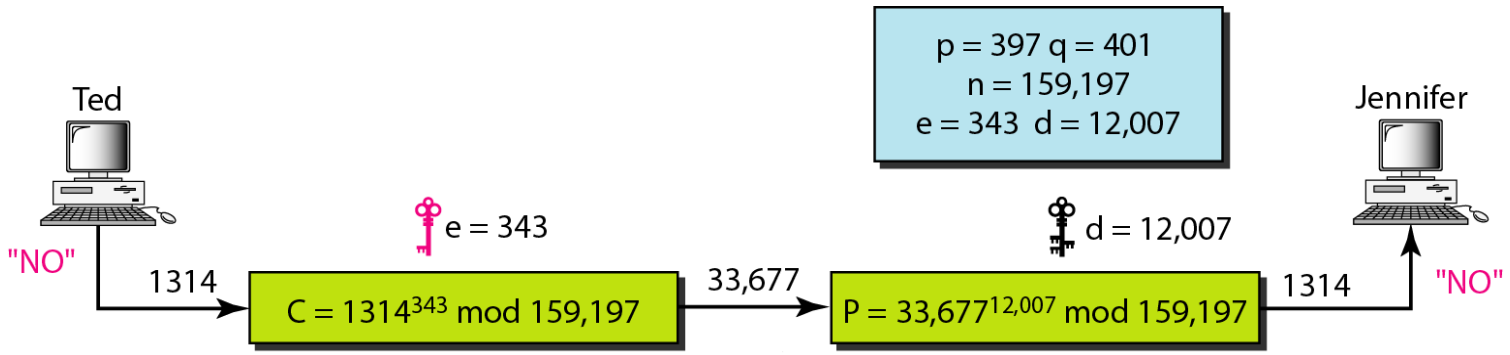
Jennifer creates a pair of keys for herself. She chooses p = 397 and q = 401. She calculates n = 159,197 and Φ = 396 · 400 = 158,400. She then chooses e = 343 and d = 12,007. Show how Ted can send a message to Jennifer if he knows e and n.

Example 30.8 (continuted)

Solution

Suppose Ted wants to send the message "NO" to Jennifer. He changes each character to a number (from 00 to 25) with each character coded as two digits. He then concatenates the two coded characters and gets a four-digit number. The plaintext is 1314. Ted then uses e and n to encrypt the message. The ciphertext is $1314^{343} = 33{,}677 \bmod 159{,}197$. *Jennifer receives the message 33,677 and uses the decryption key d to decipher it as* $33{,}677^{12{,}007} = 1314 \bmod 159{,}197$. *Jennifer then decodes 1314 as the message "NO". Figure 30.25 shows the process.*

Figure 30.25 *Example 30.8*



Example 30.9

Let us give a realistic example. We randomly chose an integer of 512 bits. The integer p is a 159-digit number.

p = 96130345313583504574191581280615427909309845594996215822583150879647940
45505647063849125716018034750312098666606492420191808780667421096063354
219926661209

The integer q is a 160-digit number.

q = 12060191957231446918276794204450896001555925054637033936061798321731482
14848376465921538945320917522527322683010712069560460251388714552496900
0359660045617

Example 30.9 (continued)

We calculate n. It has 309 digits:

$$n = 115935041739676149688925098646158875237714573754541447754855261376147885408326350817276878815968325168468849300625485764111250162414552339182927162507656772727460097082714127730434960500556347274566628060099924037102991424472292215772798531727033839381334692684137327622000966676671831831088373420823444370953$$

We calculate Φ. It has 309 digits:

$$\phi = 115935041739676149688925098646158875237714573754541447754855261376147885408326350817276878815968325168468849300625485764111250162414552339182927162507656751054233608492916752034482627988117554787657013923444405716989581728196098226361075467211864612171359107358640614008885170265377277264467341066243857664128$$

Example 30.9 (continued)

We choose e = 35,535. We then find d.

e = 35535

d = 58008302860037763936093661289677917594669062089650962180422866111380593852
82235873170628691003002171085904433840217072986908760061153062025249598844
48047568240966247081485817130463240644077704833134010850947385295645071936
77406119732655742423721761767462077637164207600337085333288532144708859551
36670294831

Alice wants to send the message "THIS IS A TEST" which can be changed to a numeric value by using the 00–26 encoding scheme (26 is the space character).

P = 19070818260818260026190418 19

Example 30.9 (continued)

The ciphertext calculated by Alice is $C = P^e$, which is.

$$C = 4753091236462268272063655506105451809423717960704917165232392430544529$$
$$6061319932856661784341835911415119741125200568297979457173603610127821$$
$$8847892741566090480023507190715277185914975188465886321011483541033616$$
$$5789846796838676373376577746562507928052114814184404814184430812773059$$
$$00469287424855916646210865 6$$

Bob can recover the plaintext from the ciphertext by using $P = C^d$, which is

$$P = 190708182608182600261904 1819$$

The recovered plaintext is THIS IS A TEST after decoding.

Note

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

Example 30.10

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 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; $g^{xy} \bmod p = 7^{18} \bmod 23 = 18$.

Figure 30.27 *Diffie-Hellman idea*

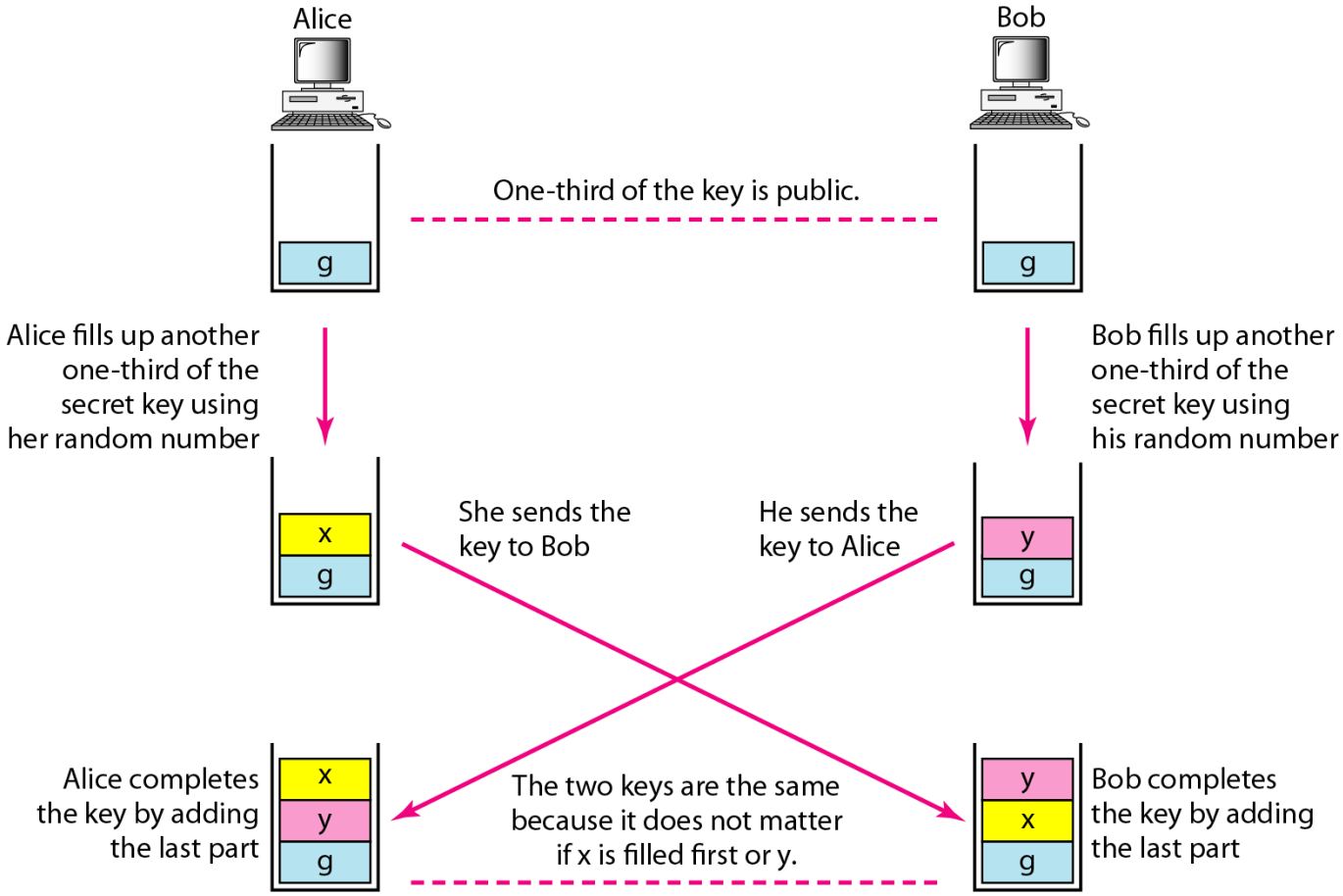


Figure 30.28 *Man-in-the-middle attack*