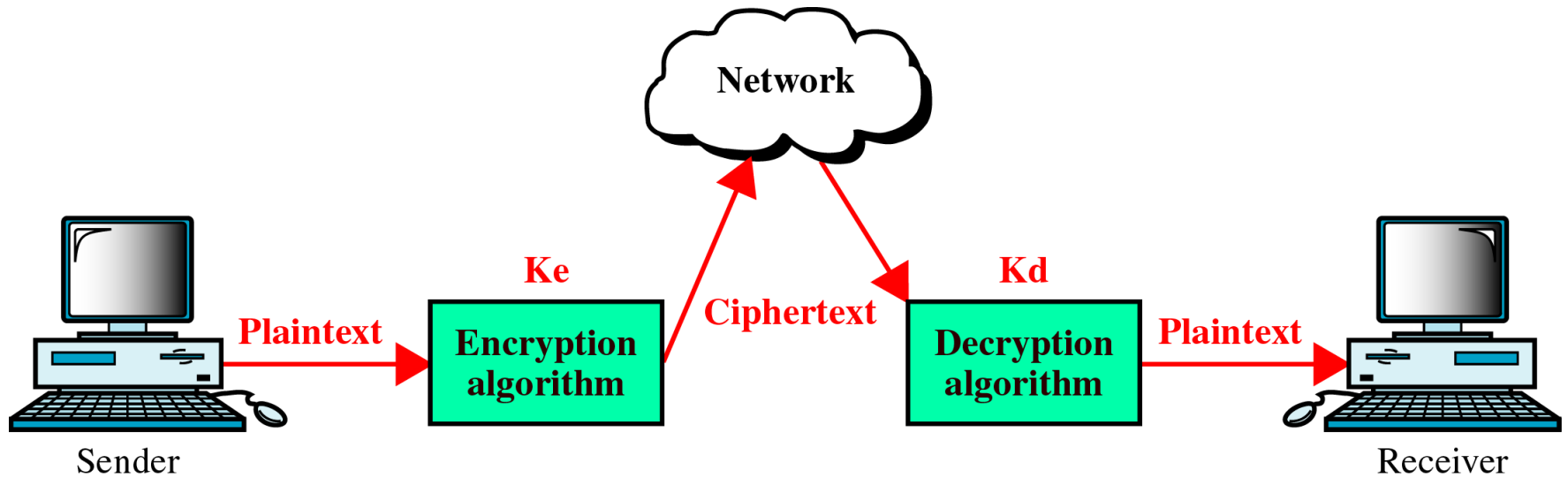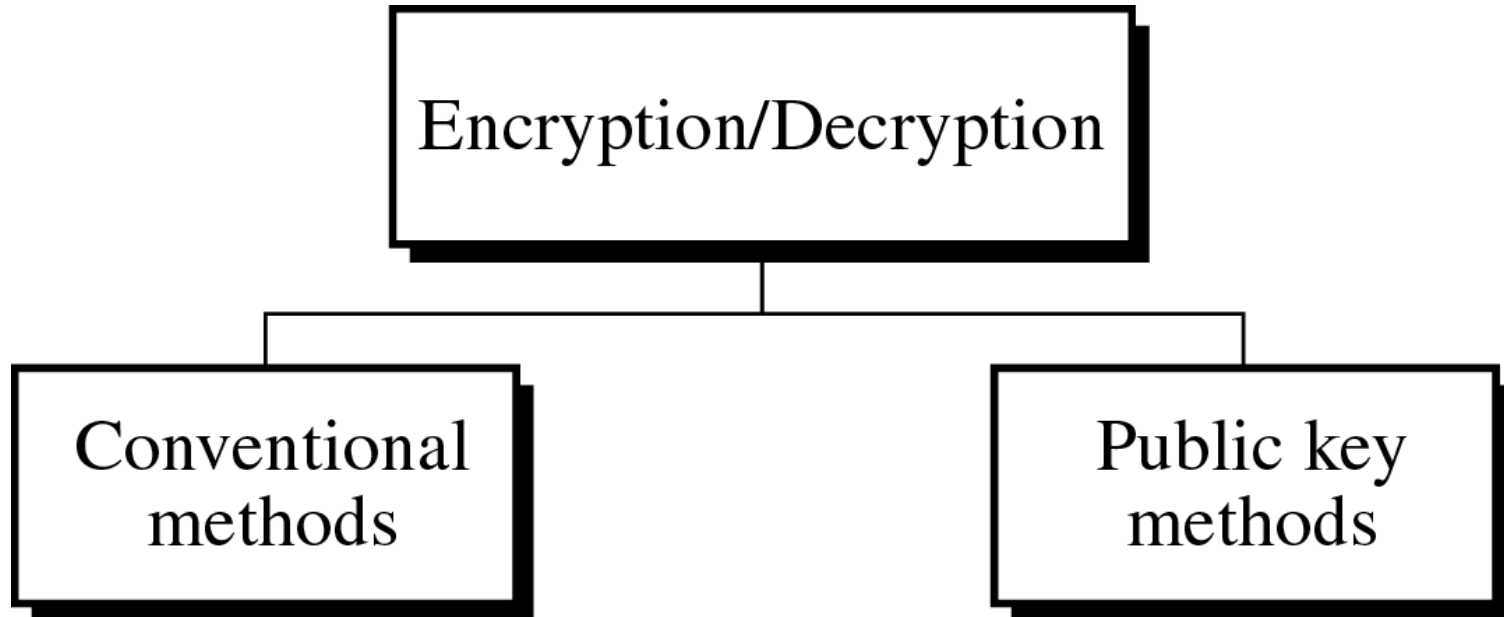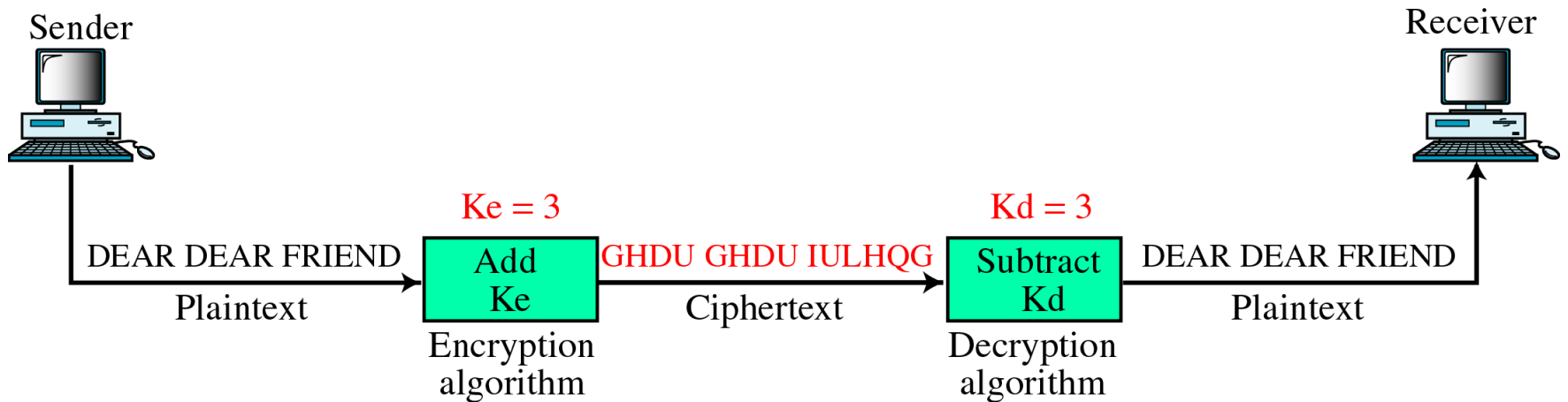# CRYPTOGRAPHY

Encryption and Decryption

Encryption/Decryption Methods

Monoalphabetic Substitution

Polyalphabetic Substitution

Figure 23-11
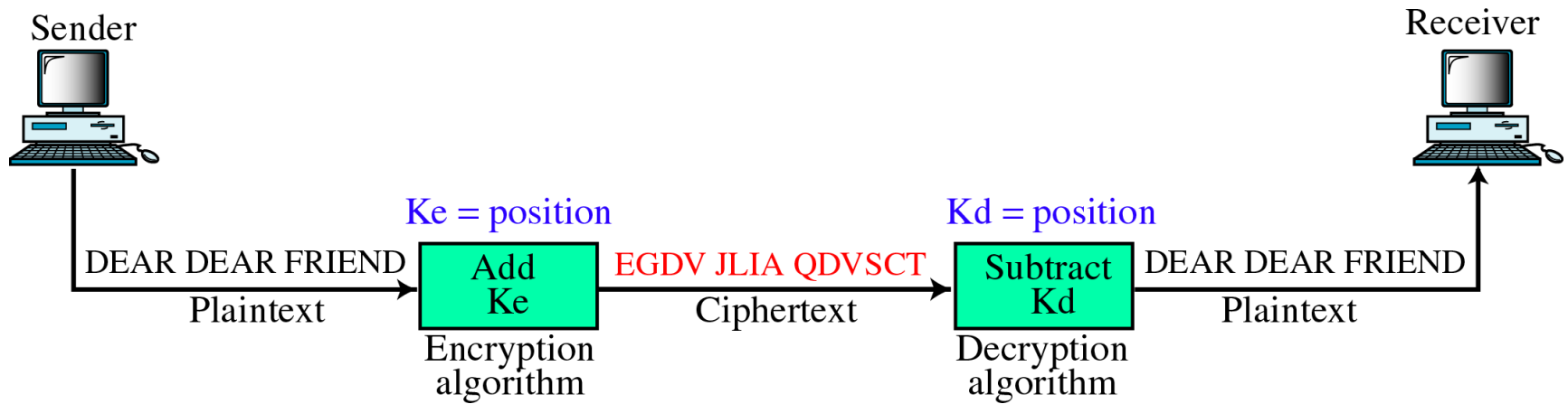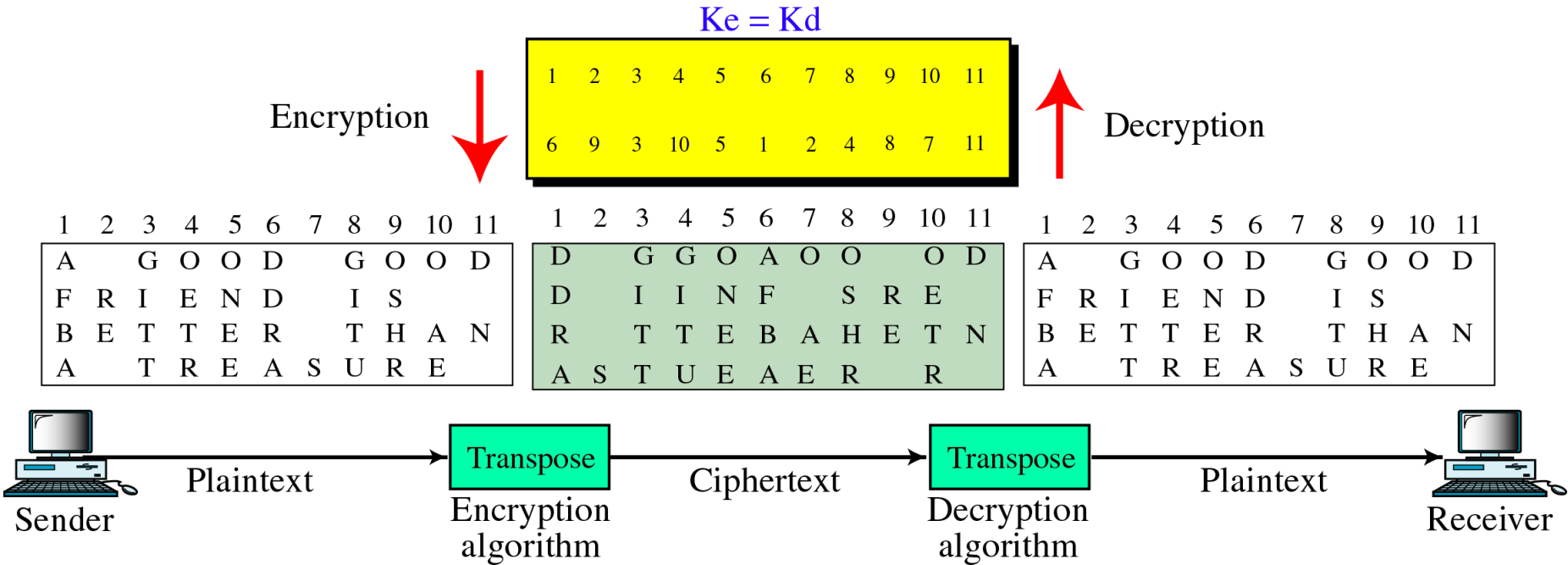
Transpositional Encryption

Ke = Kd

1	2	3	4	5	6	7	8	9	10	11
6	9	3	10	5	1	2	4	8	7	11

Encryption

Decryption

1	2	3	4	5	6	7	8	9	10	11
A	G	O	O	D		G	O	O	D	
F	R	I	E	N	D		I	S		
B	E	T	T	E	R		T	H	A	N
A		T	R	E	A	S	U	R	E	

1	2	3	4	5	6	7	8	9	10	11
D		G	G	O	A	O	O		O	D
D		I	I	N	F		S	R	E	
R		T	T	E	B	A	H	E	T	N
A	S	T	U	E	A	E	R		R	

1	2	3	4	5	6	7	8	9	10	11
A	G	O	O	D		G	O	O	D	
F	R	I	E	N	D		I	S		
B	E	T	T	E	R		T	H	A	N
A		T	R	E	A	S	U	R	E	

Sender — Plaintext → **Transpose** Encryption algorithm — Ciphertext → **Transpose** Decryption algorithm — Plaintext → Receiver
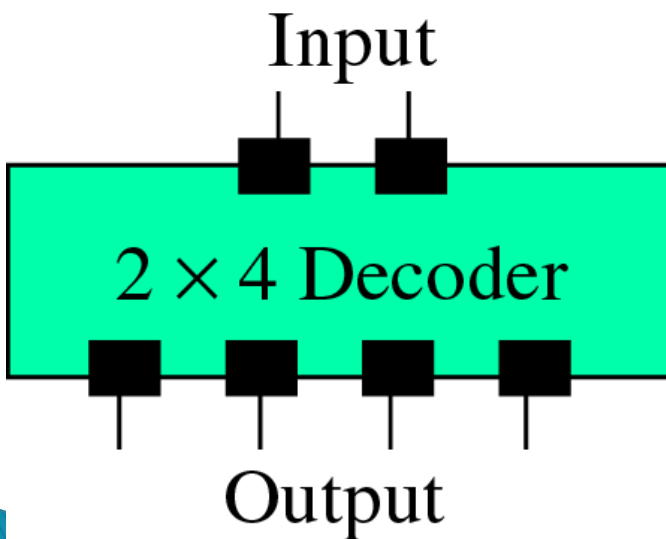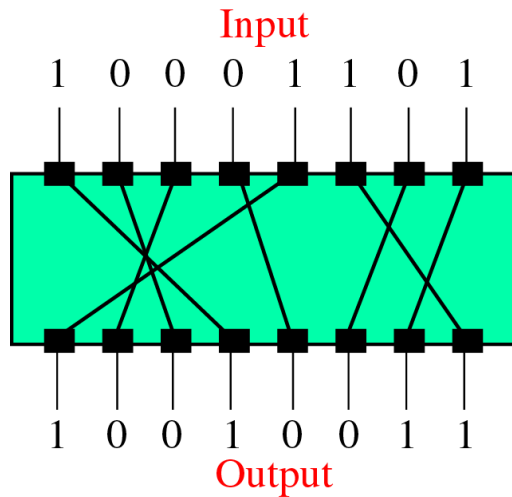
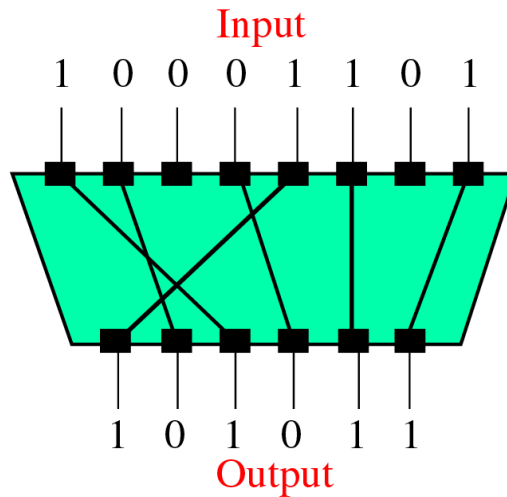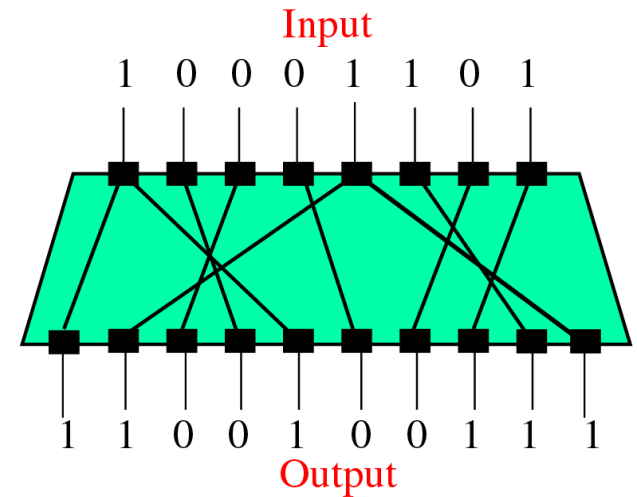**Figure 23-12**

Encoding/Decoding
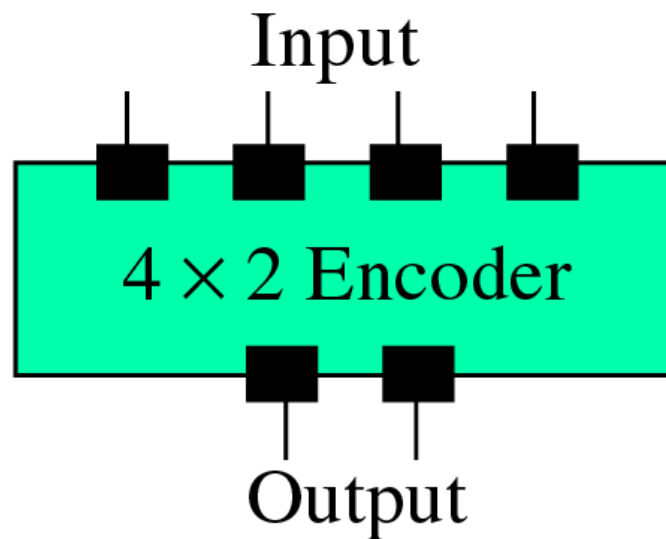
Permutation

a. Straight permutation

b. Compressed permutation

c. Expanded permutation

Figure 23-14

Substitution

Figure 23-15
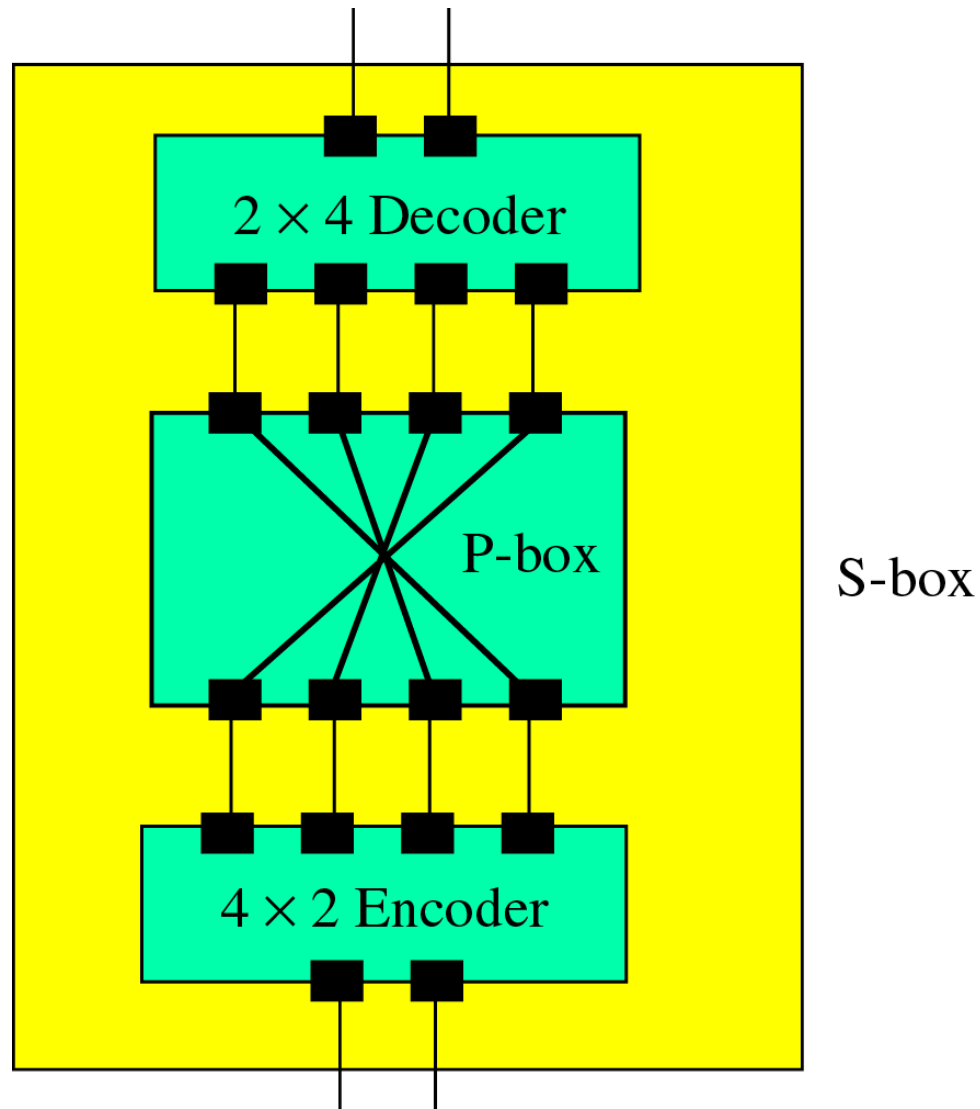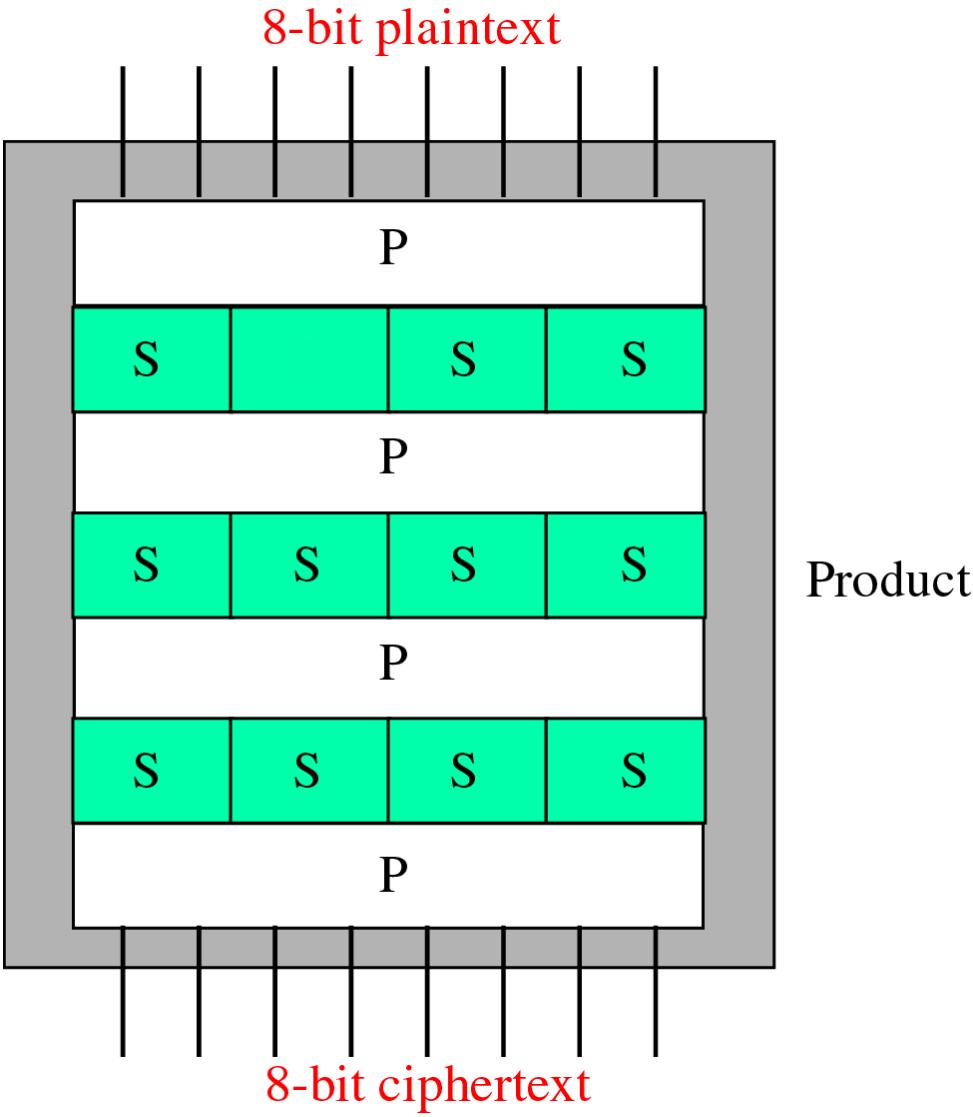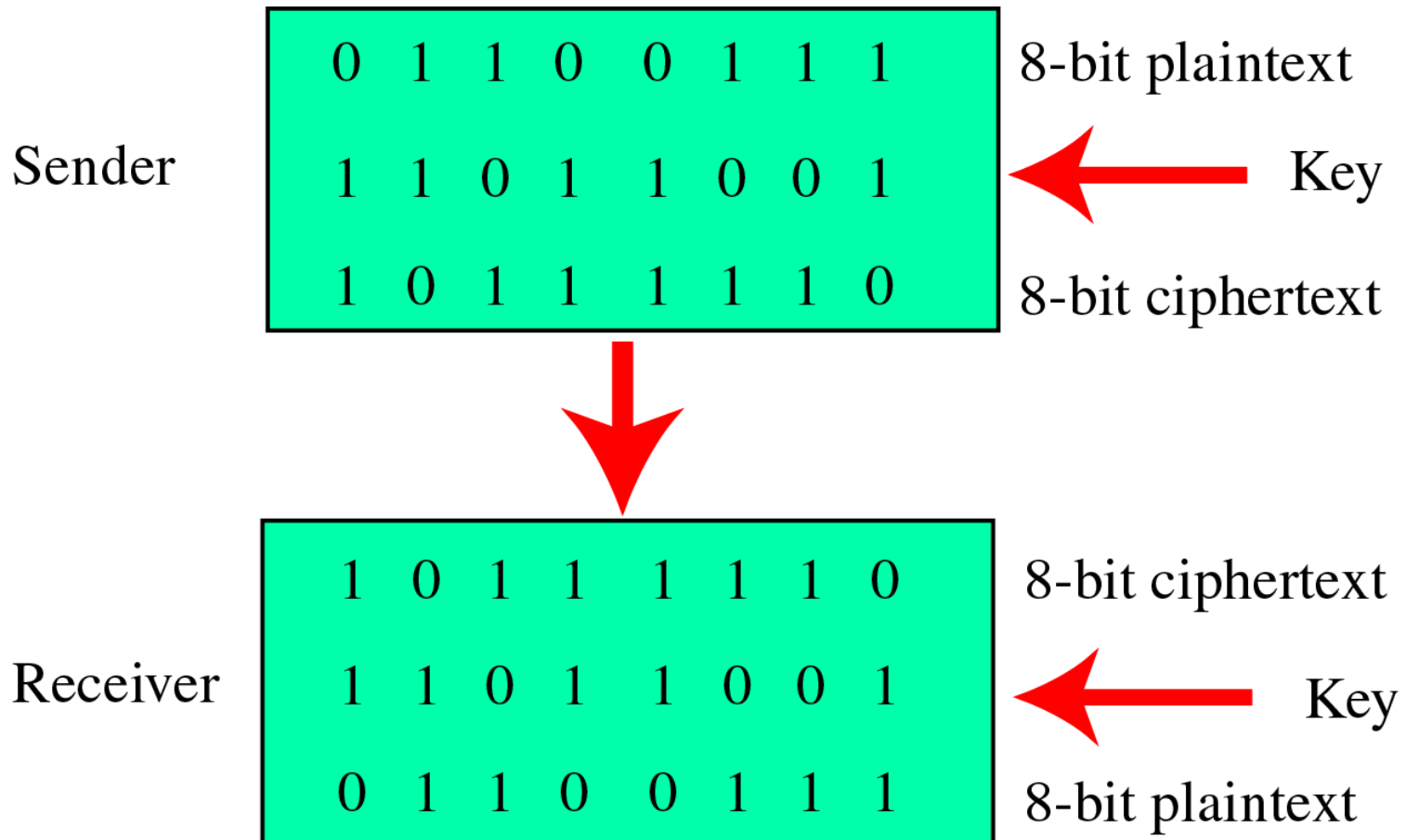
Product

Figure 23-16

Exclusive OR

Figure 23-17

Rotation

Ptext →

| 0 | 1 | 1 | 0 | 0 | 0 | 1 | 1 | Before |

| 1 | 0 | 1 | 1 | 0 | 0 | 0 | 1 | After one rotation |

| 1 | 1 | 0 | 1 | 1 | 0 | 0 | 0 | After two rotations |

Ctext →

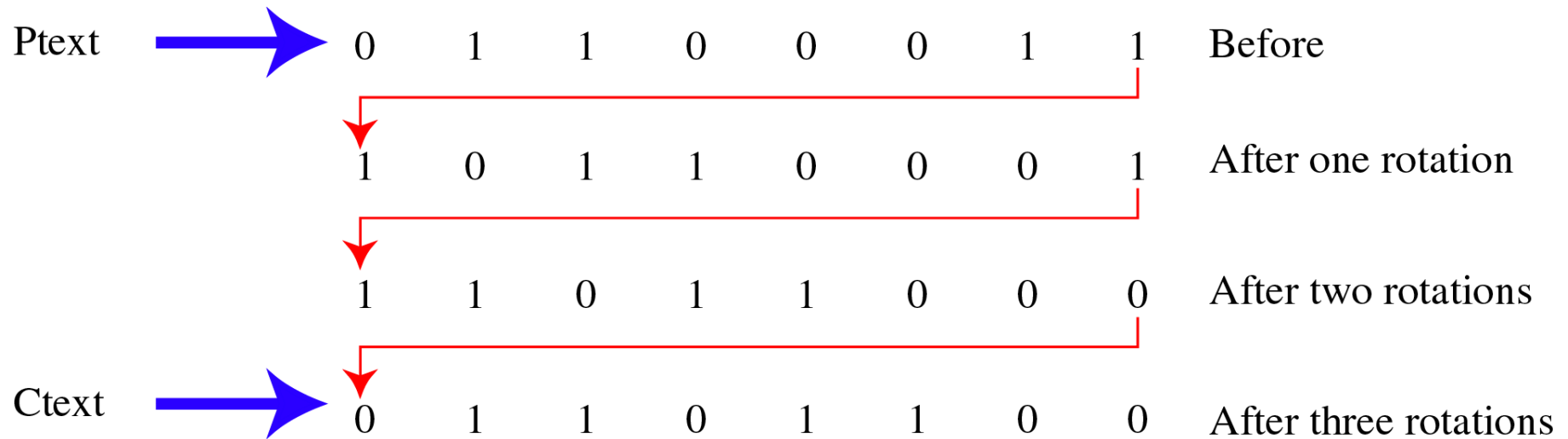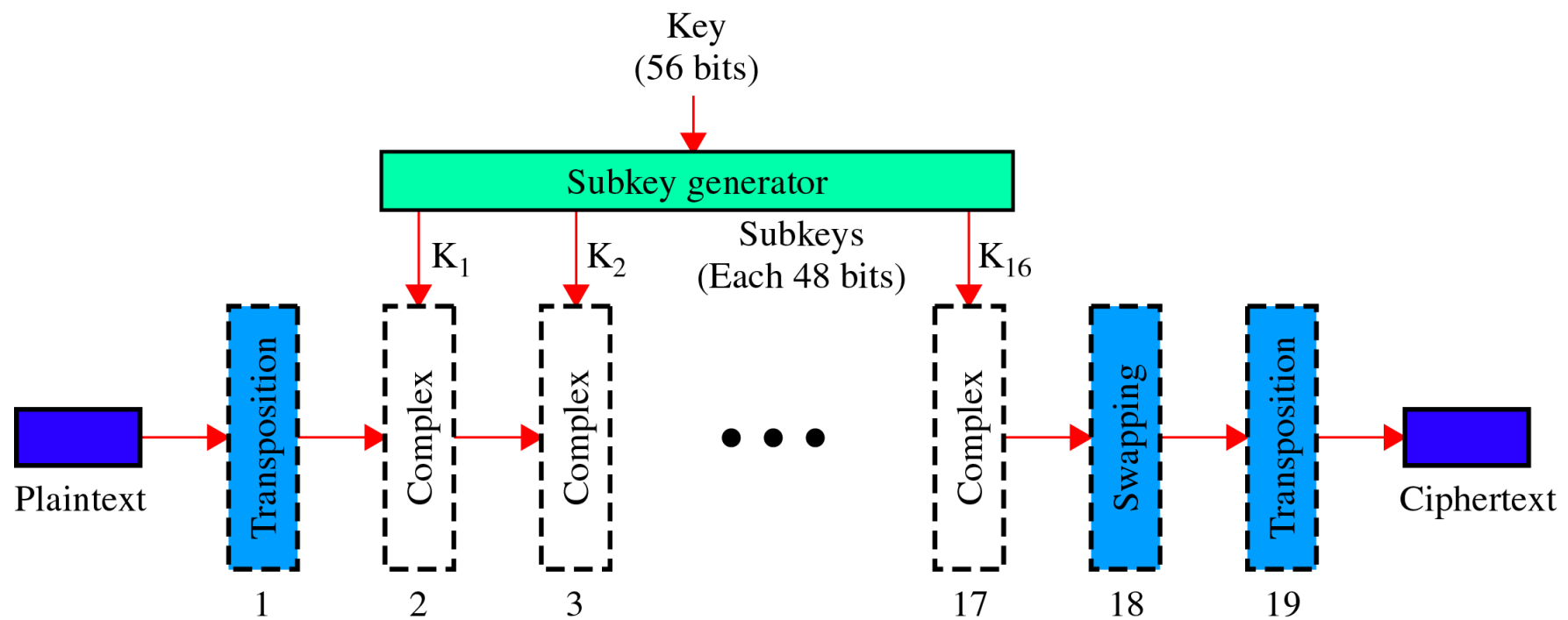| 0 | 1 | 1 | 0 | 1 | 1 | 0 | 0 | After three rotations |

Figure 23-18

DES

Figure 23-19

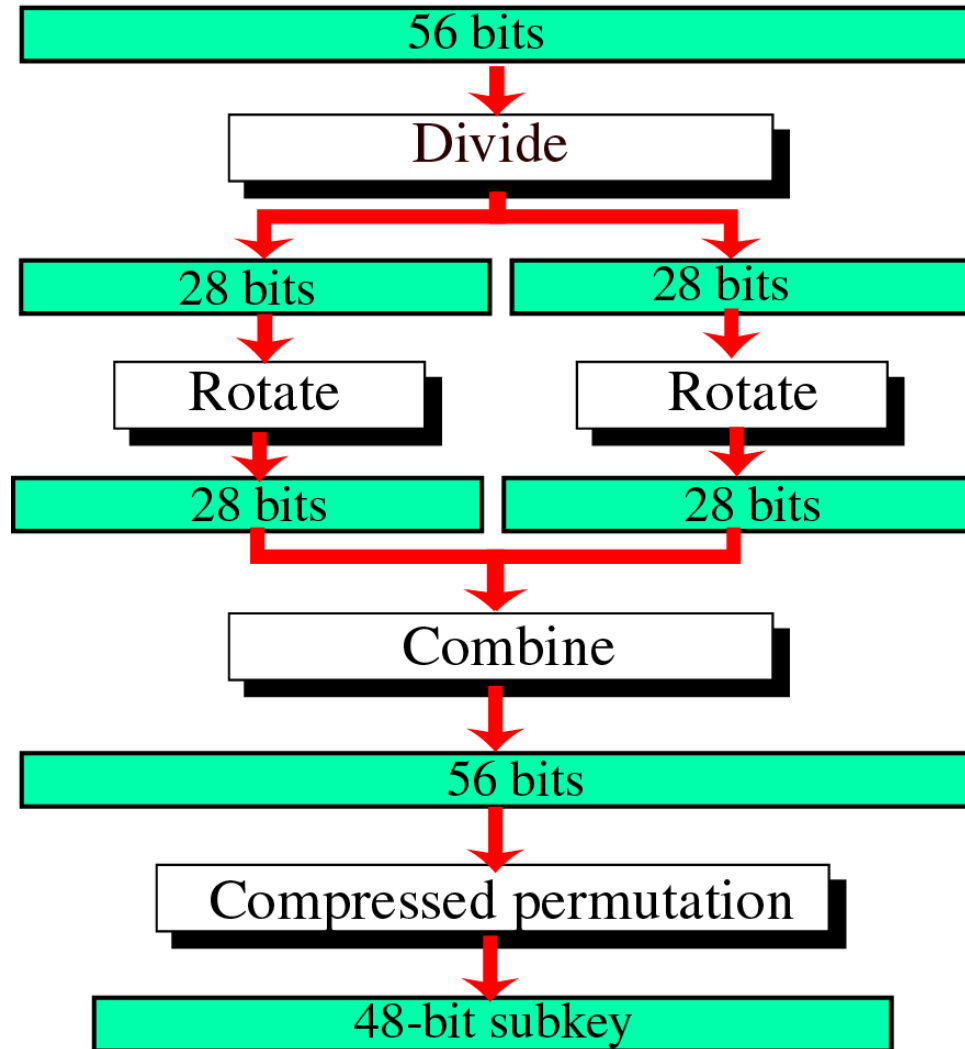# Subkey Generation in DES
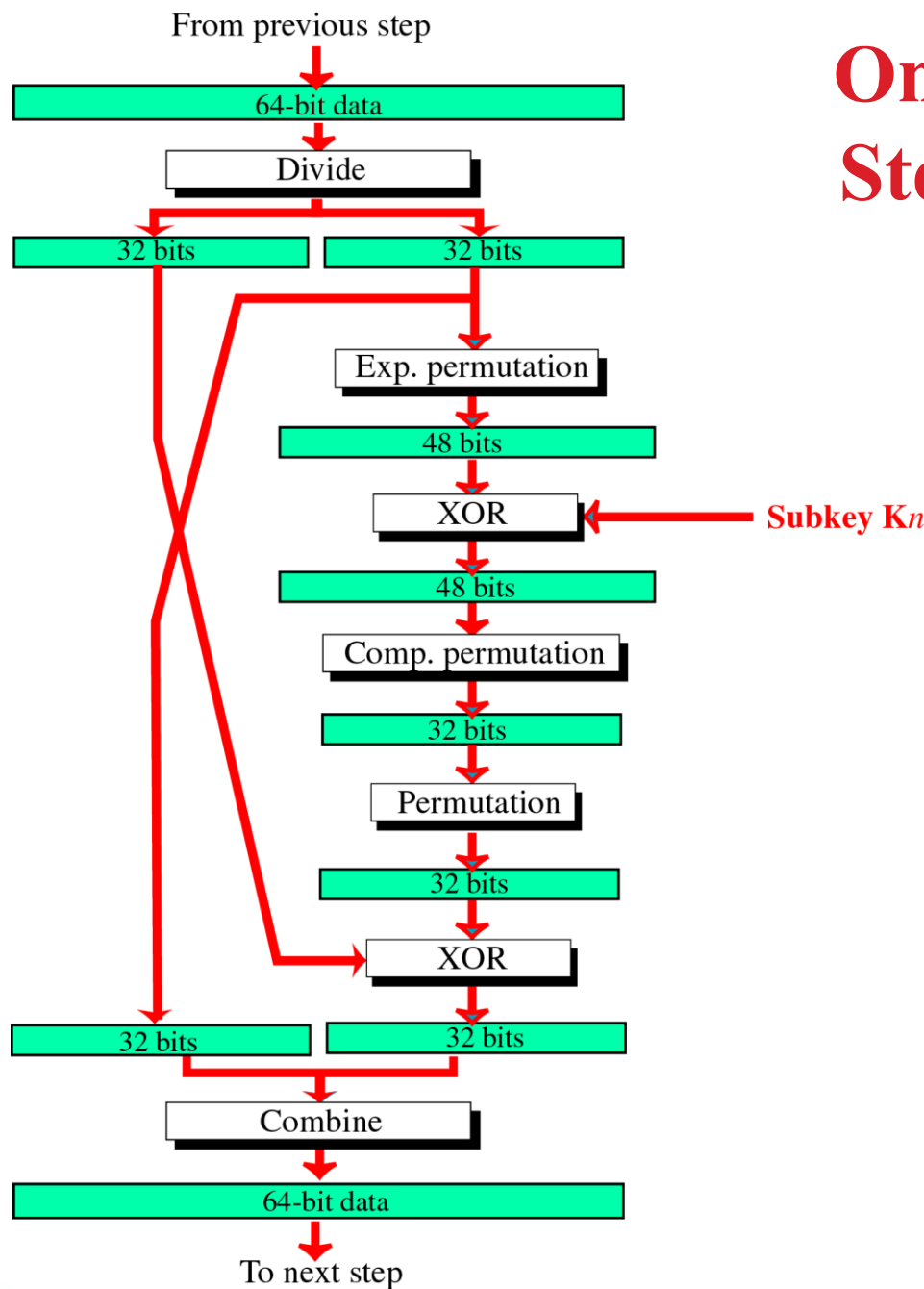
Figure 23-20

One of the 16 Steps in DES

Figure 23-21

Public Key Encryption

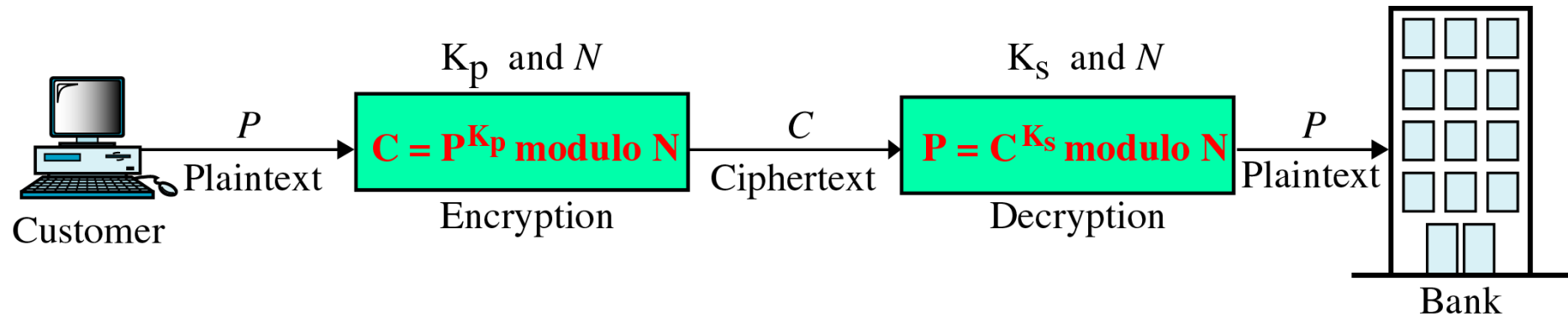**Figure 23-22**

RSA

Customer P Plaintext

K_p and N

$C = P^{K_p} \text{ modulo } N$

Encryption

C Ciphertext

K_s and N

$P = C^{K_s} \text{ modulo } N$

Decryption

P Plaintext

Bank
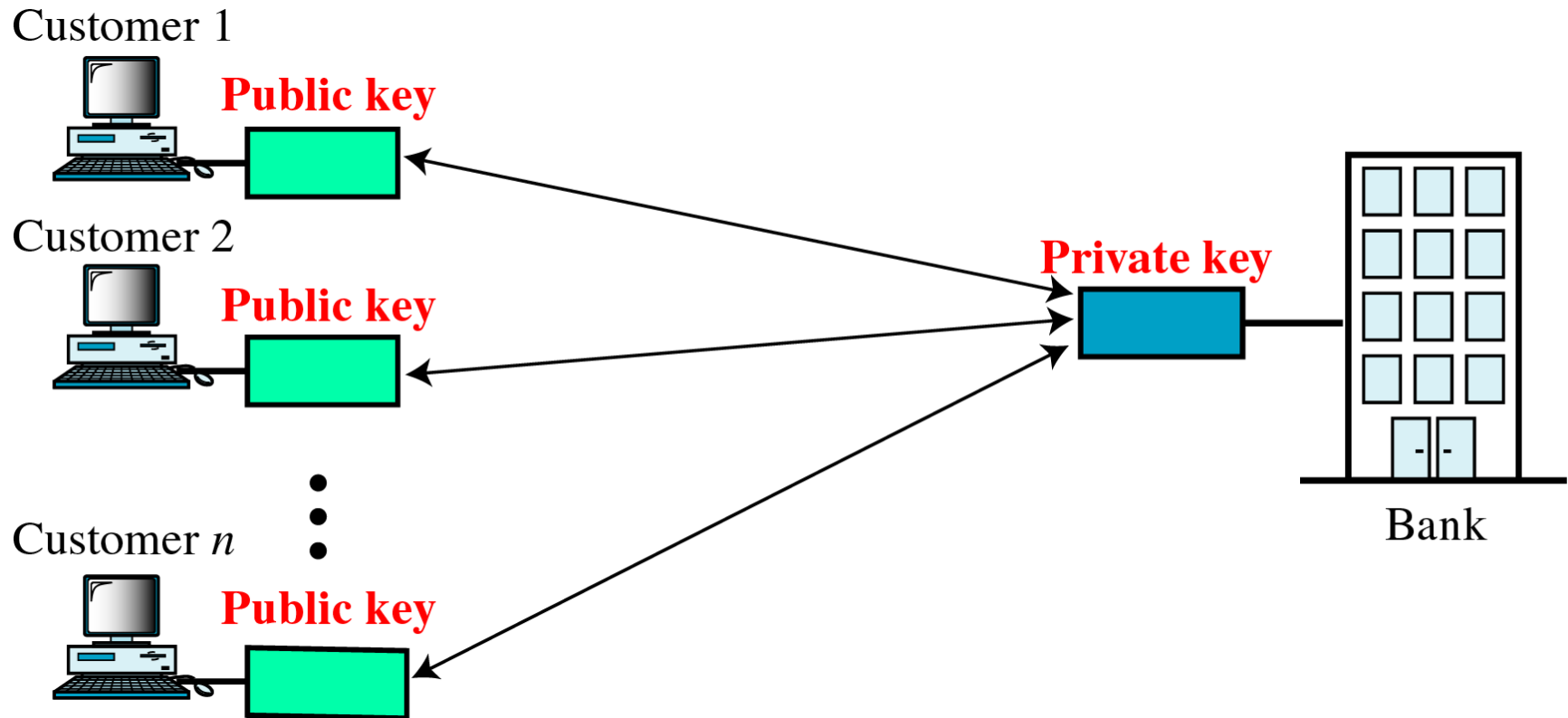
Figure 23-23

RSA Encryption and Decryption

Encryption algorithm using public key

1. Change the character in the plaintext to a number (for example, use 1–26 for A–Z).

2. Raise the number to the power K_p, in this case 5. Divide the result by 119 to get the remainder (modulo division). Send the number as the ciphertext.

Decryption algorithm using secret key

1. Raise the ciphertext (number) to the power K_s, in this case 77. Divide the result by 119 to get the remainder (modulo division).

2. Change the number to the appropriate character.

Customer

F

$F \longrightarrow 6$
$41 = 6^5 \bmod 119$

41

$6 = 41^{77} \bmod 119$
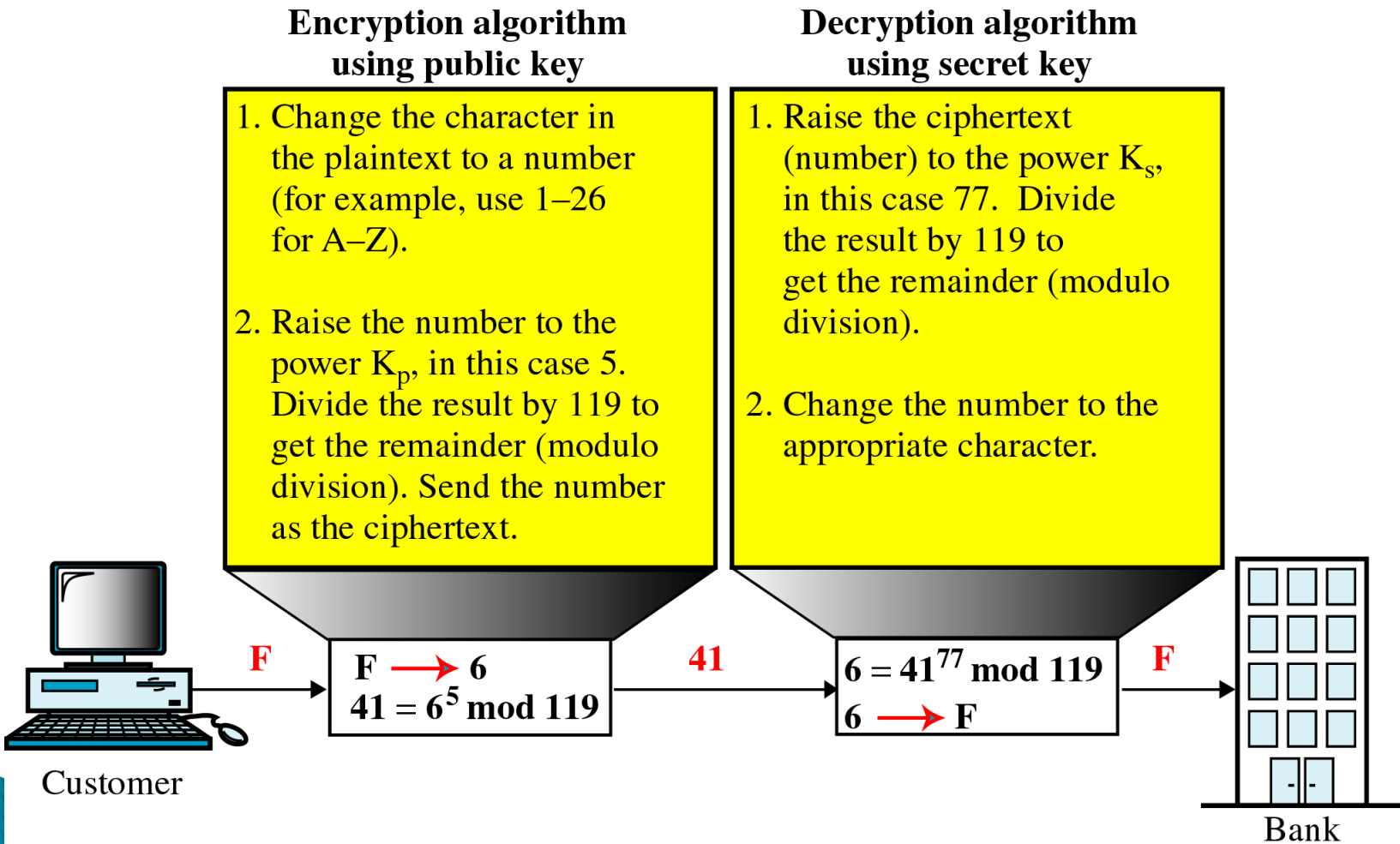$6 \longrightarrow F$

F

Bank

Figure 23-24

Security of RSA
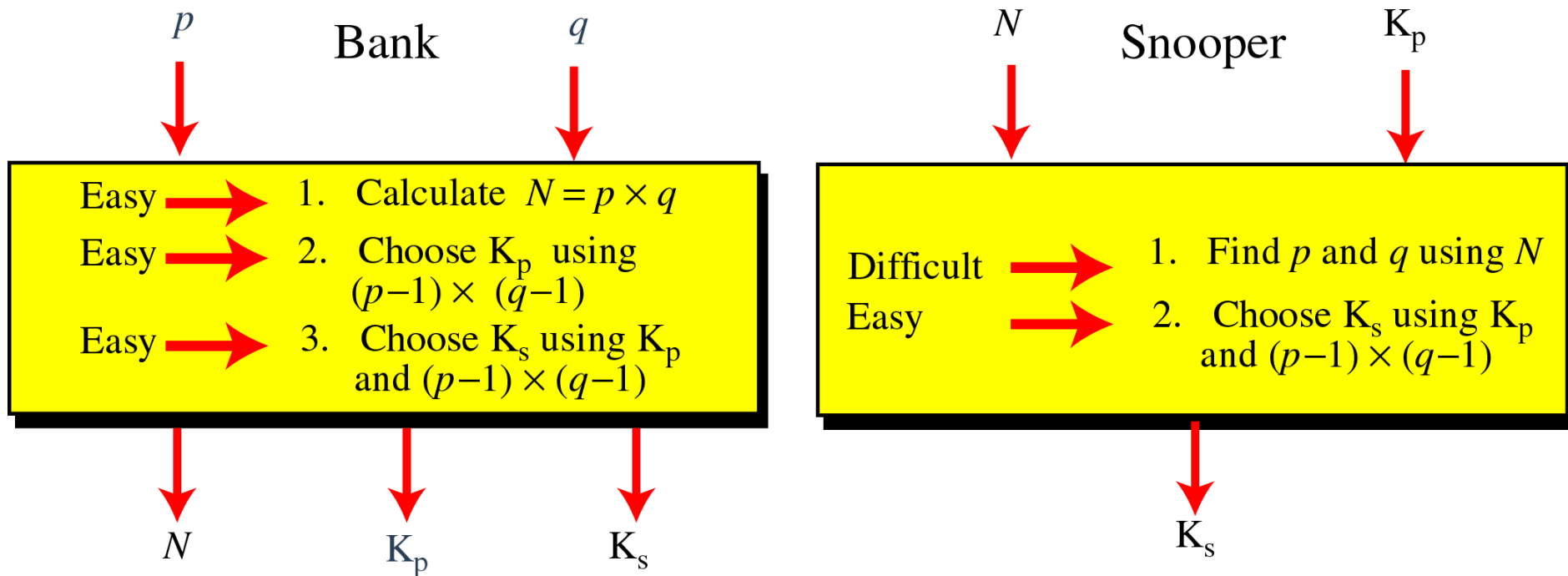
Figure 23-25

Signature Authentication
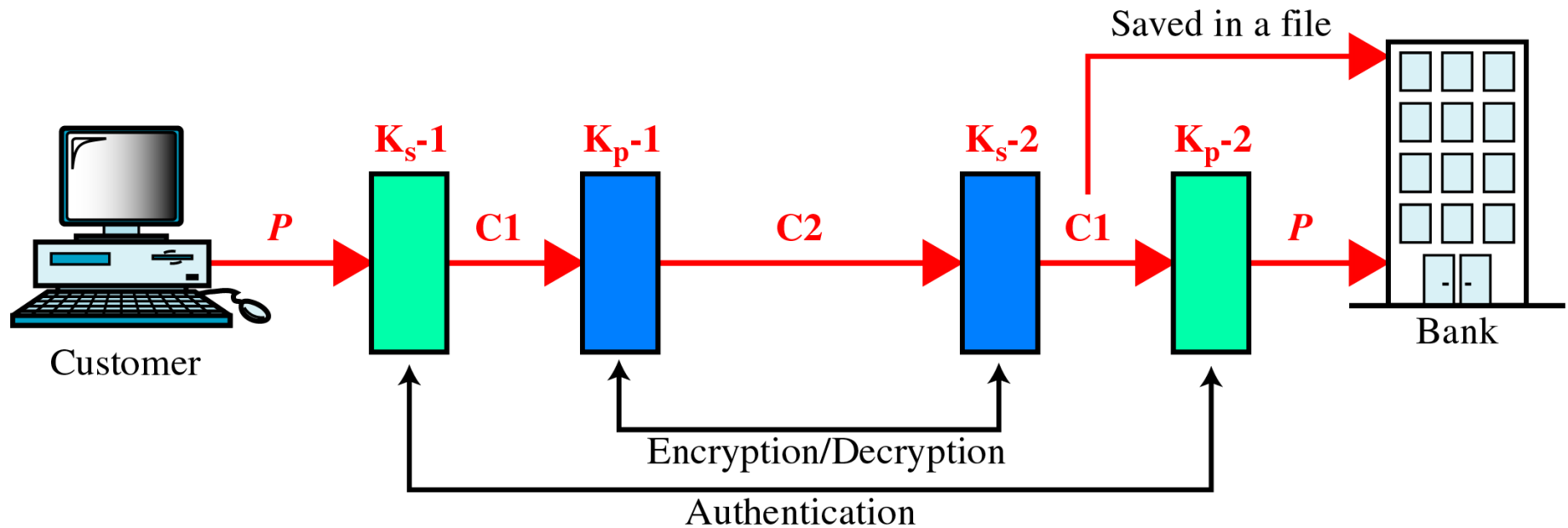
Figure 23-26

Data Compression Methods
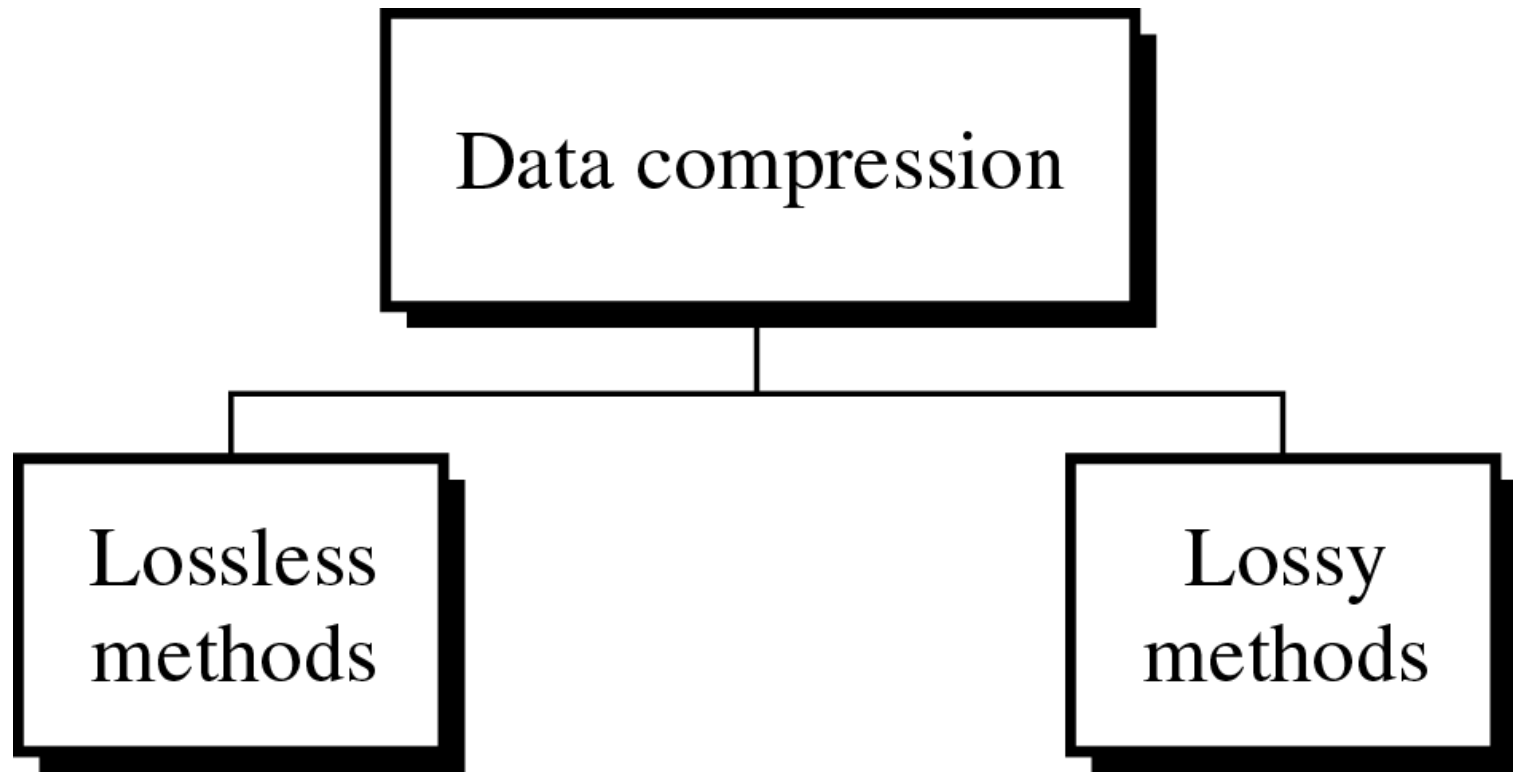
Figure 23-27

Run-Length Encoding

a. Original data

b. Compressed data

Figure 23-28

MHS

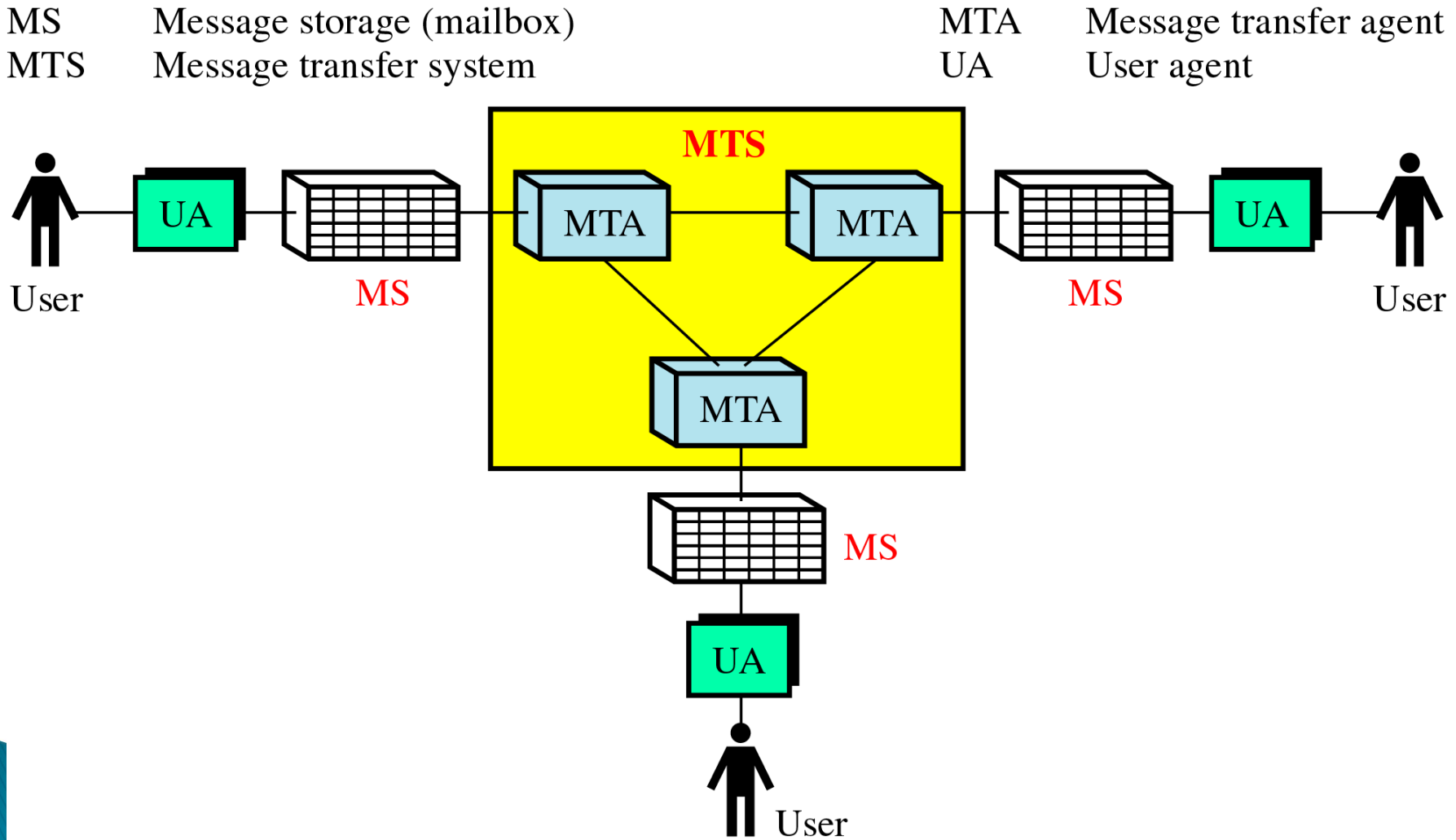|			
MS	Message storage (mailbox)	MTA	Message transfer agent
MTS	Message transfer system	UA	User agent

Figure 23-29

Message Format in MHS
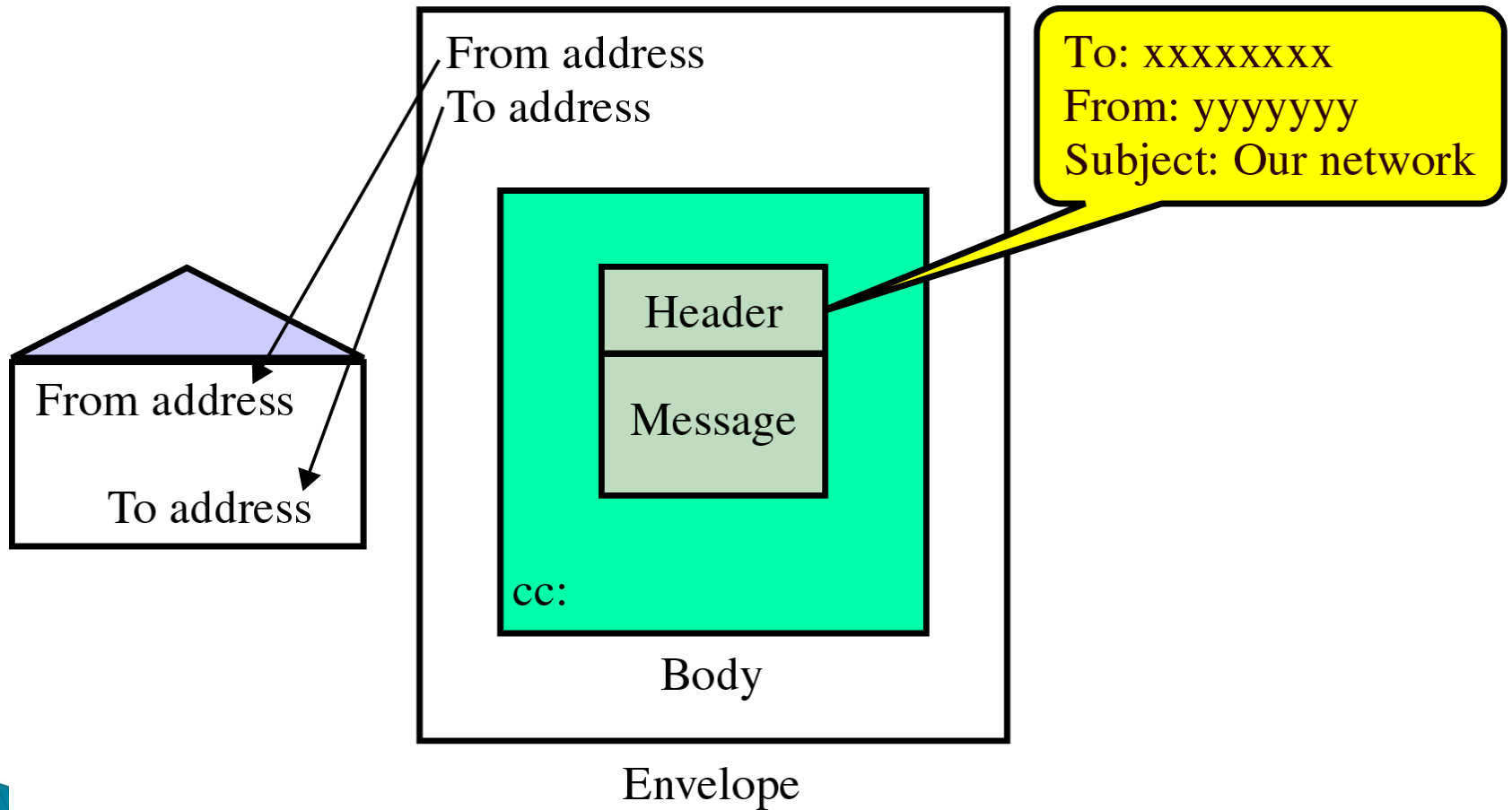
Figure 23-30
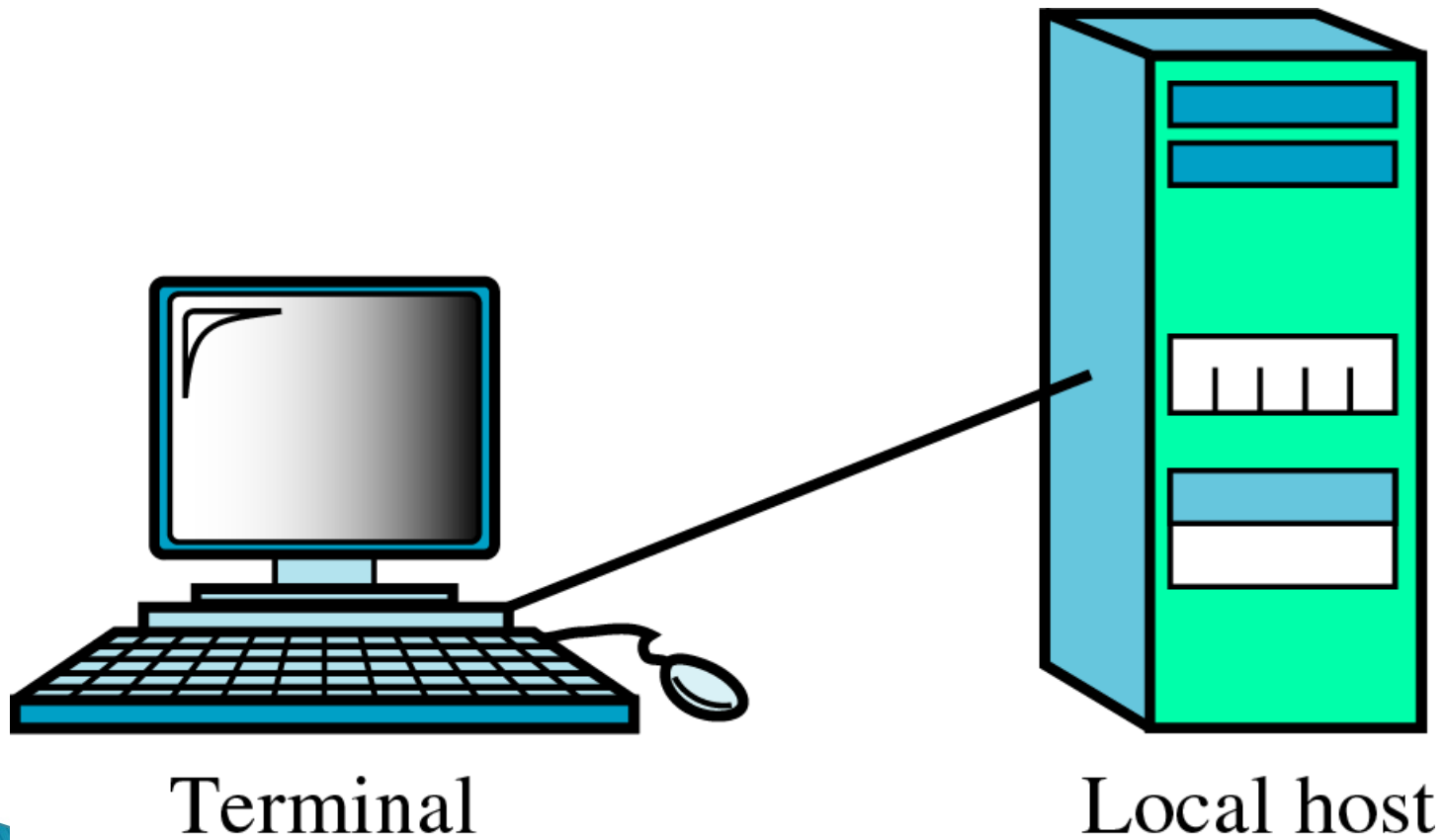
Virtual File Storage
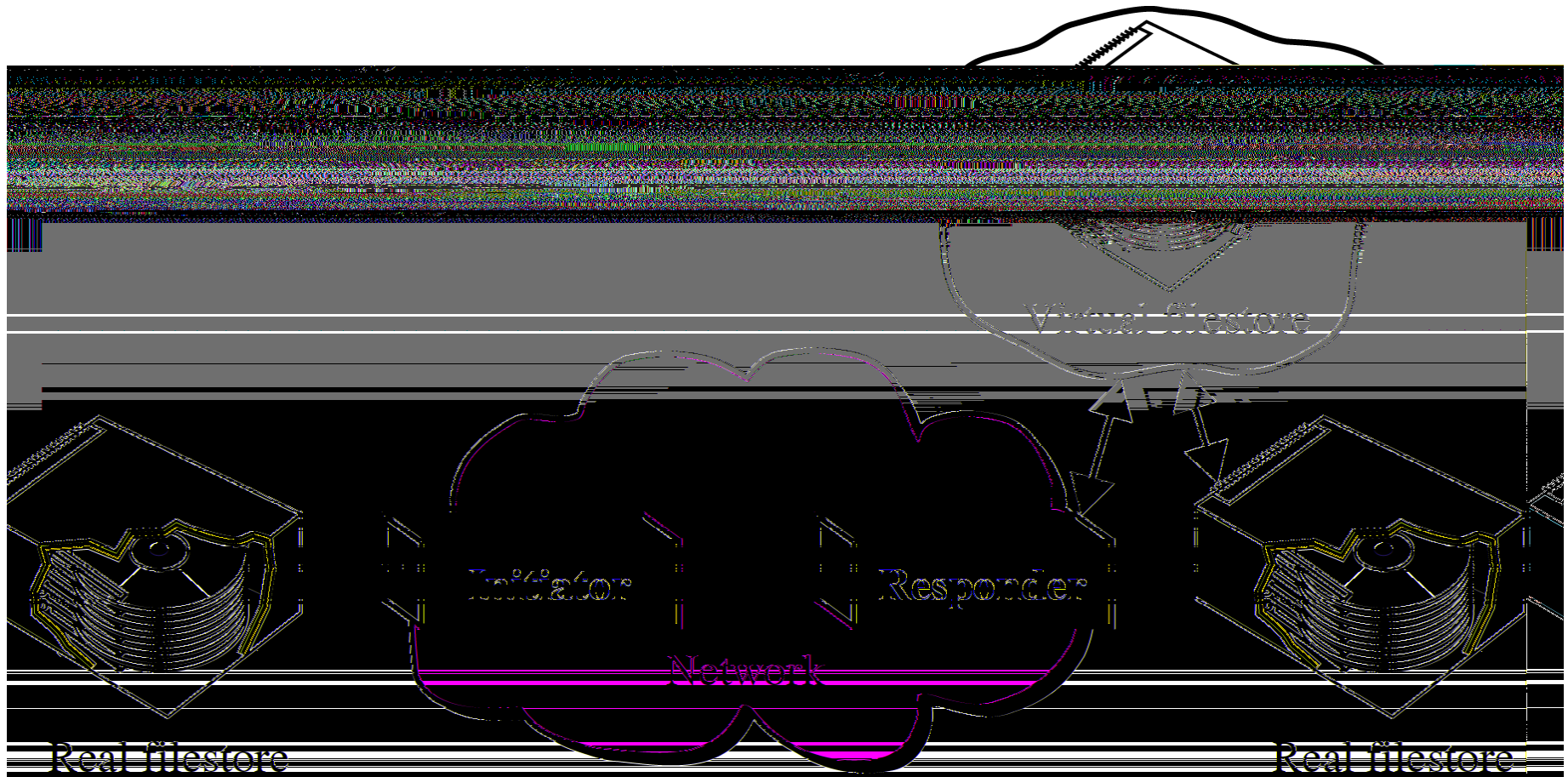
Figure 23-31

Local Access

Terminal

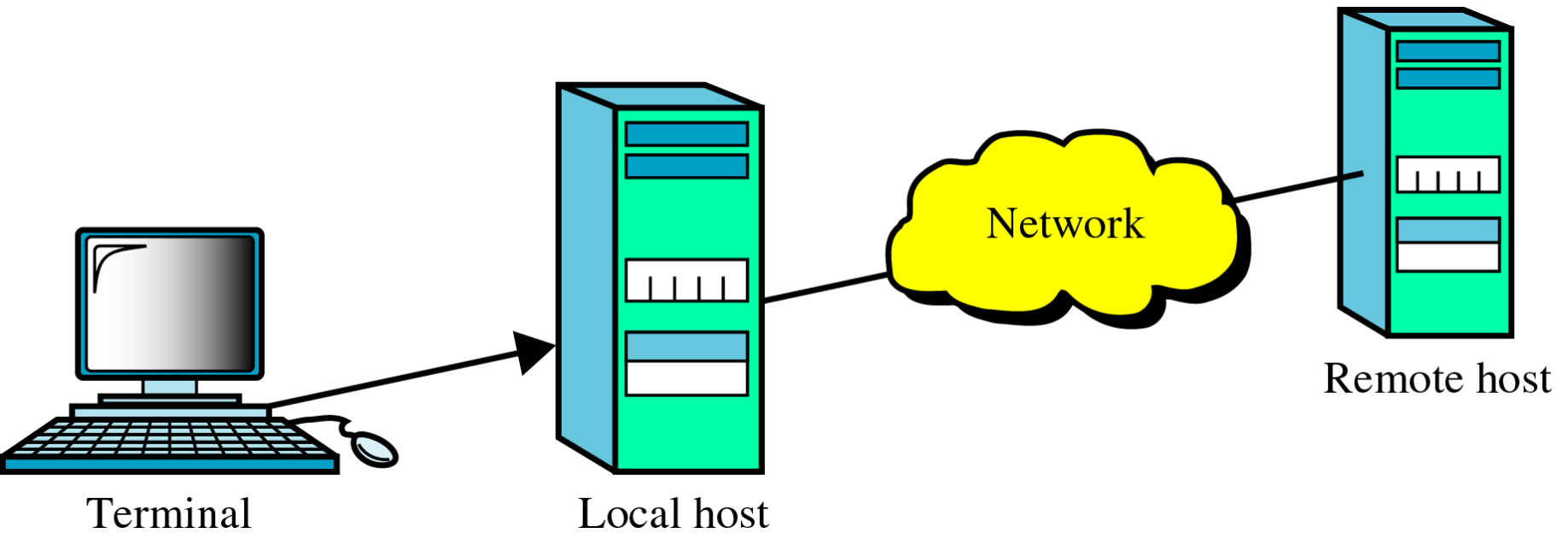Local host

Figure 23-32

Remote Access

Terminal   Local host   Remote host

Figure 23-33

Virtual Terminal