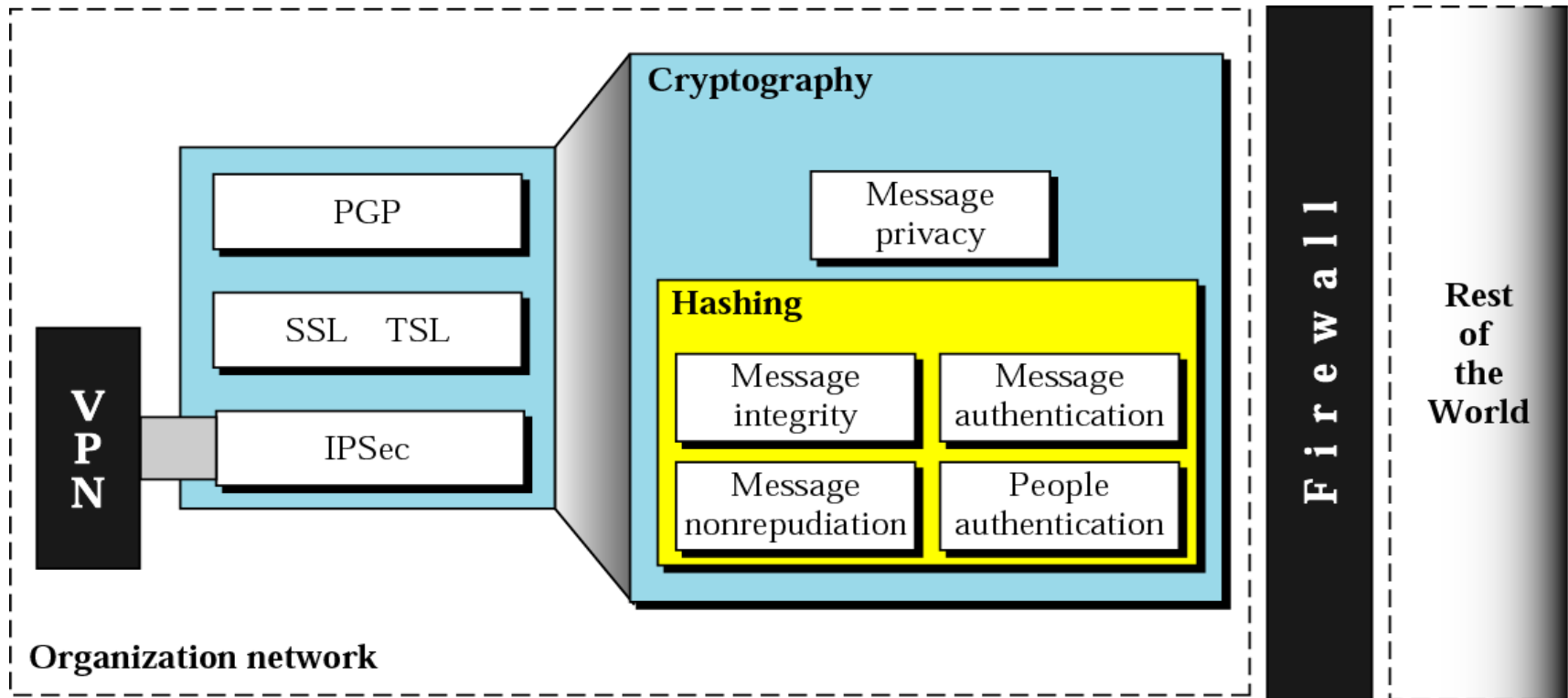




PART VII

Security

Security Topics





Chapters

Chapter 29 ***Cryptography***

Chapter 30 ***Message Authentication, User Authentication, and Key Management***

Chapter 31 ***Security Protocols in The Internet***

Chapter 29

Cryptography

29.1 Introduction

Introduction to Cryptography

Figure 29.1 Cryptography components

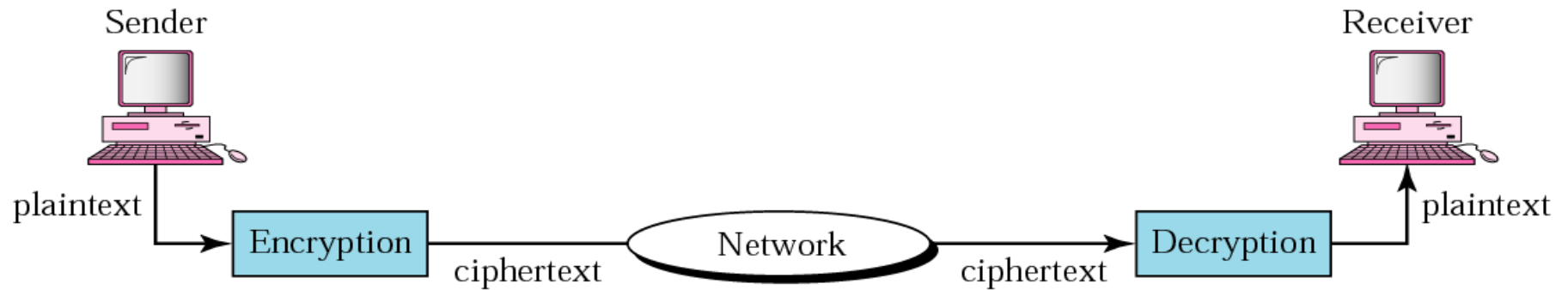
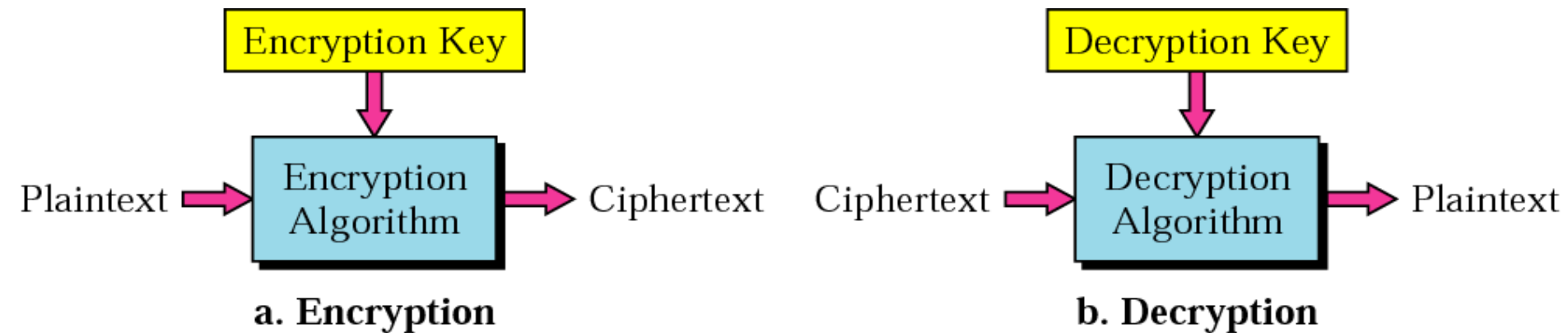


Figure 29.2 Encryption and decryption





Note:

*In cryptography,
the encryption/decryption algorithms
are public; the keys are secret.*

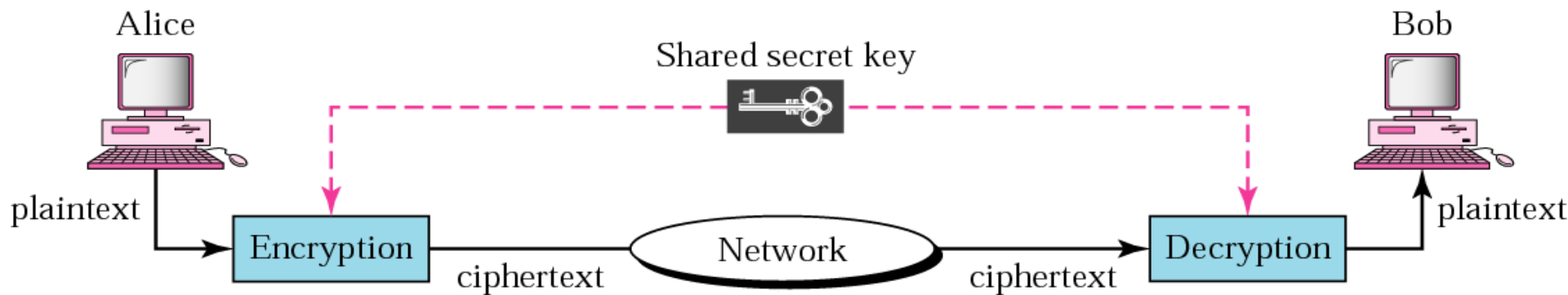
29.2 Symmetric-Key Cryptography

Traditional Cipher

Block Cipher

Operation Modes

Figure 29.3 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.



Note:

In symmetric-key cryptography, the same key is used in both directions.



Note:

Symmetric-key cryptography is often used for long messages.

Figure 29.4 Caesar cipher

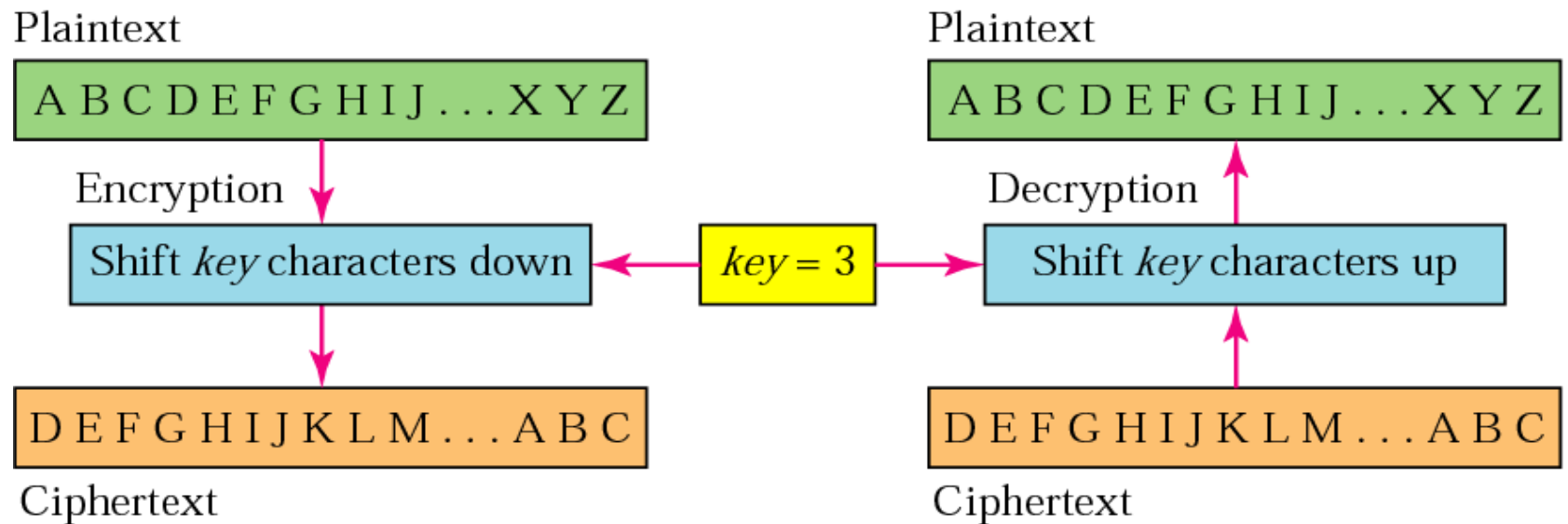


Figure 29.5 Example of monoalphabetic substitution

Encryption algorithm

Substitute top row character
with bottom row character

Decryption algorithm

Substitute bottom row character
with top row character

A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
K	C	P	S	V	M	H	F	D	B	U	W	Q	N	R	Y	T	J	O	I	X	E	L	A	Z	G

Key



Note:

In monoalphabetic substitution, the relationship between a character in the plaintext to the character in the ciphertext is always one-to-one.

Figure 29.6 Vigenere cipher

Character in plaintext

	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
0	W	R	K	D	O	V	C	A	S	B	Y	Q	M	L	H	I	T	U	F	E	Z	N	G	J	P	X
1	H	Q	B	G	W	E	R	K	F	C	O	A	Z	J	M	S	L	V	N	I	P	U	D	T	X	Y
2	P	I	D	Z	X	V	S	T	O	C	M	J	N	L	B	Q	R	U	W	K	H	G	E	F	A	Y
⋮																										
25	M	C	I	D	A	X	V	S	T	O	N	L	K	U	R	E	W	Z	H	F	P	G	Y	J	B	Q

Character in Ciphertext

Key = (Position of character in the text) mod 26



Note:

In polyalphabetic substitution, the relationship between a character in the plaintext and a character in the ciphertext is one-to-many.

Figure 29.7 Transpositional cipher

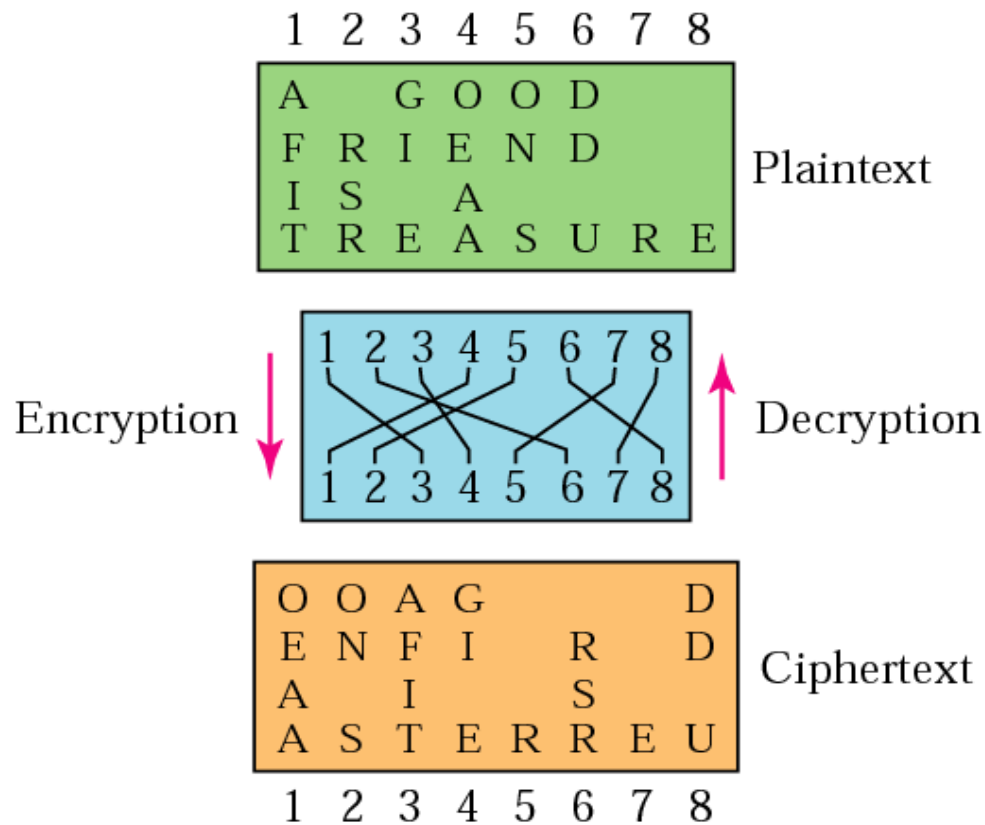


Figure 29.8 Block cipher

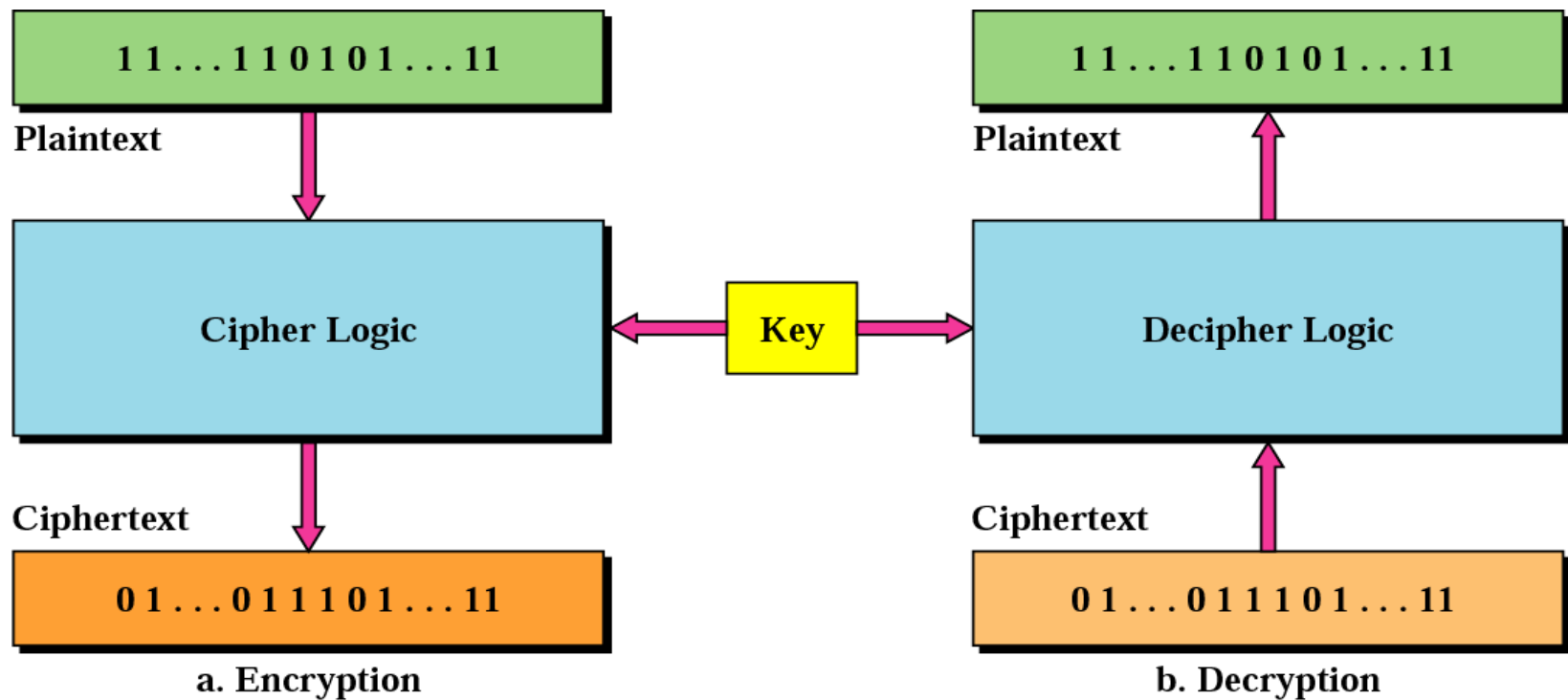


Figure 29.9 P-box

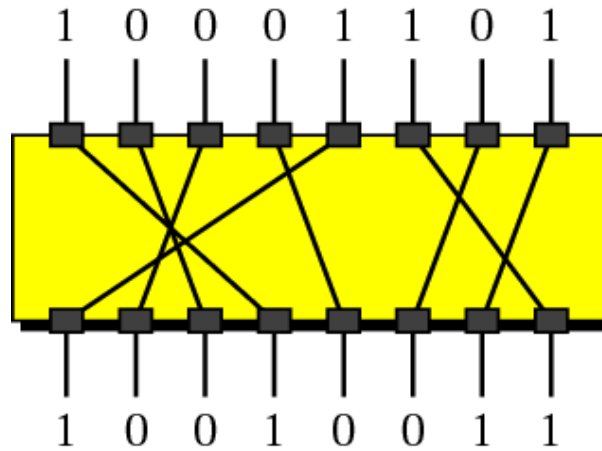


Figure 29.10 S-box

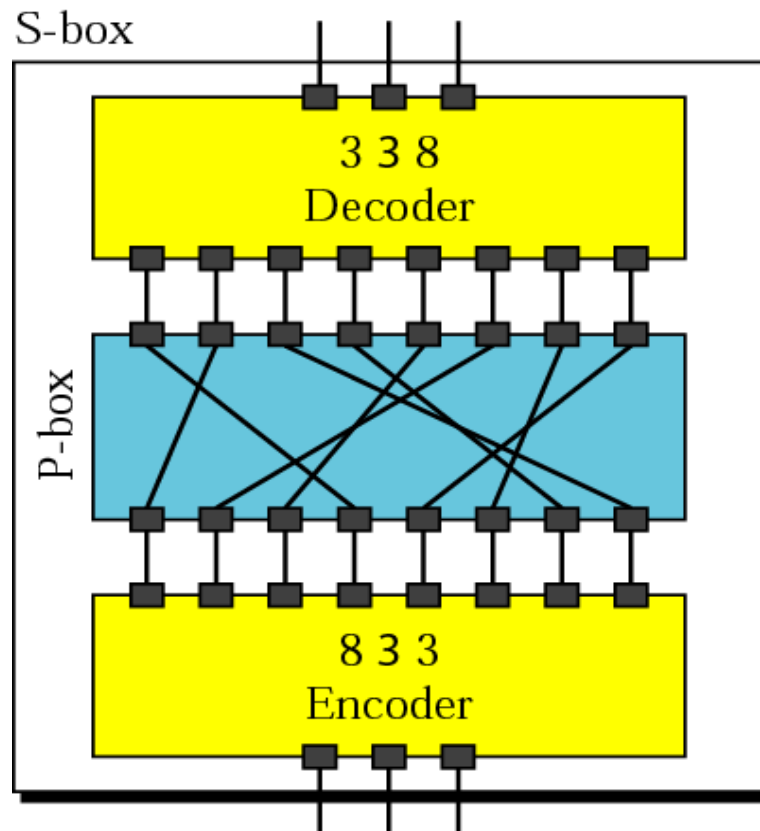


Figure 29.11 Product block

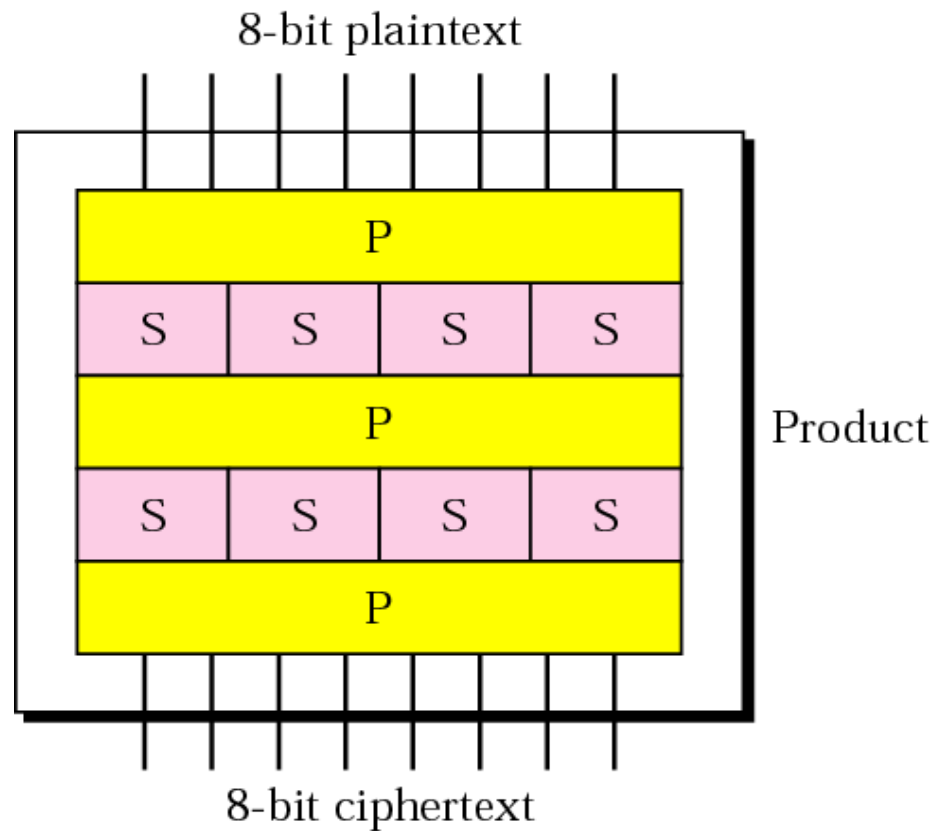


Figure 29.12 DES

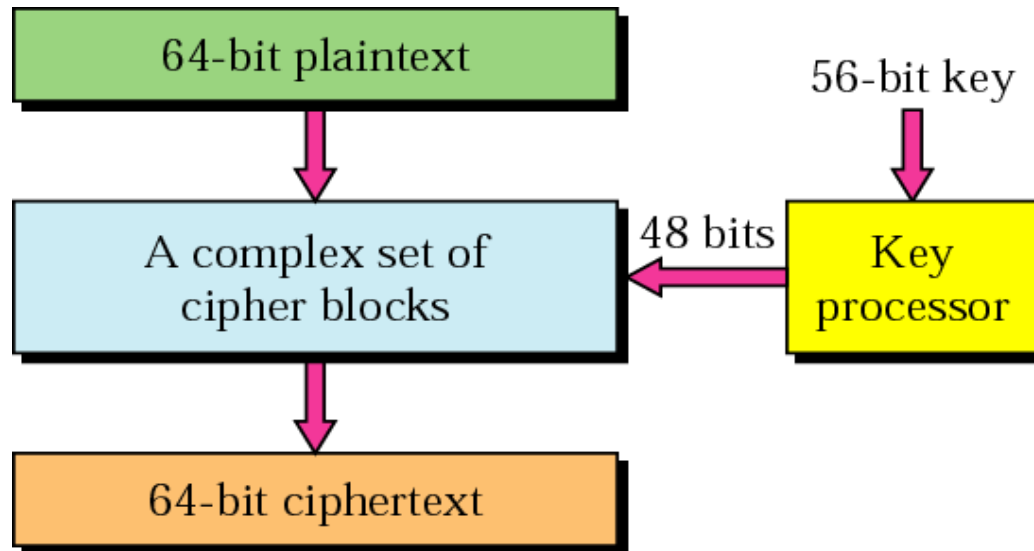


Figure 29.13 General scheme of DES

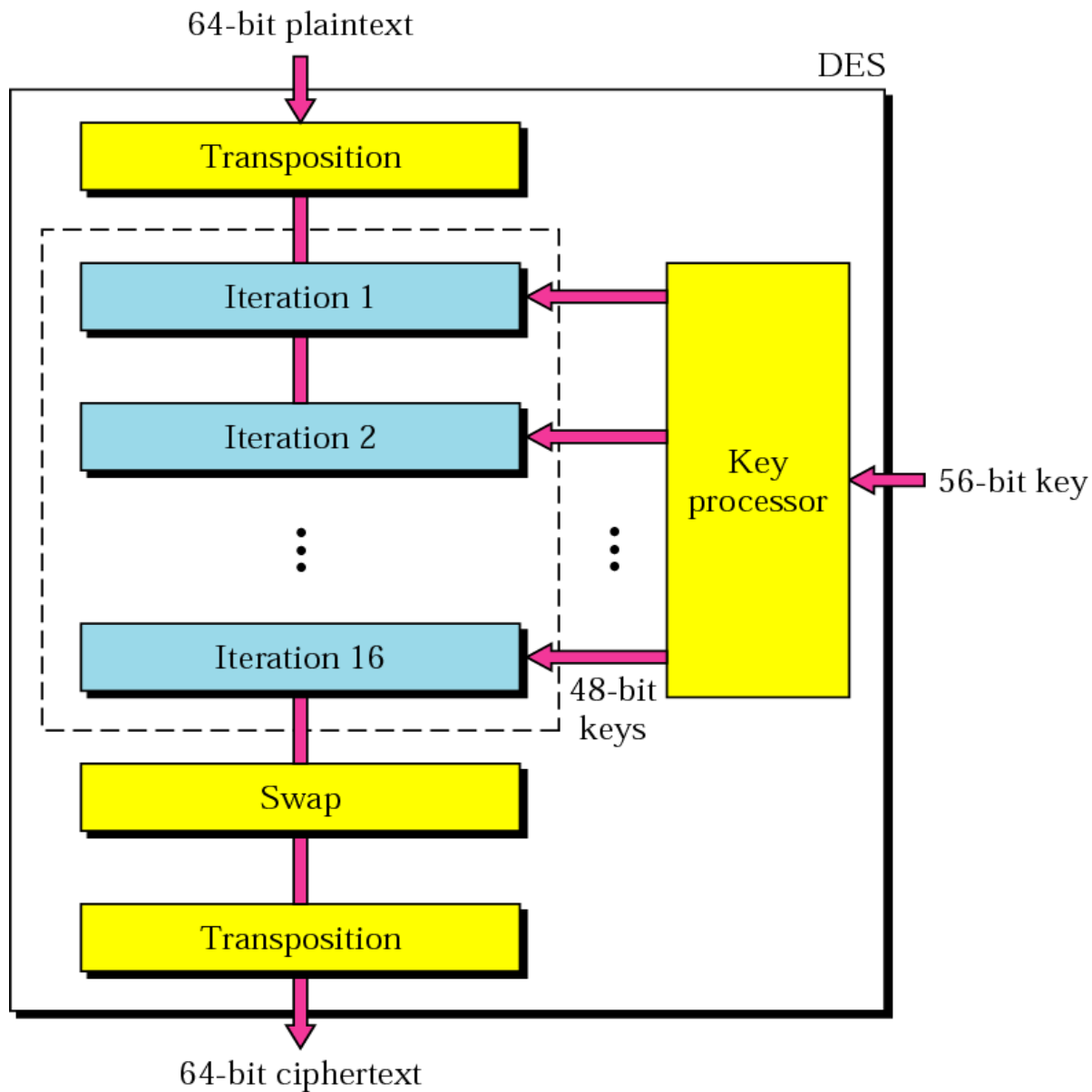


Figure 29.14 Iteration block

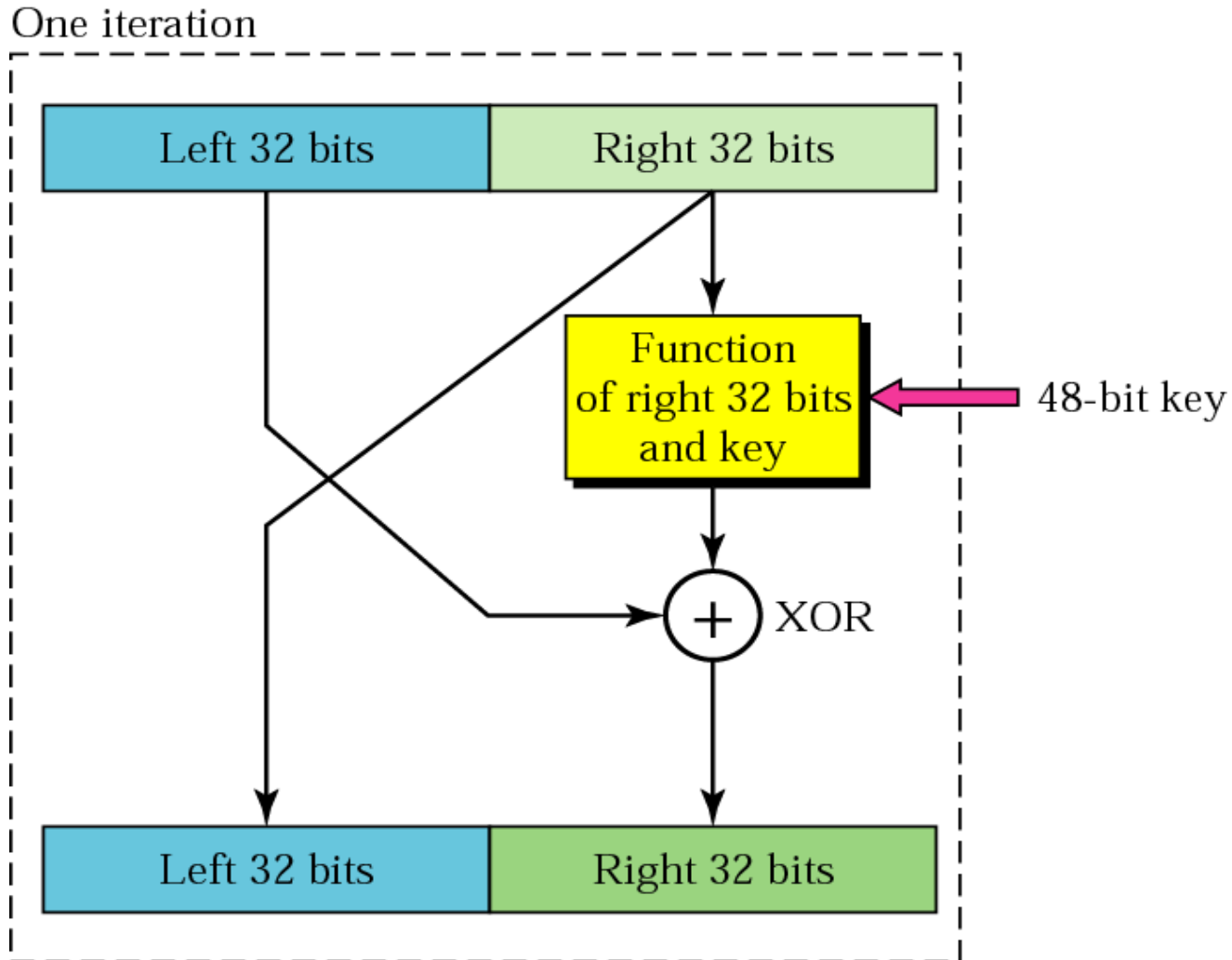
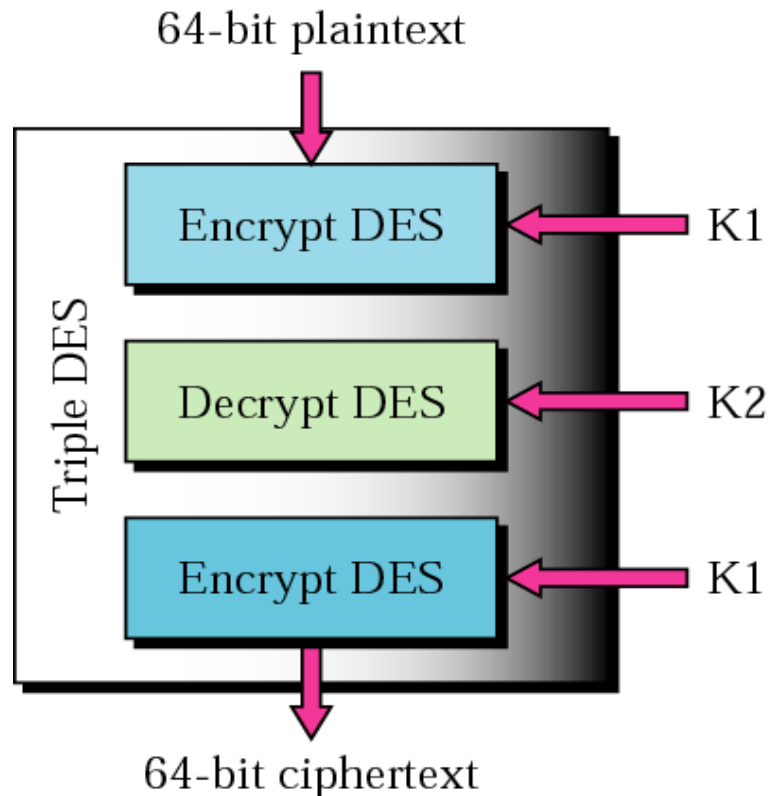
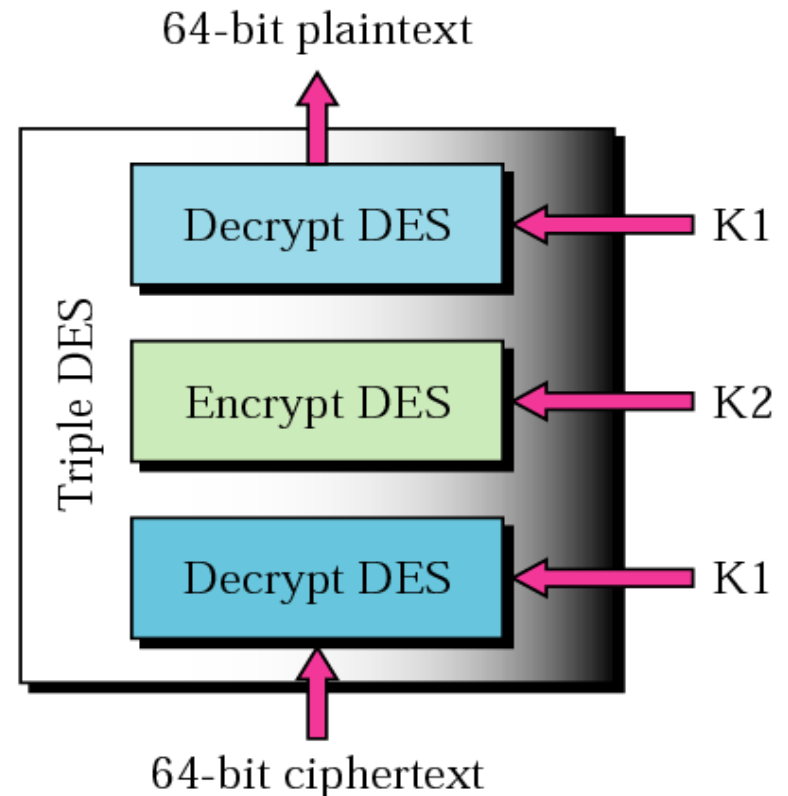


Figure 29.15 Triple DES



a. Encryption triple DES



b. Decryption triple DES



Note:

The DES cipher uses the same concept as the Caesar cipher, but the encryption/decryption algorithm is much more complex due to the sixteen 48-bit keys derived from a 56-bit key.

Figure 29.16 ECB mode

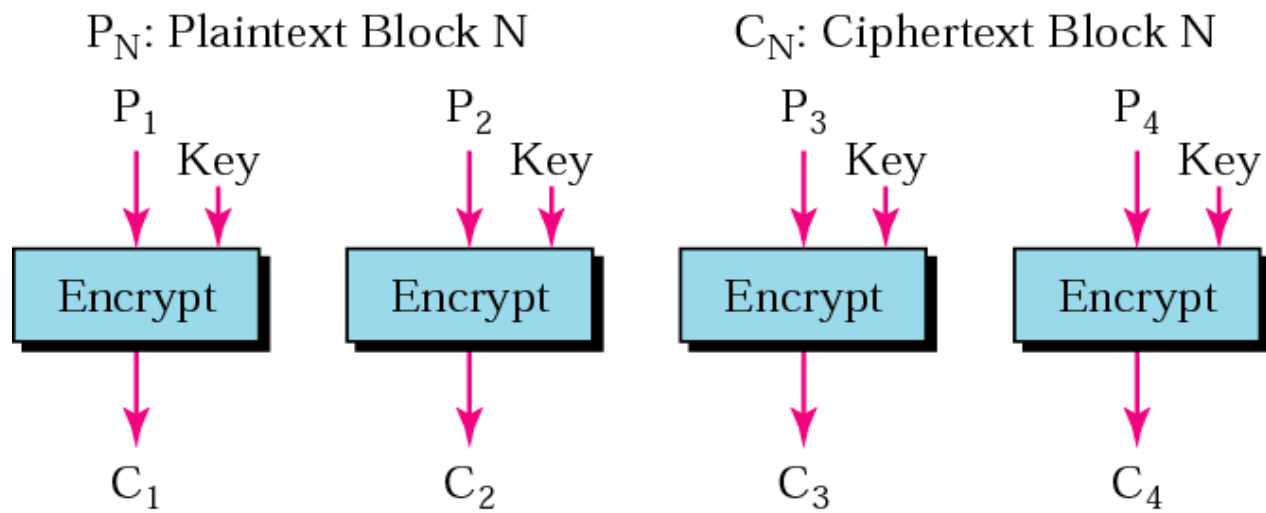


Figure 29.17 CBC mode

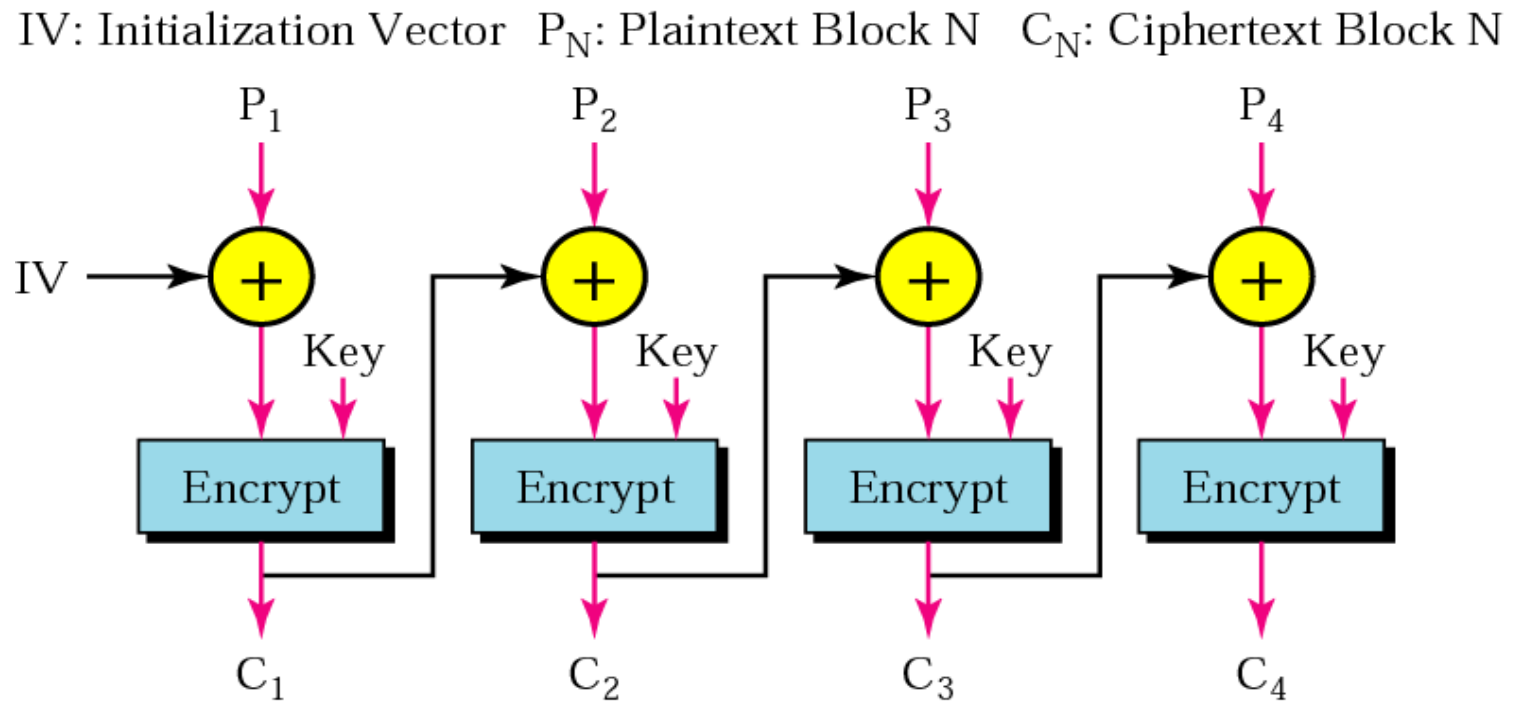


Figure 29.18 CFM

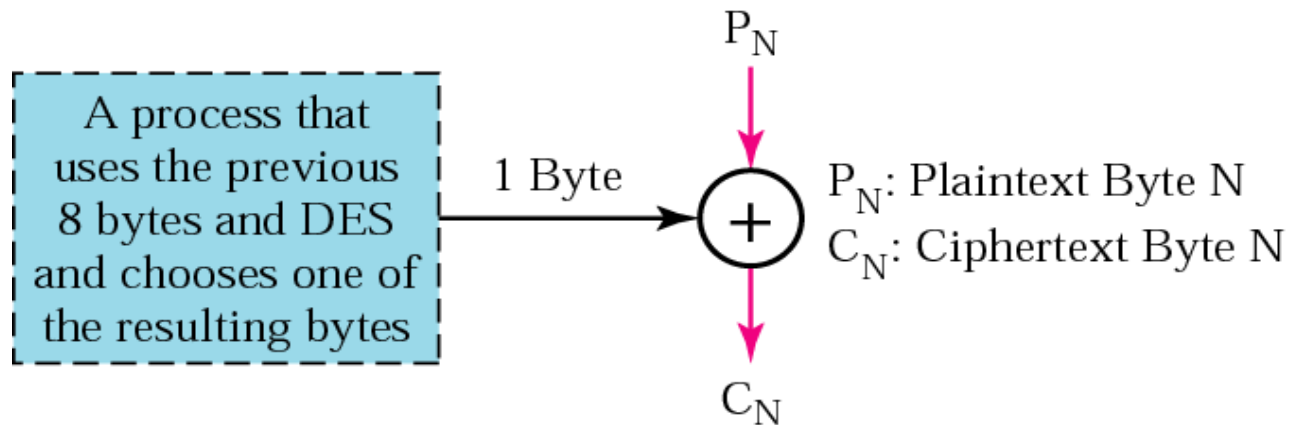
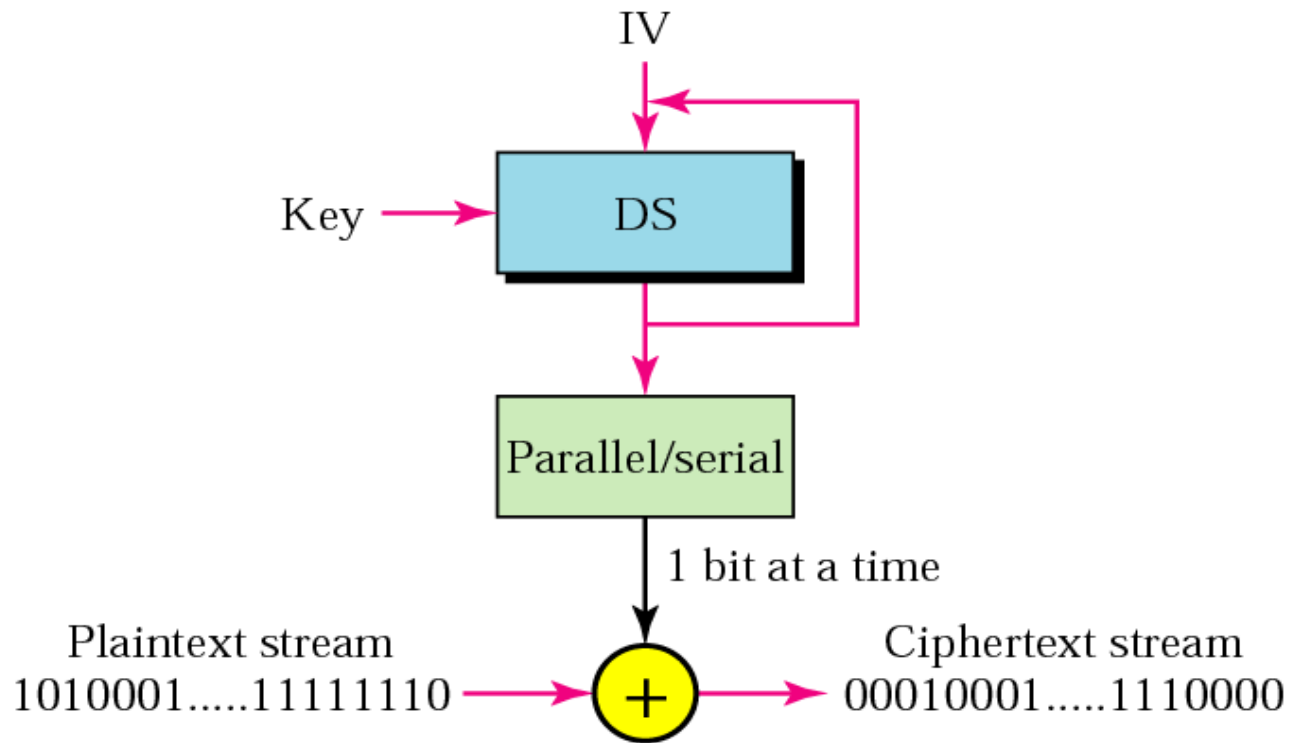


Figure 29.19 CSM

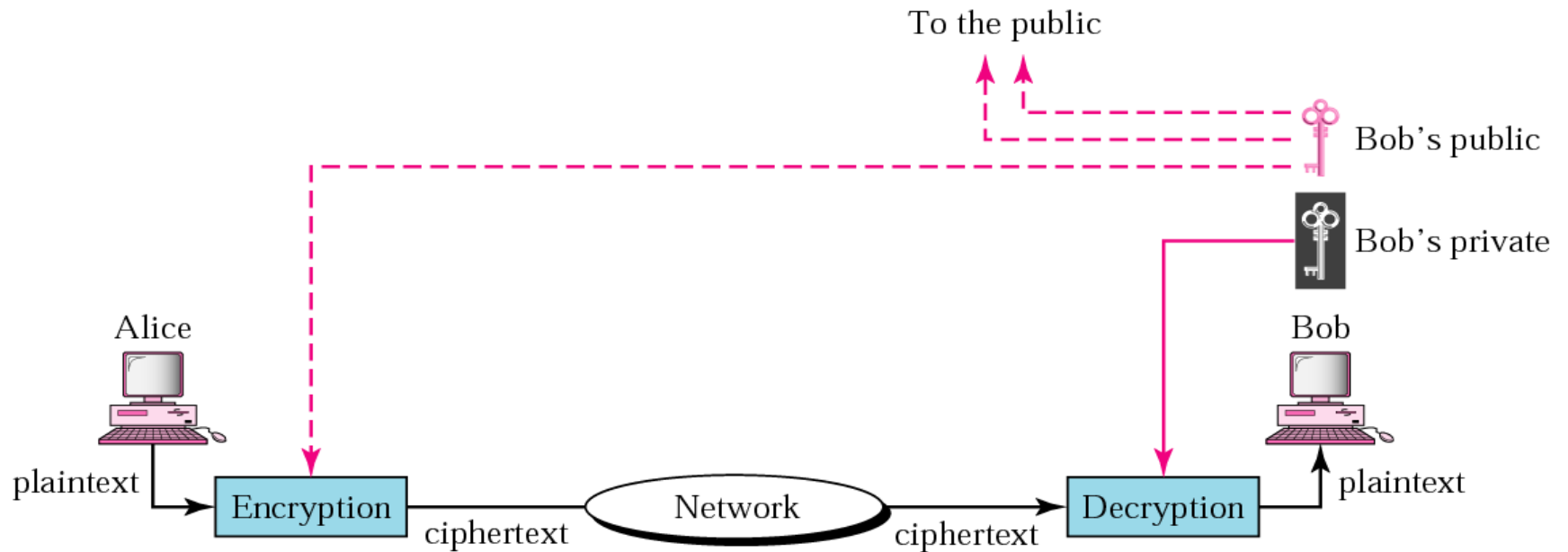


29.3 Public-Key Cryptography

RSA

Choosing Public and Private Keys

Figure 29.20 Public-key cryptography





Note:

Public-key algorithms are more efficient for short messages.

Figure 29.21 RSA

