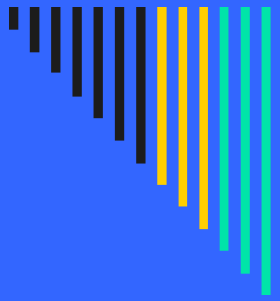
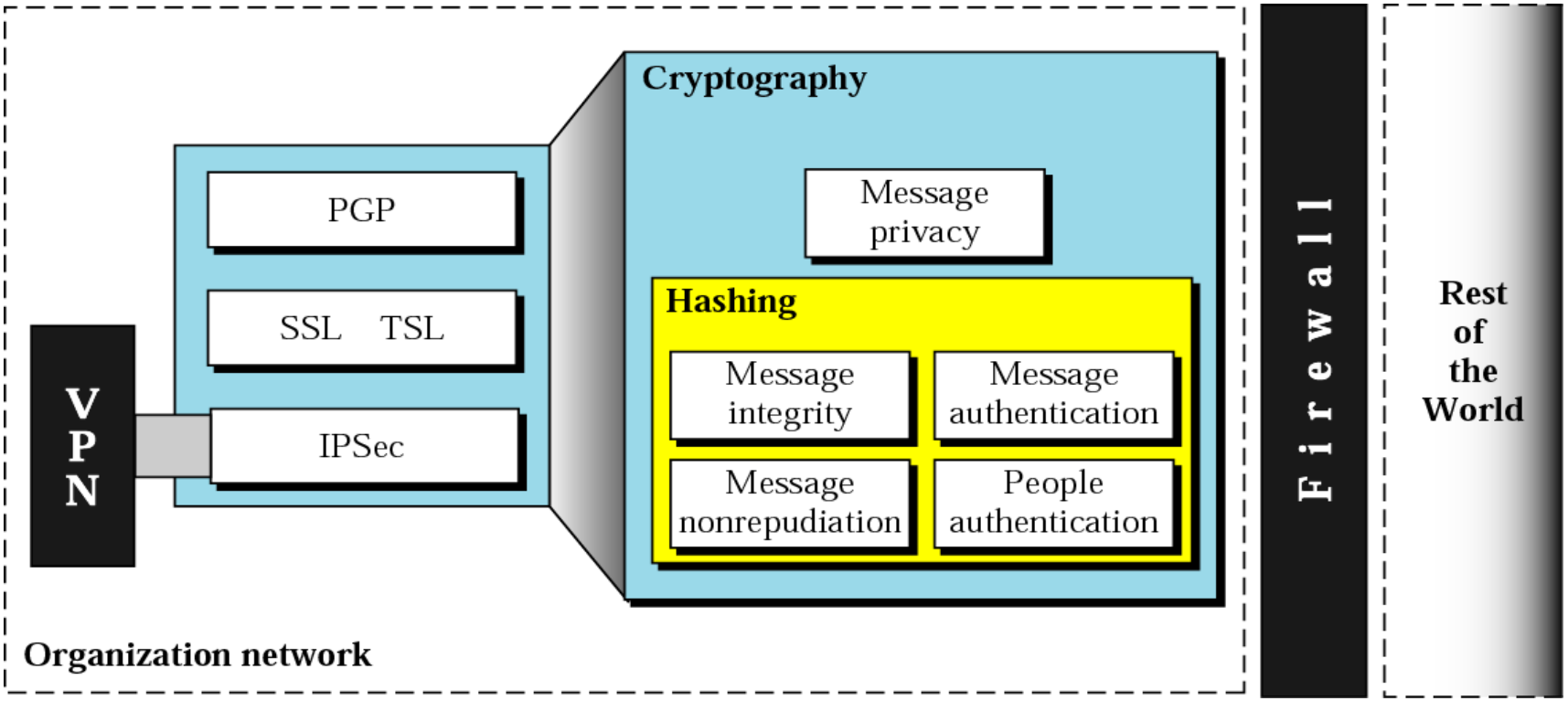


PART VII

Security

Security Topics



Chapters

Chapter 29

Cryptography

29.1 Introduction

Introduction to Cryptography

Figure 29.1 Cryptography components

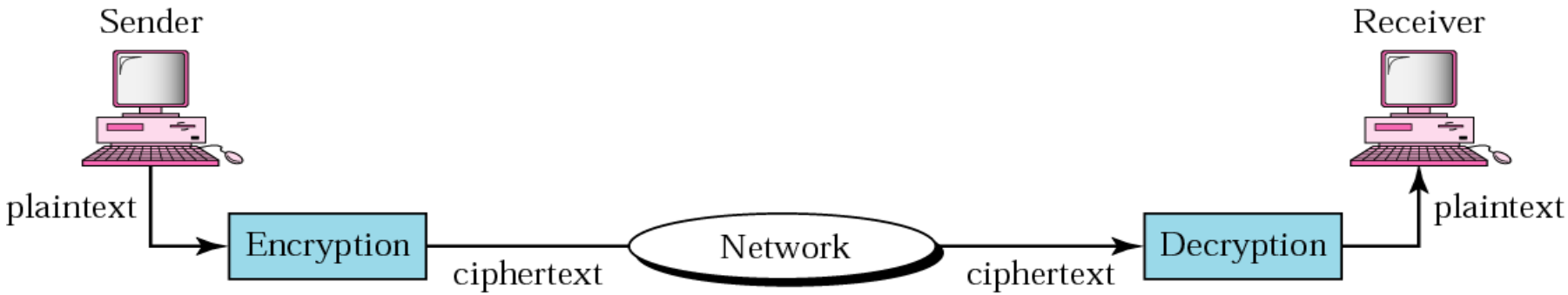
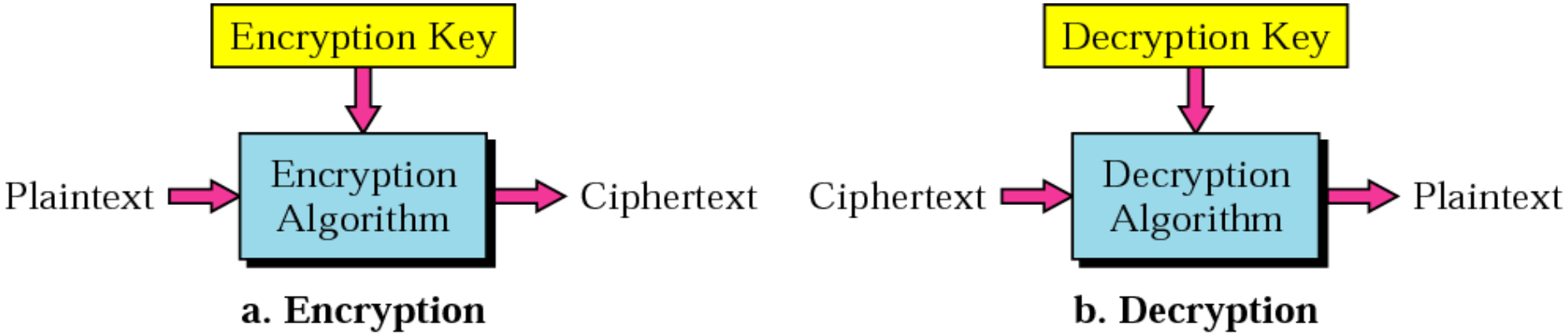


Figure 29.2 Encryption and decryption



Note:

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

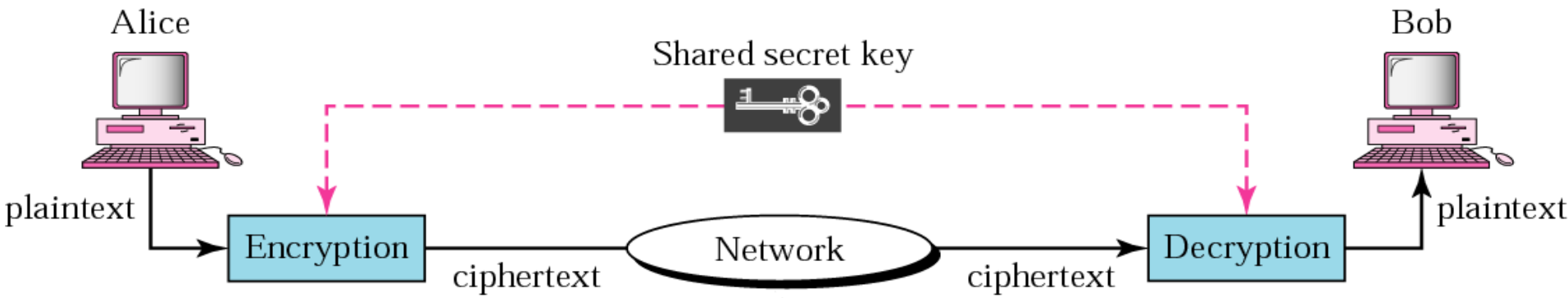
29.2 Symmetric-Key Cryptography

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.

Symmetric-key cryptography is often used for long messages.

Figure 29.4 Caesar cipher

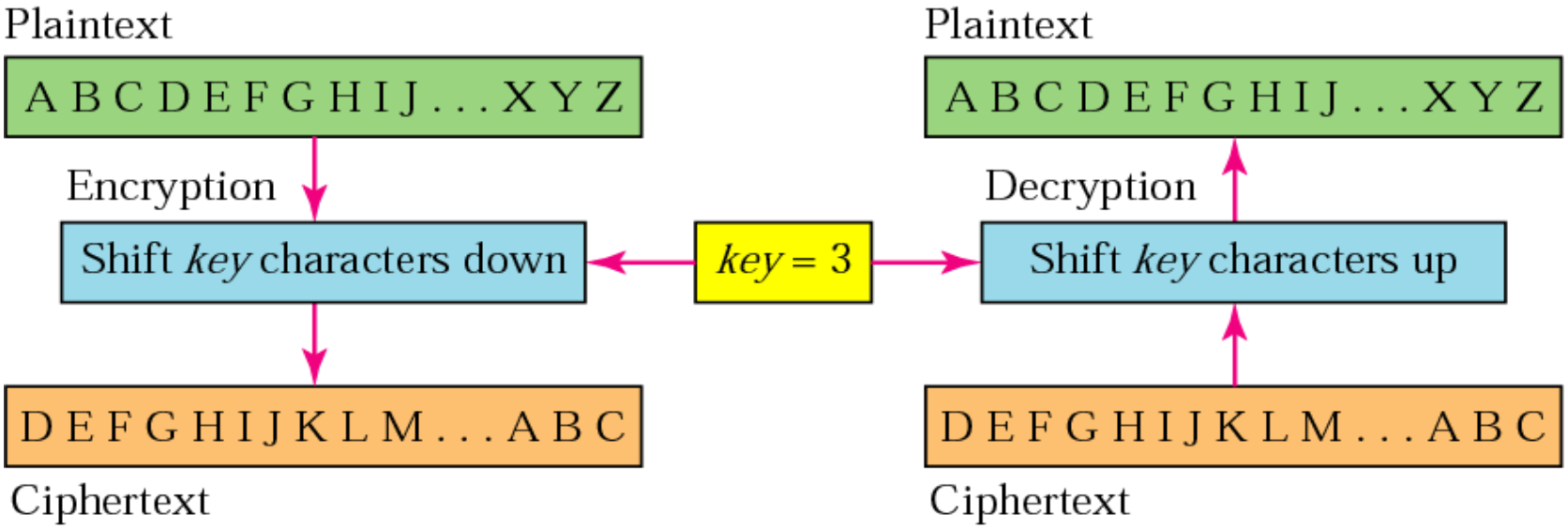


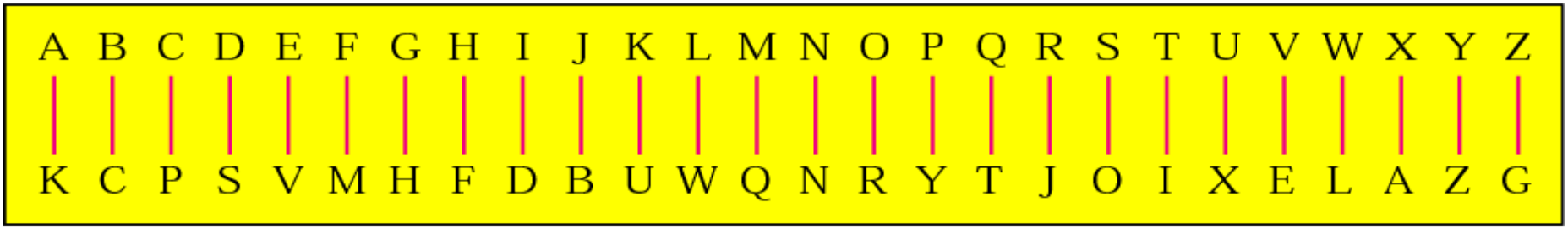
Figure 29.5 Example of monoalphabetic substitution

Encryption algorithm

Substitute top row character with bottom row character

Decryption algorithm

Substitute bottom row character with top row character

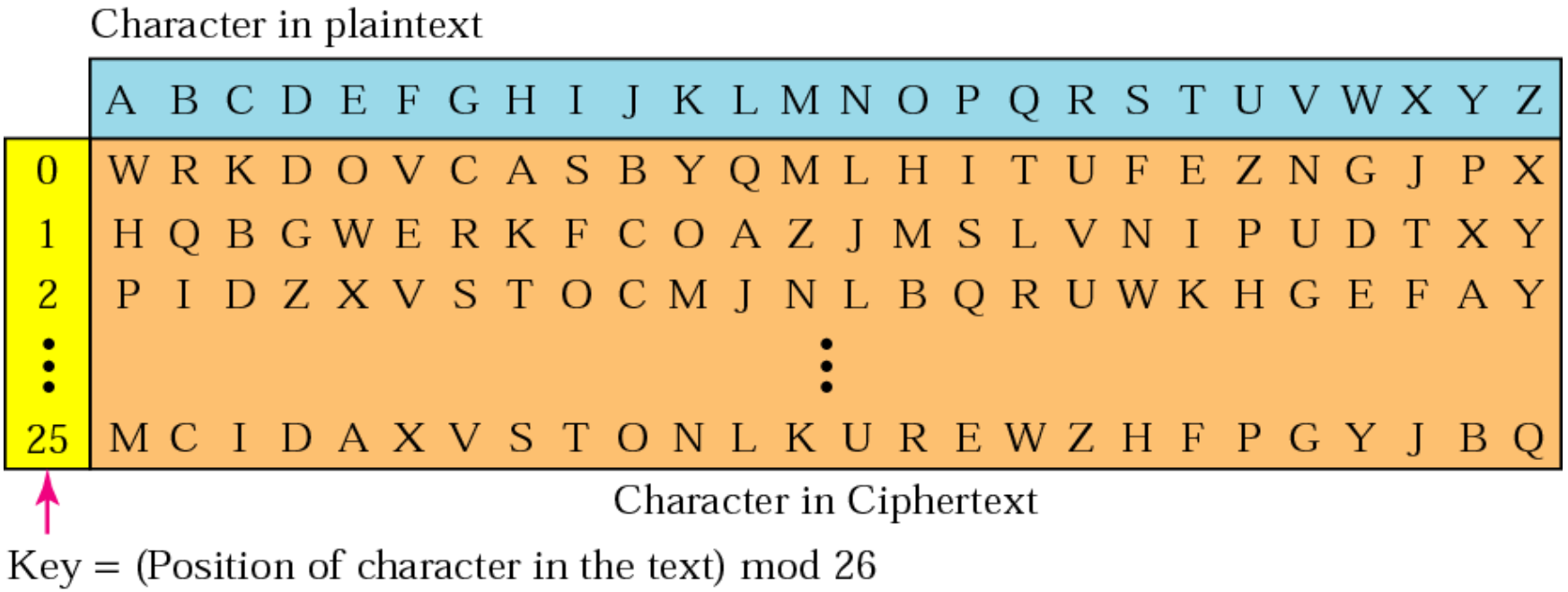


Key

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



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

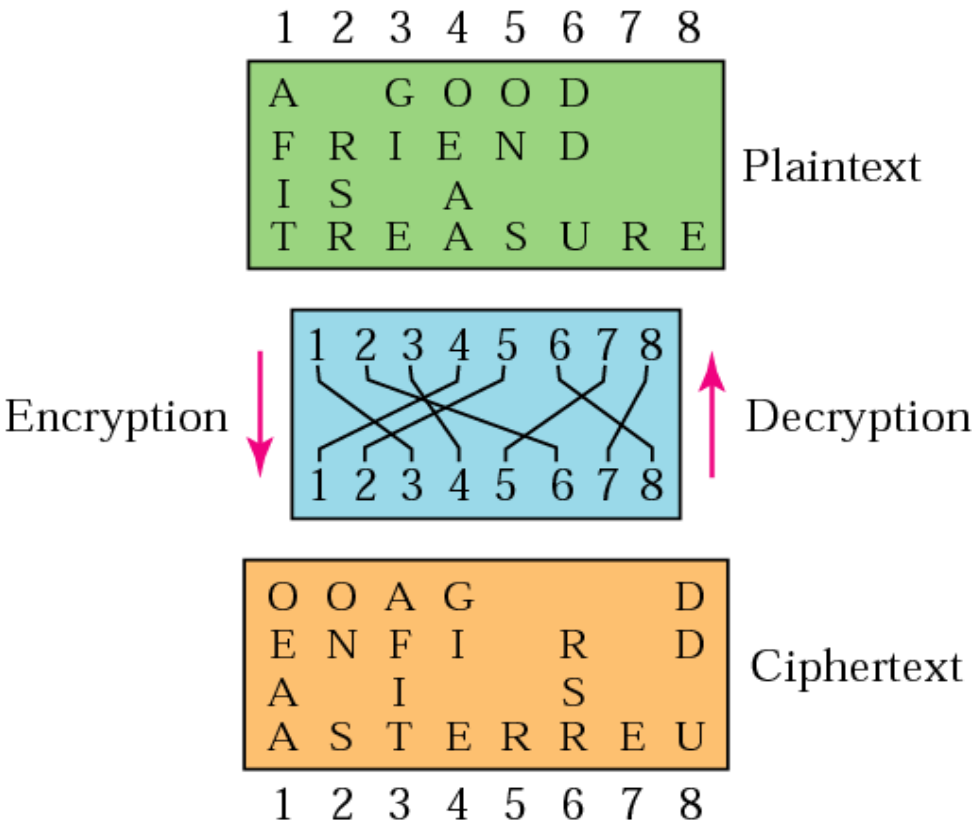


Figure 29.8 Block cipher

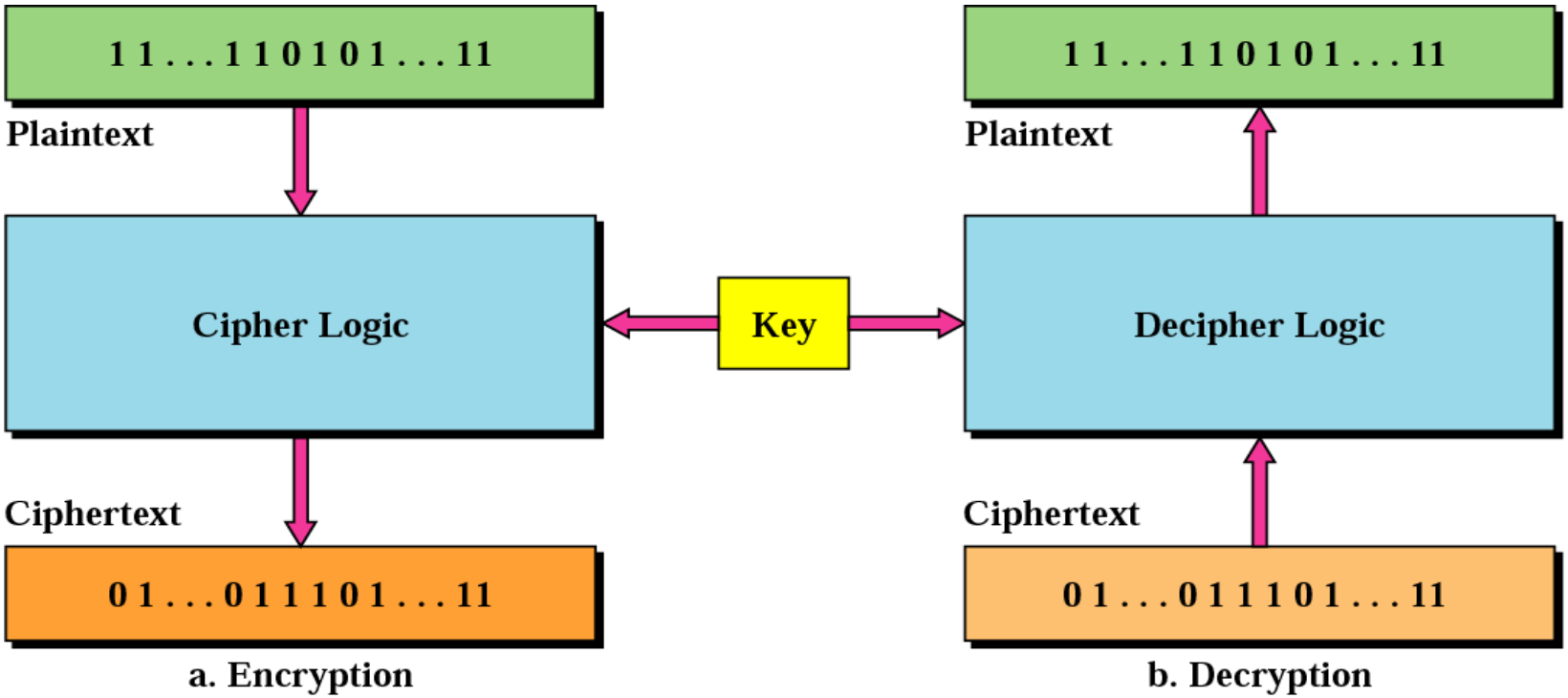


Figure 29.9 P-box

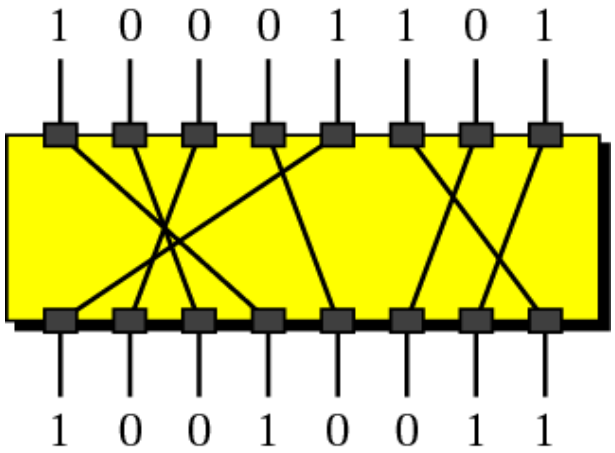


Figure 29.10 S-box

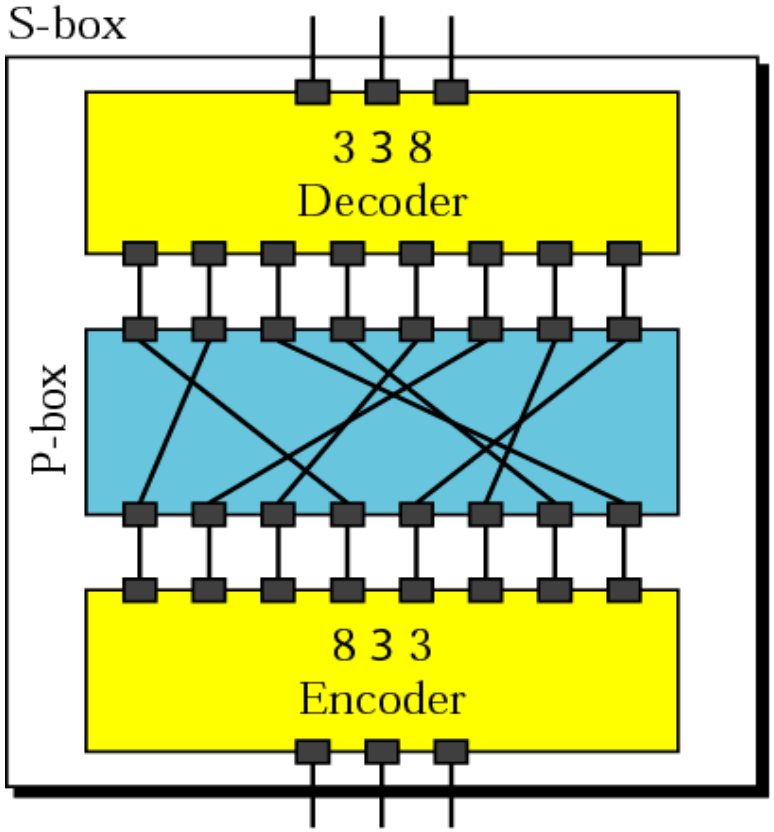


Figure 29.11 Product block

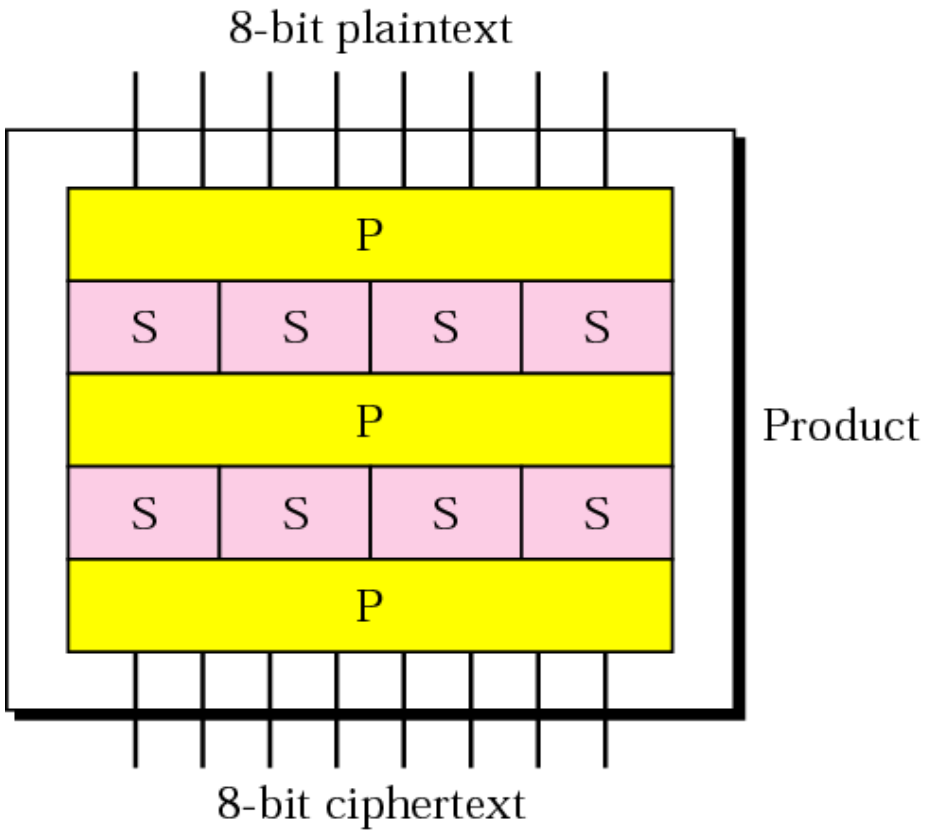


Figure 29.12 DES

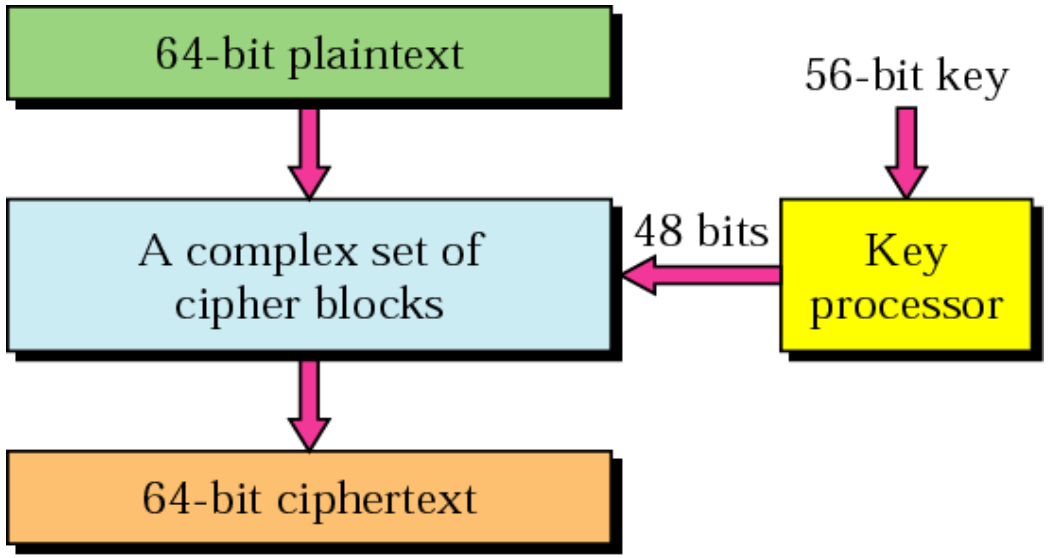


Figure 29.13 General scheme of DES

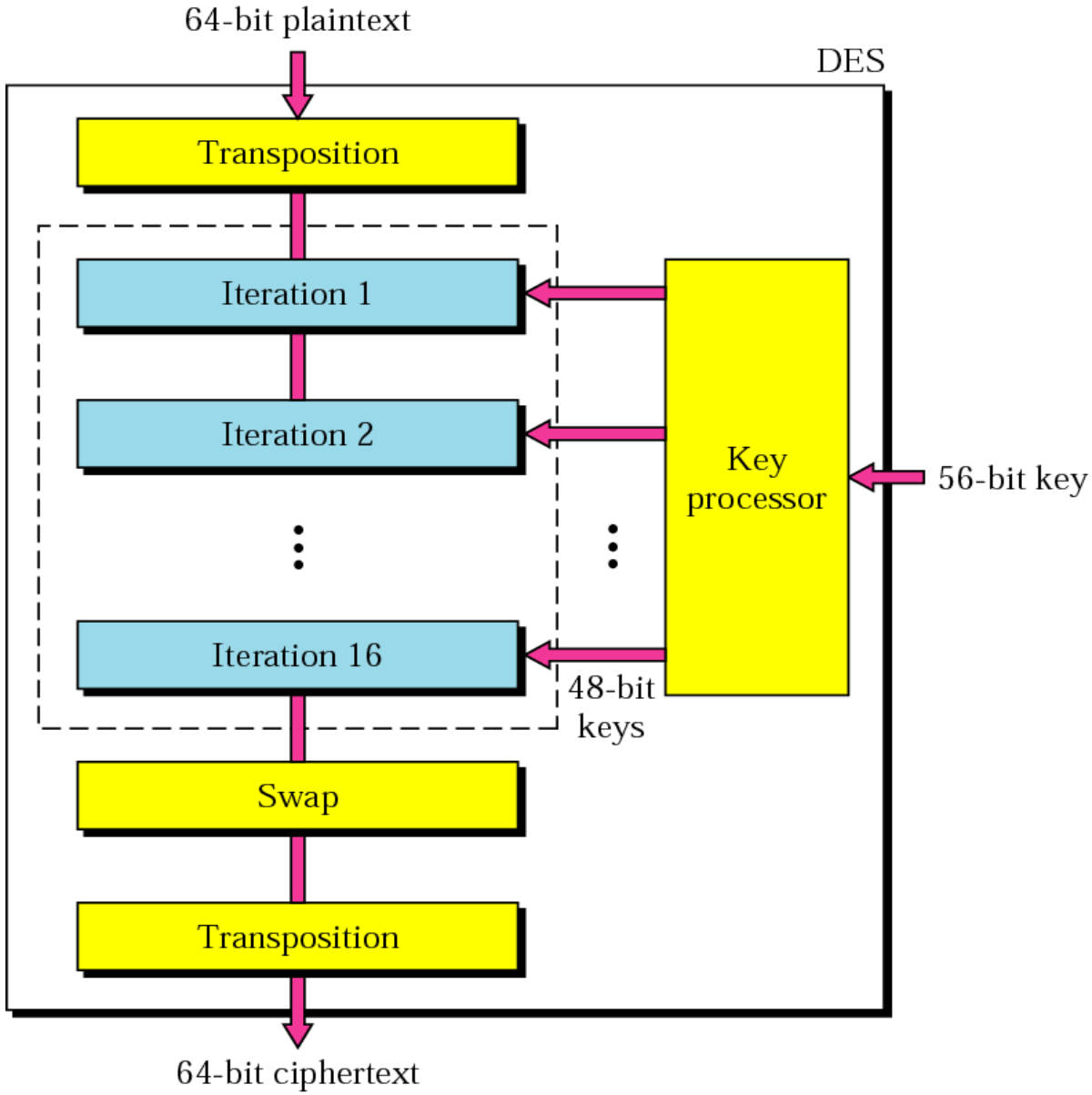


Figure 29.14 Iteration block

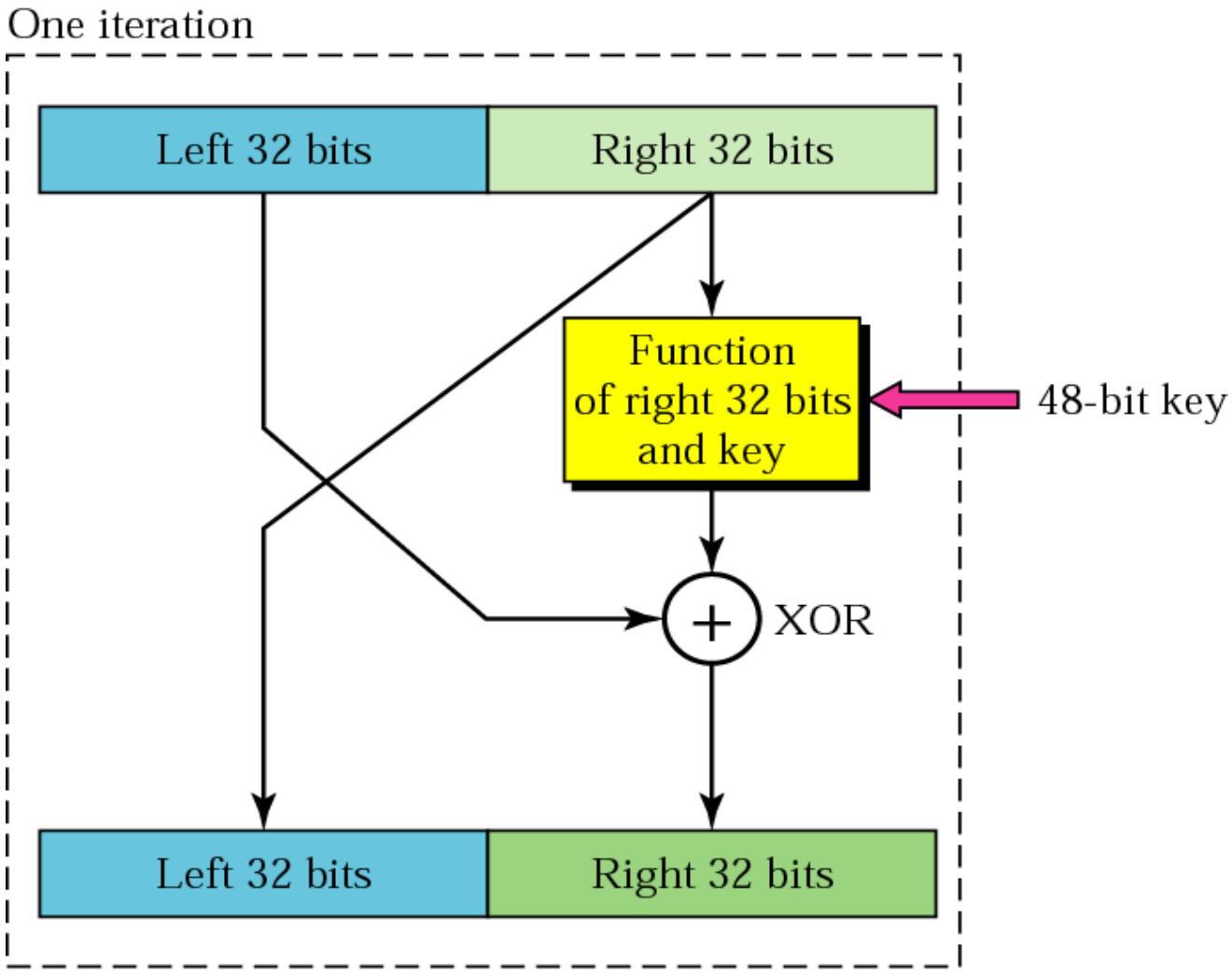
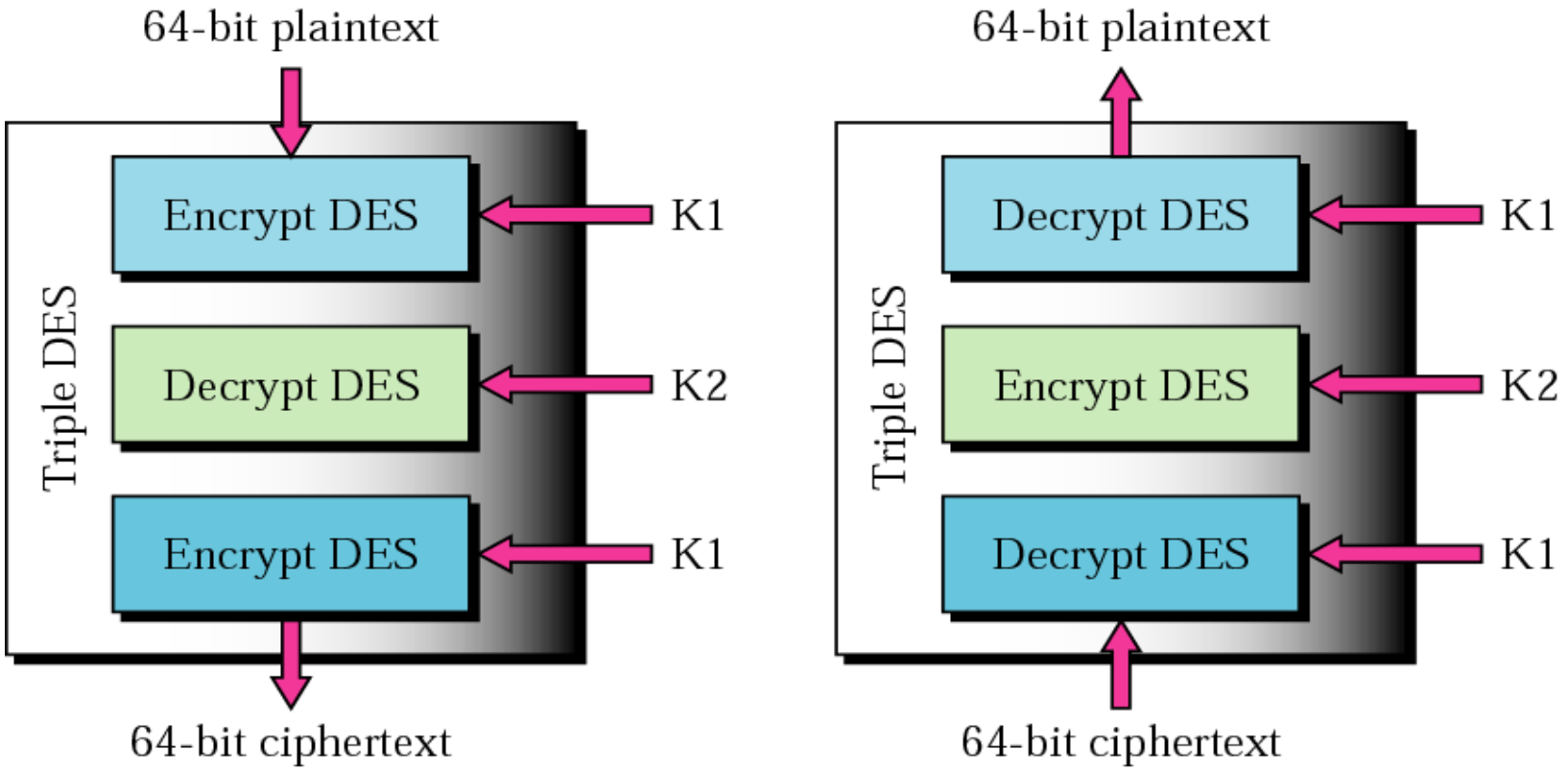


Figure 29.15 Triple DES



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

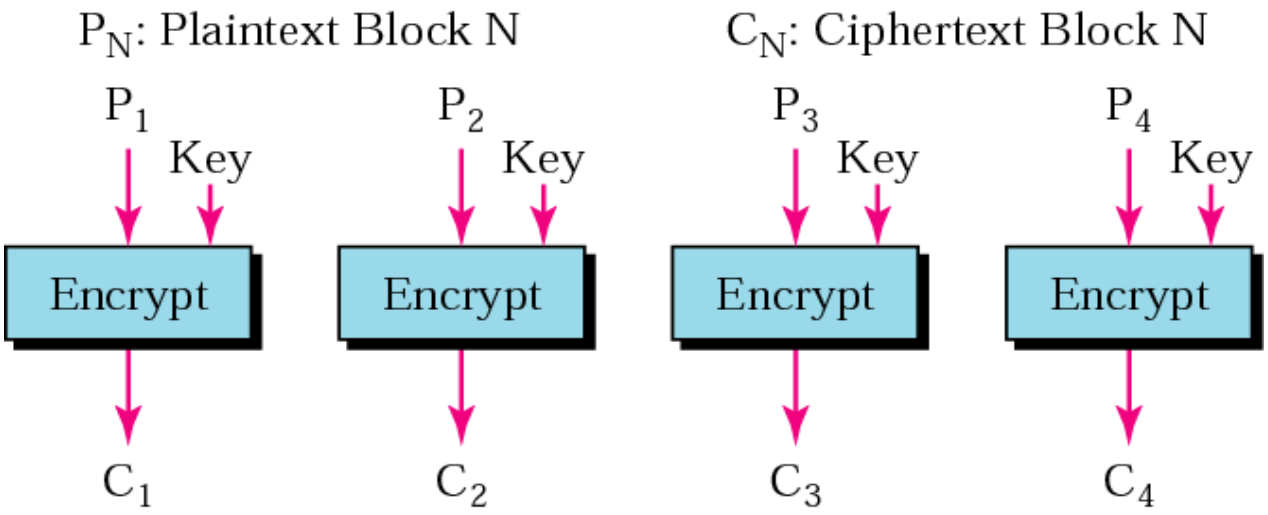


Figure 29.17 CBC mode

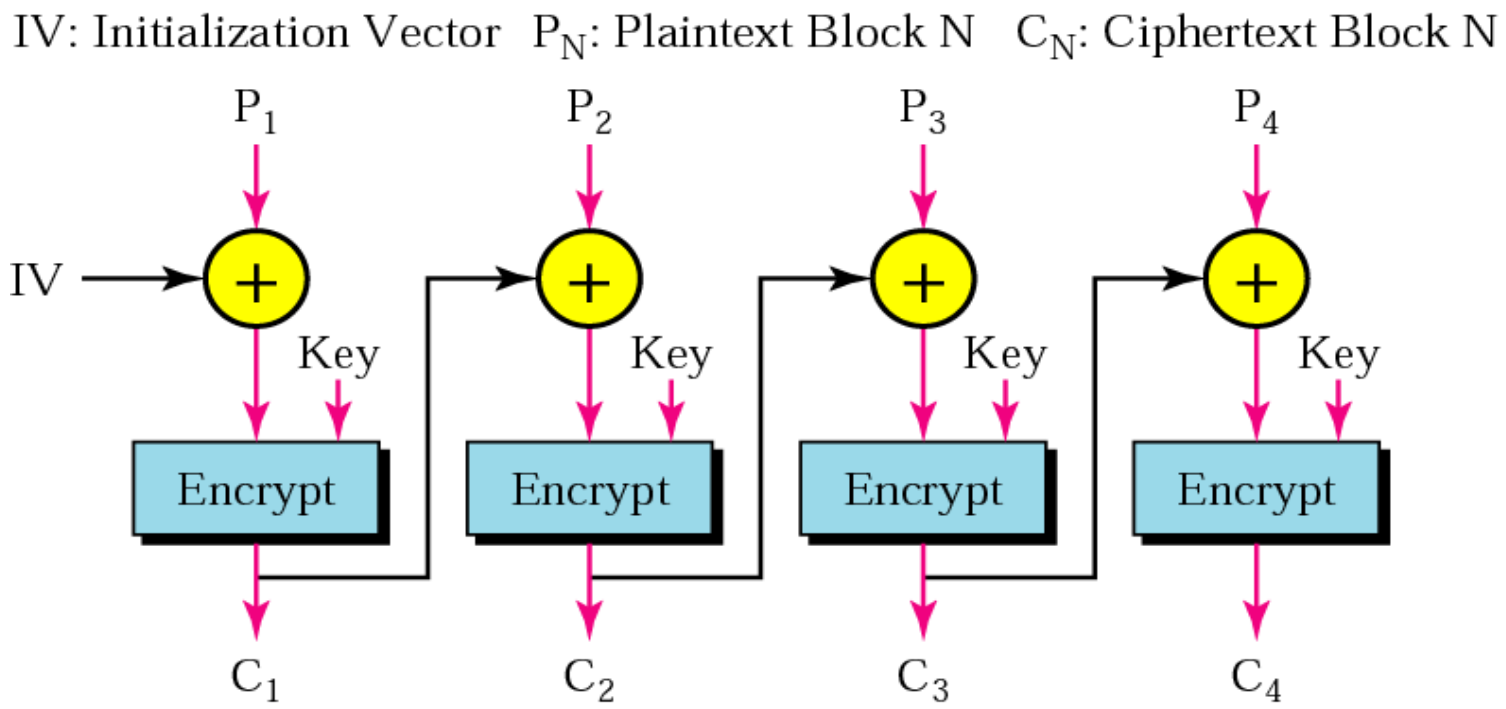


Figure 29.18 CFM

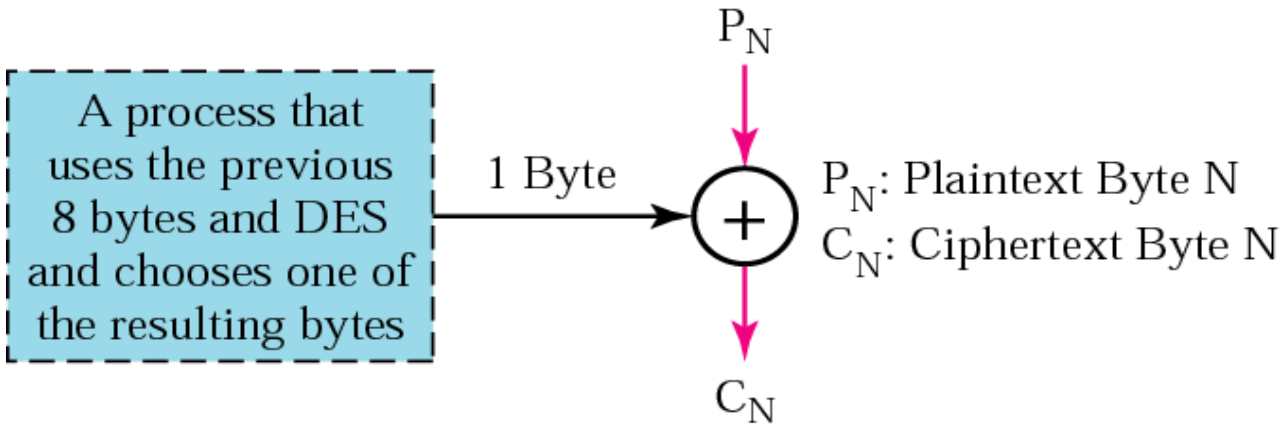
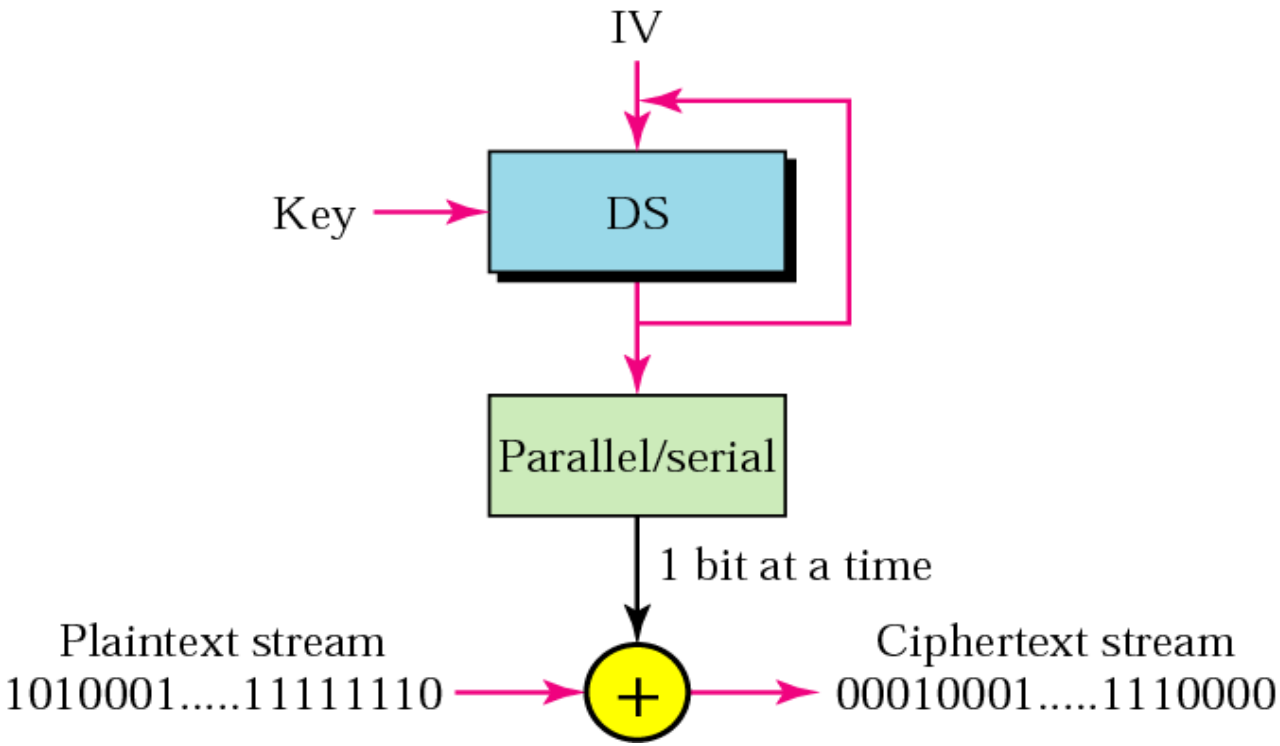


Figure 29.19 CSM

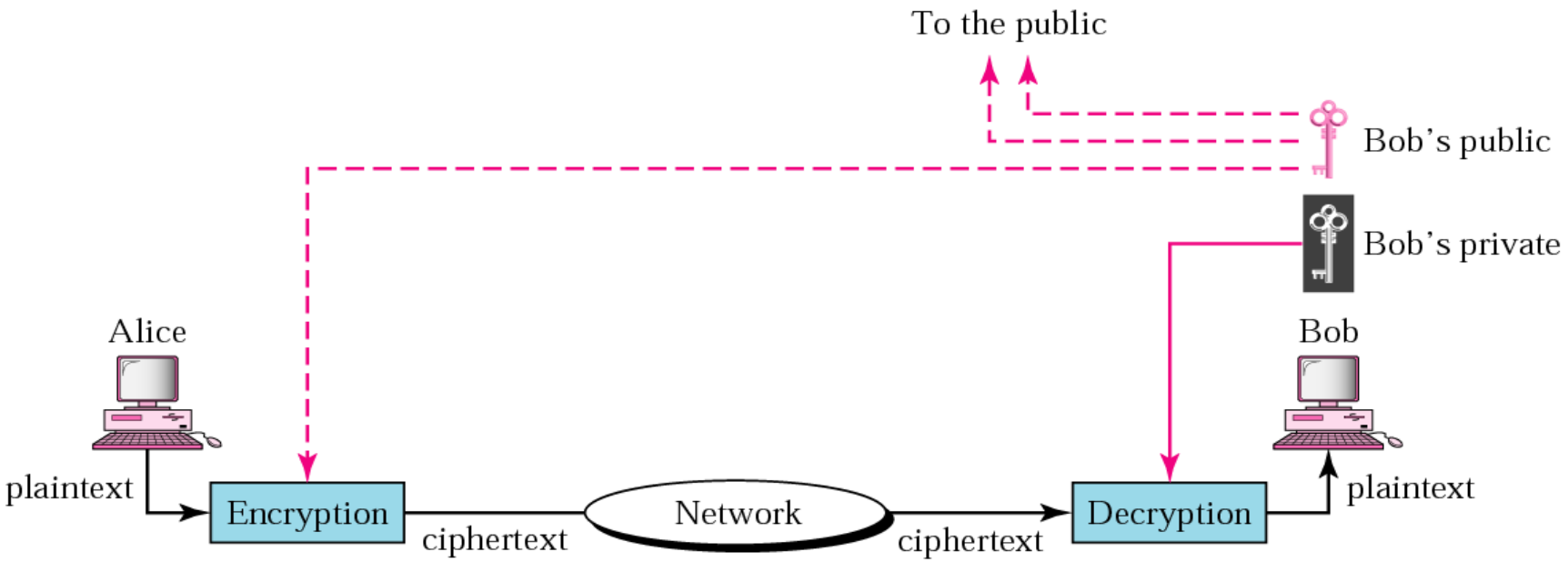


29.3 Public-Key Cryptography

RSA

Choosing Public and Private Keys

Figure 29.20 Public-key cryptography



Public-key algorithms are more efficient for short messages.

Figure 29.21 RSA