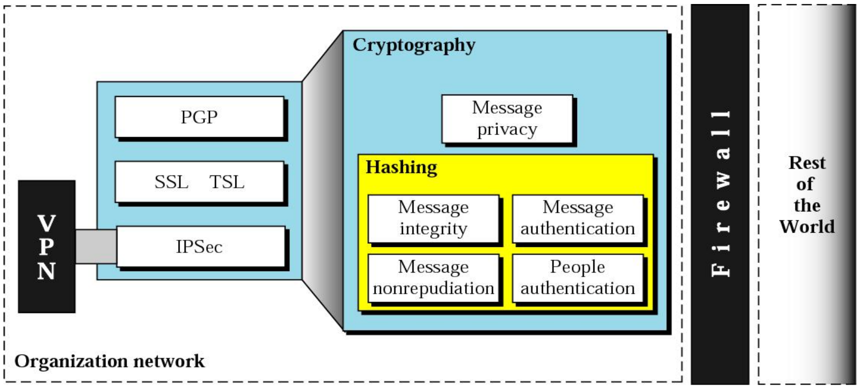
UNIT 2: Cryptography and Cryptographic Algorithms

Cryptography

Message Authentication,
User Authentication,
and Key Management

Security Topics



1 Introduction

Introduction
to
Cryptography

Figure 1 Cryptography components

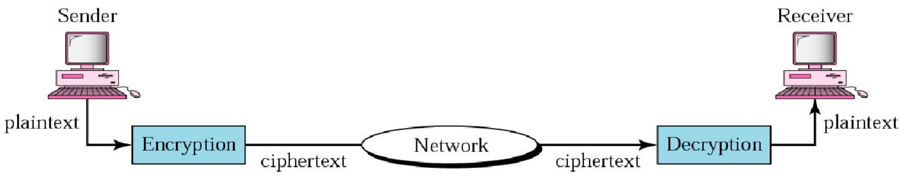
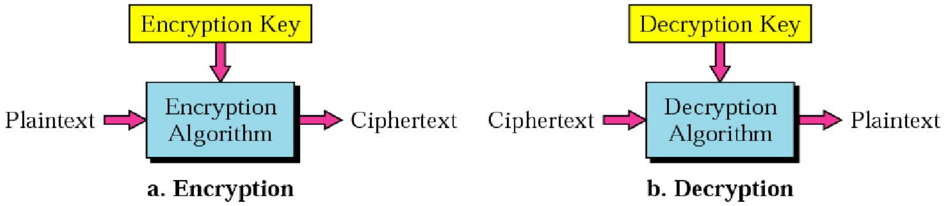


Figure 2 Encryption and decryption



Note:

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

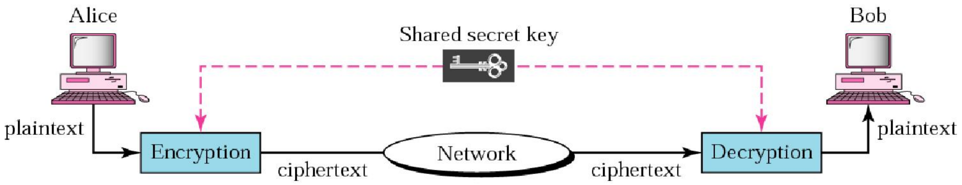
2 Symmetric-Key Cryptography

Traditional Cipher

Block Cipher

Operation Modes

Figure 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 4 Caesar cipher

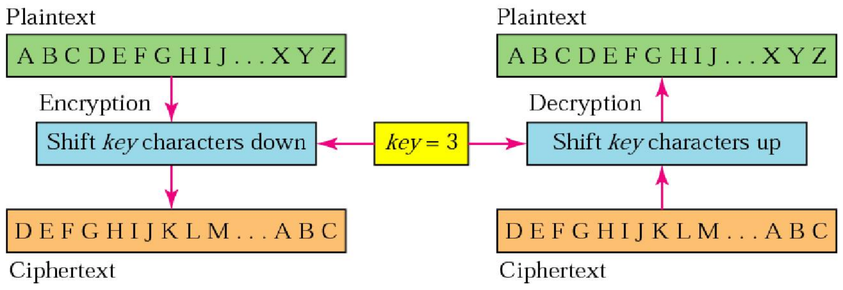
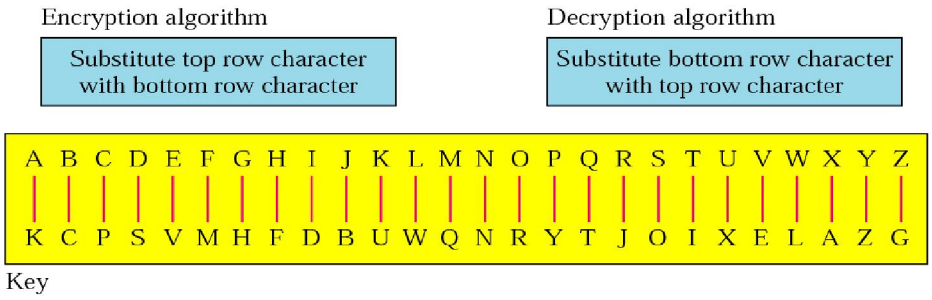

Plaintext
A B C D E F G H I J . . . X Y Z
Encryption
Shift *key* characters down
D E F G H I J K L M . . . A B C
Ciphertext
key = 3
Plaintext
A B C D E F G H I J . . . X Y Z
Decryption
Shift *key* characters up
D E F G H I J K L M . . . A B C
Ciphertext

Figure 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

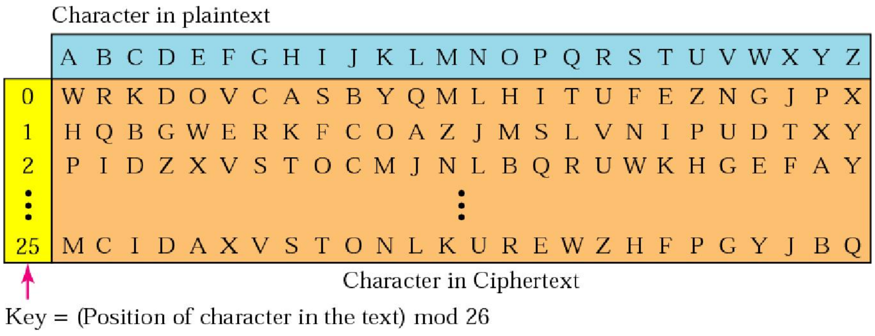
A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
K	C	P	S	V	M	H	F	D	B	U	W	Q	N	R	Y	T	J	O	I	X	E	L	A	Z	G

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 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

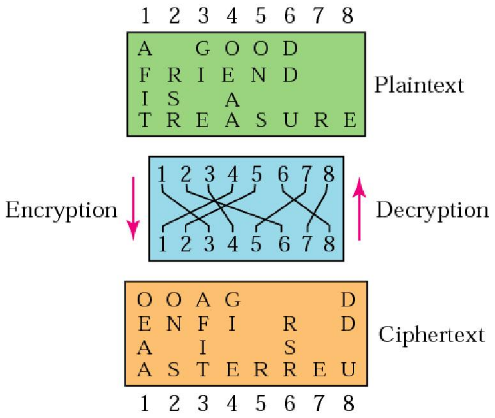
Character in Ciphertext

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 7 Transpositional cipher



Plaintext

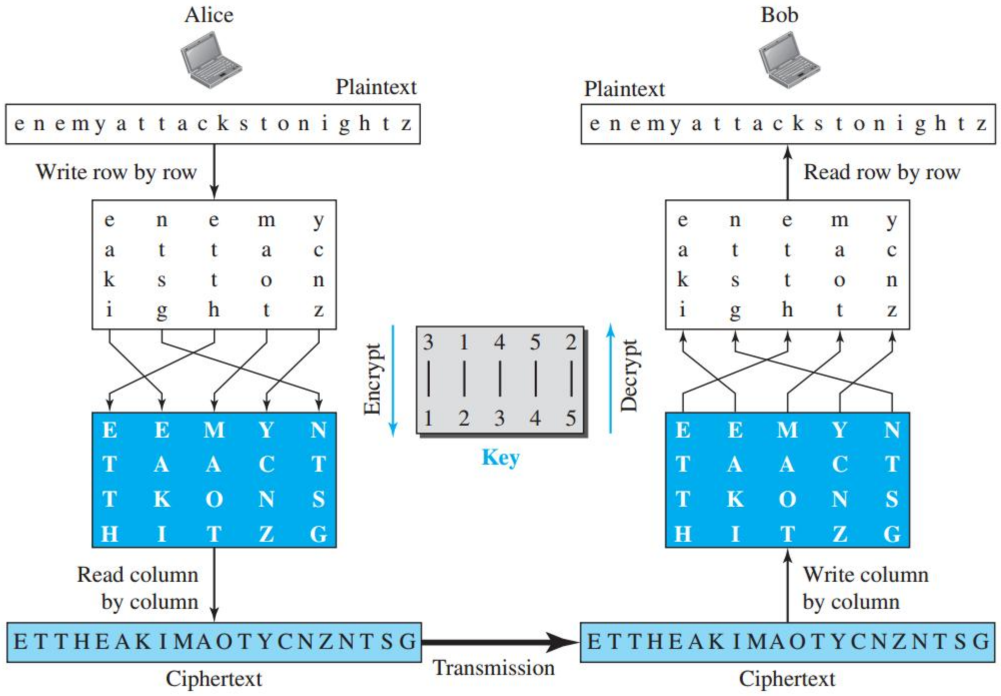
1	2	3	4	5	6	7	8
A		G	O	O	D		
F	R	I	E	N	D		
I	S		A				
T	R	E	A	S	U	R	E

Encryption

Decryption

Ciphertext

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



Alice

Bob

Plaintext

e n e m y a t t a c k s t o n i g h t z

Write row by row

e	n	e	m	y
a	t	t	a	c
k	s	t	o	n
i	g	h	t	z

Encrypt

Decrypt

3	1	4	5	2
1	2	3	4	5

Key

E	E	M	Y	N
T	A	A	C	T
T	K	O	N	S
H	I	T	Z	G

Read column by column

ETTHEAKIMAOTYCNZNTSG

Ciphertext

Transmission

ETTHEAKIMAOTYCNZNTSG

Ciphertext

Write column by column

Read row by row

Plaintext

e n e m y a t t a c k s t o n i g h t z

Figure 8 Block cipher

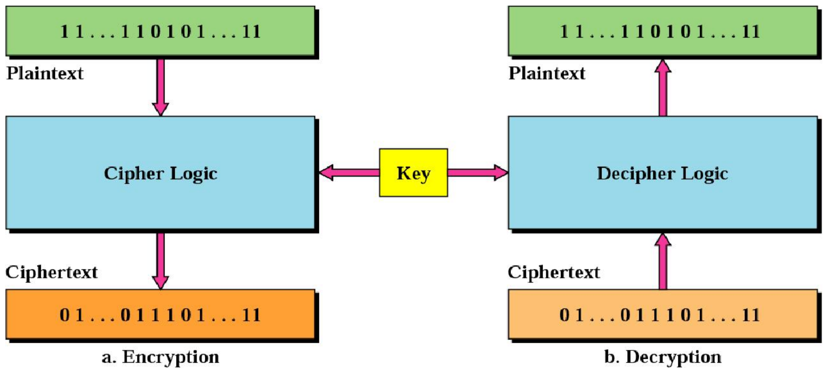


Figure 9 P-box

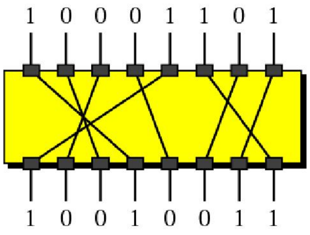
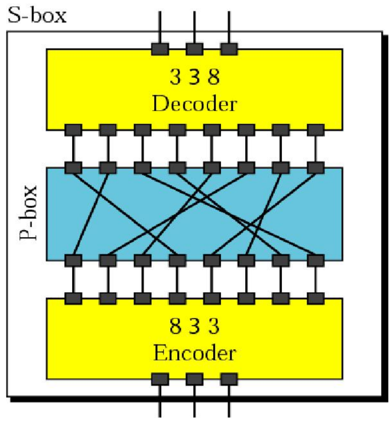


Figure 10 S-box



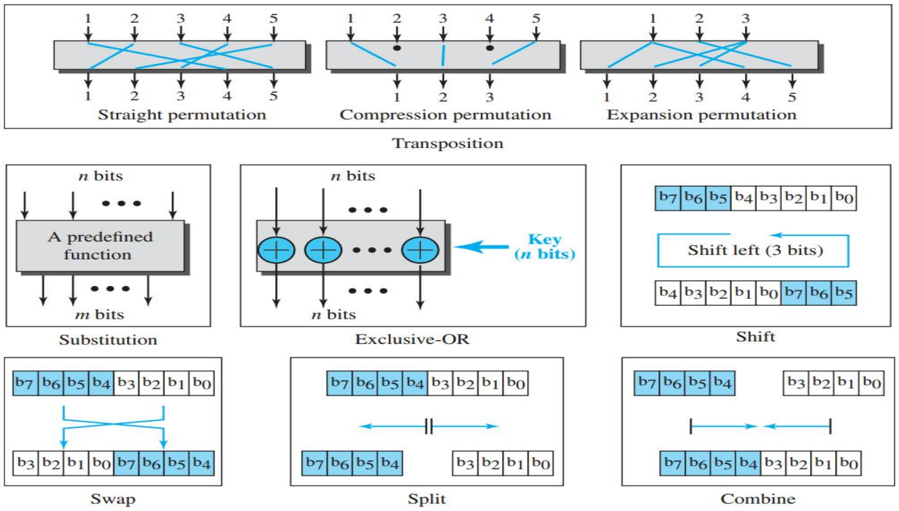


Figure Components of a modern block cipher

Figure 11 Product block

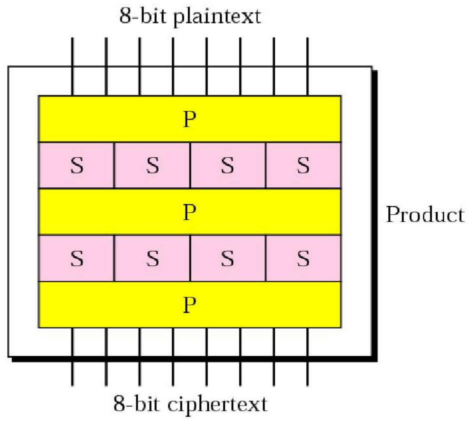


Figure 12 Data Encryption Standard (DES)

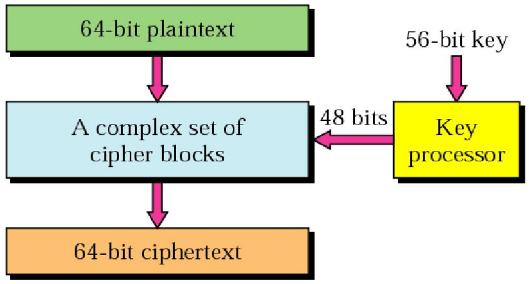


Figure 13 General scheme of DES

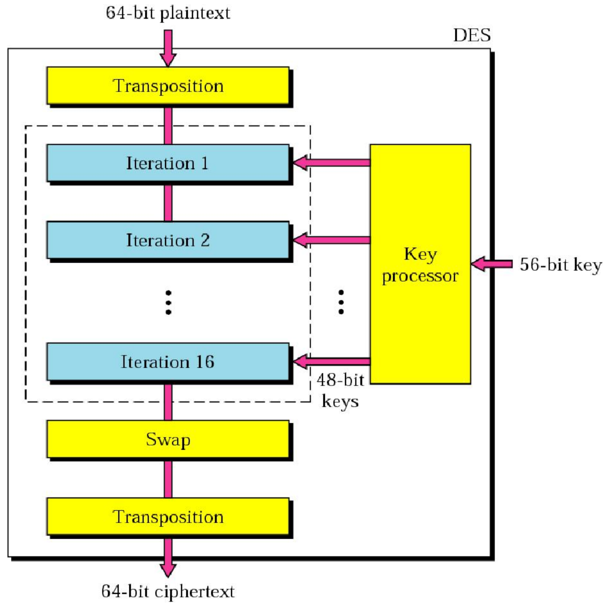


Figure 31.9 *General structure of DES*

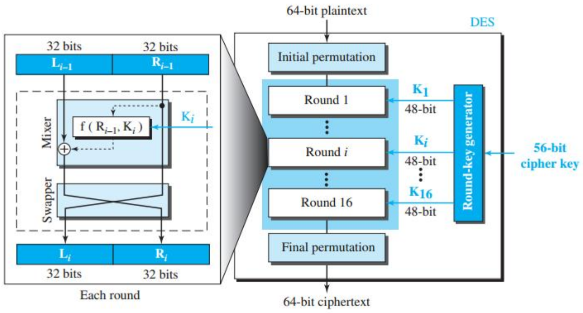


Figure 31.10 *DES function*

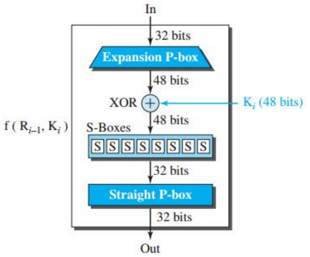


Figure 14 Iteration block

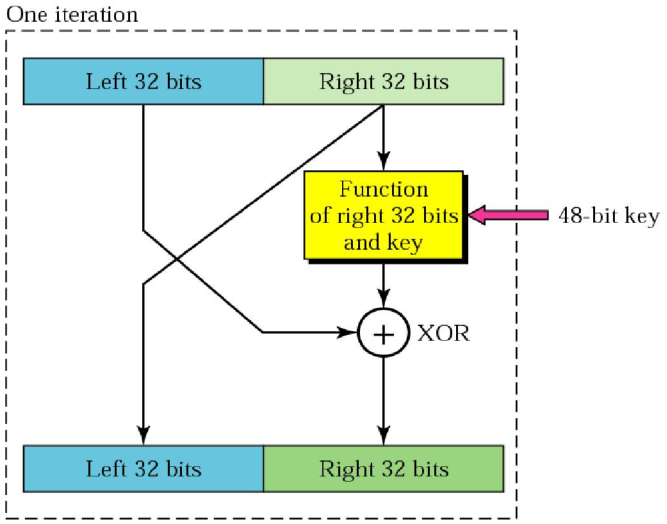


Figure 31.11 *Key generation*

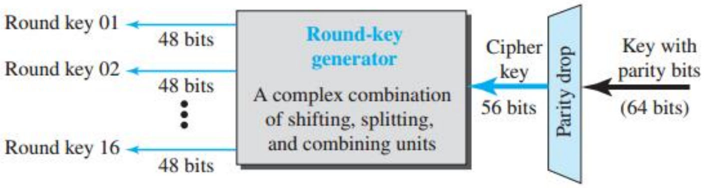
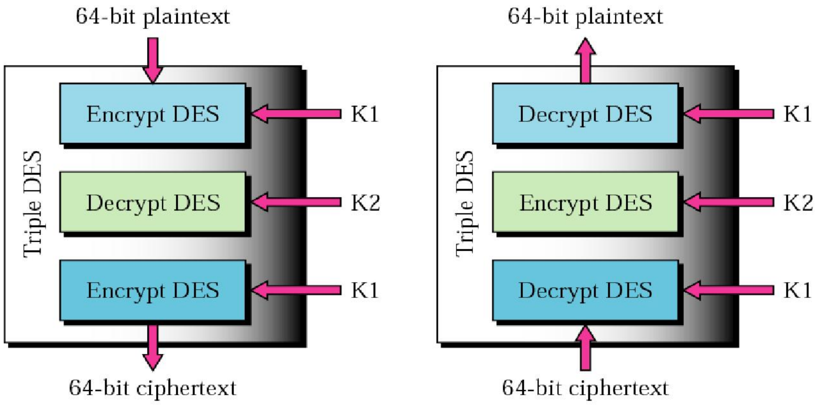


Figure 15 Triple DES



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.

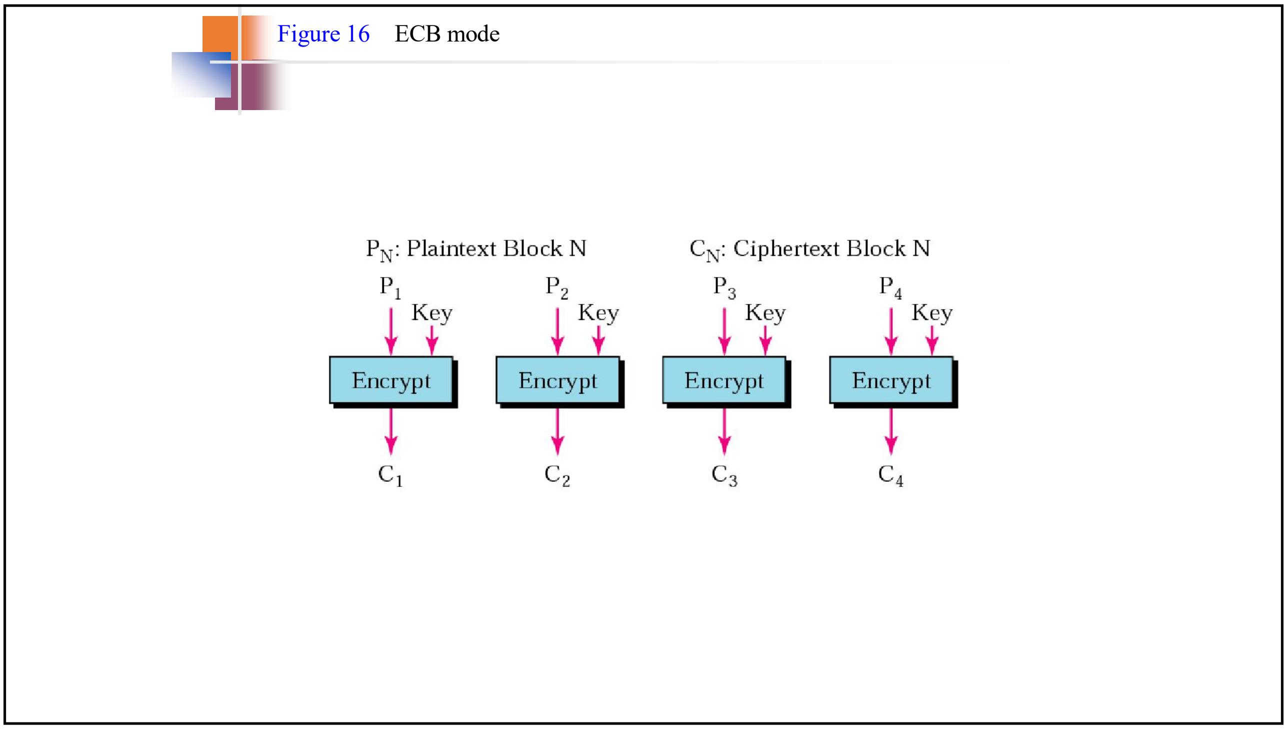


Figure 16 ECB mode

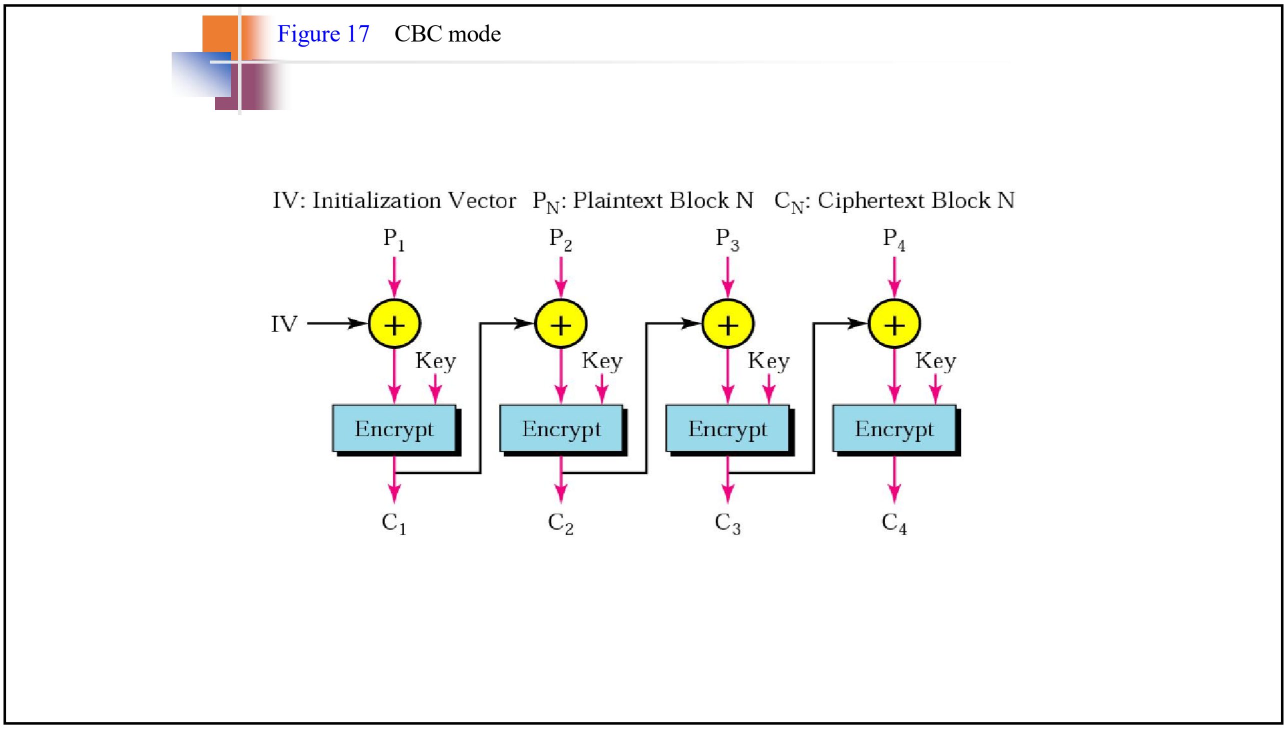


Figure 17 CBC mode

Figure 18 CFM

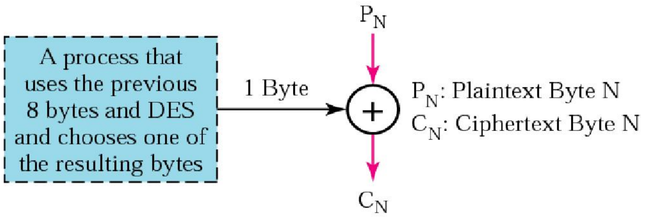
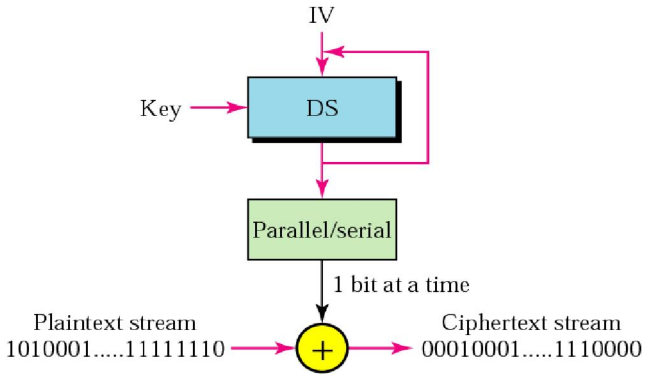

A process that uses the previous 8 bytes and DES and chooses one of the resulting bytes
1 Byte
P_N
+
C_N
P_N: Plaintext Byte N
C_N: Ciphertext Byte N

Figure 19 CSM



3 Public-Key Cryptography

RSA (Rivest, Shamir, and Adleman)

Choosing Public and Private Keys

Figure 20 Public-key cryptography

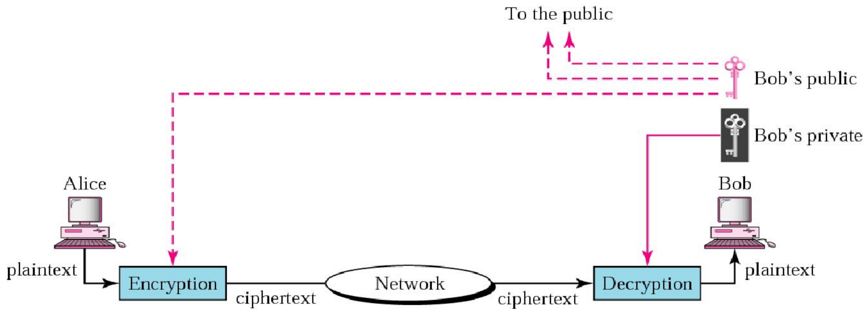
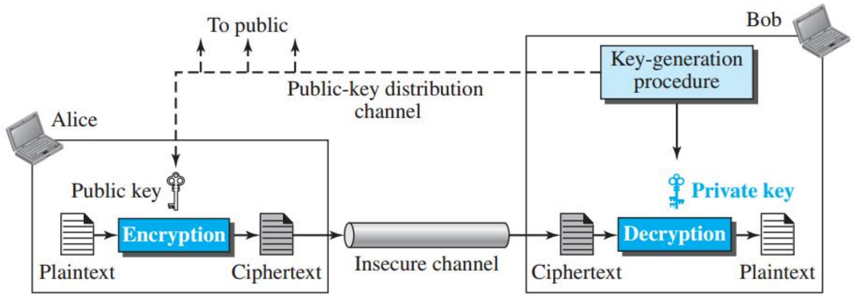
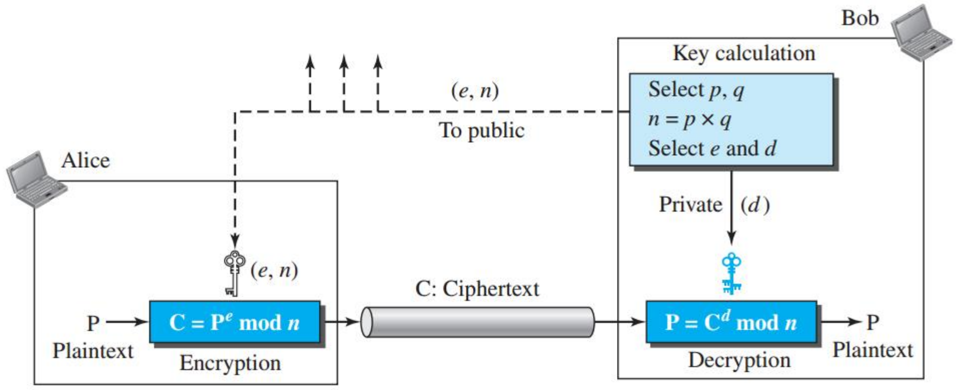


Figure *General idea of asymmetric-key cryptosystem*



Note:

Public-key algorithms are more efficient for short messages.



Plaintext: 5

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

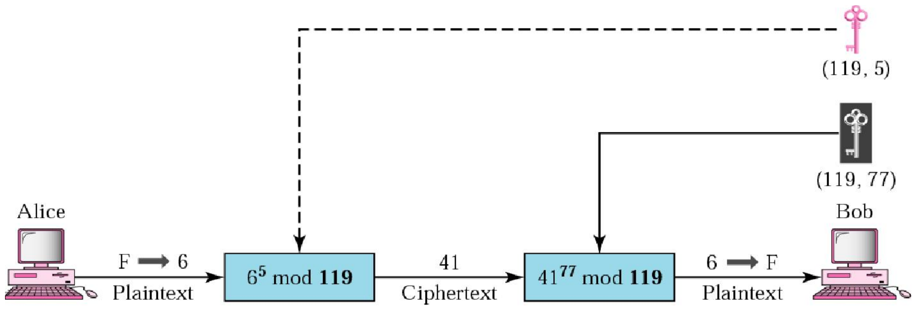
Ciphertext: 26

Ciphertext: 26

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

Plaintext: 5

Figure 21 RSA



3 MD, MAC

Message Digest

Message Authentication Code

Figure *Message and digest*

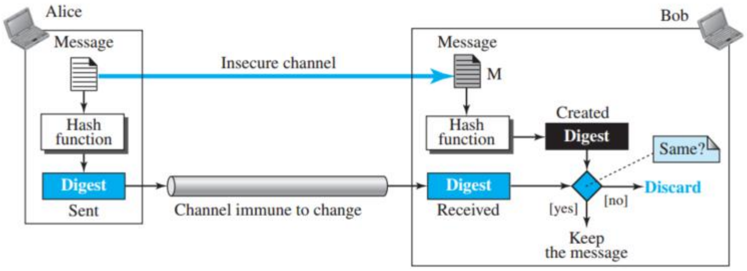
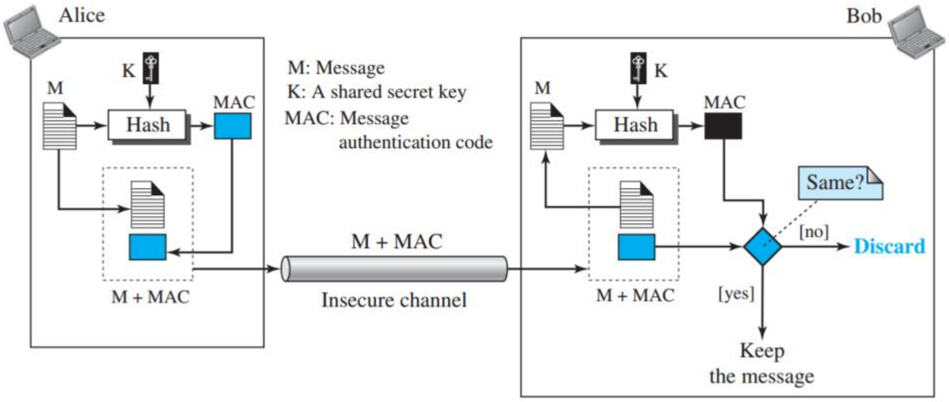


Figure *Message authentication code*



Note:

A MAC provides message integrity and message authentication using a combination of a hash function and a secret key..