Cryptography and Network Security

Dr. Rafiqul Islam

Classical Encryption Techniques

- Symmetric Cipher Techniques
- Asymmetric Cipher Techniques

Symmetric Cipher

- **Plaintext**: Input Text
- **Encryption algorithm**: The encryption algorithm performs various substitutions and transformations on the plaintext.
- **Secret key**: The secret key is also input to the encryption algorithm. The key is a value independent of the plaintext and of the algorithm.
- **Cipher text**: This is the scrambled message produced as output. It depends on the plaintext and the secret key. The ciphertext is an apparently random stream of data and, as it stands, is unintelligible.
- **Decryption algorithm**: This is essentially the encryption algorithm run in reverse. It takes the ciphertext and the secret key and produces the original plaintext.

Symmetric Cipher

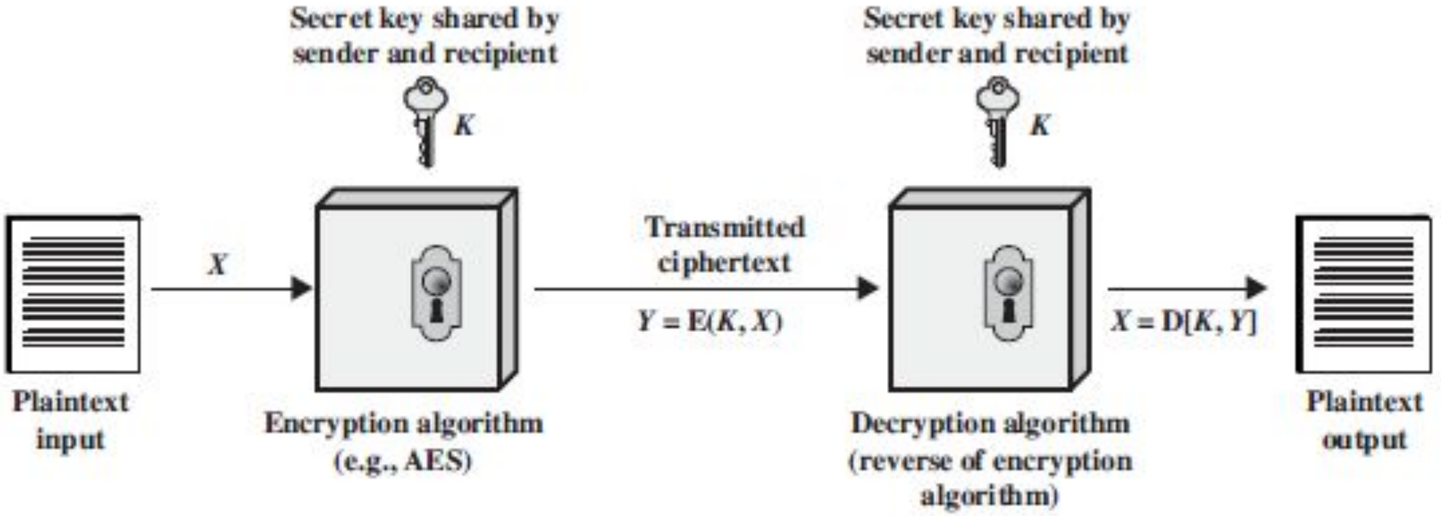

Secret key shared by sender and recipient
K
Secret key shared by sender and recipient
K
X
Transmitted ciphertext
Y = E(K, X)
X = D[K, Y]
Plaintext input
Encryption algorithm (e.g., AES)
Decryption algorithm (reverse of encryption algorithm)
Plaintext output

Figure 2.1 Simplified Model of Symmetric Encryption

Different Types of Ciphers

- Traditional Ciphers
- Modern Ciphers
- Asymmetric-Key Ciphers

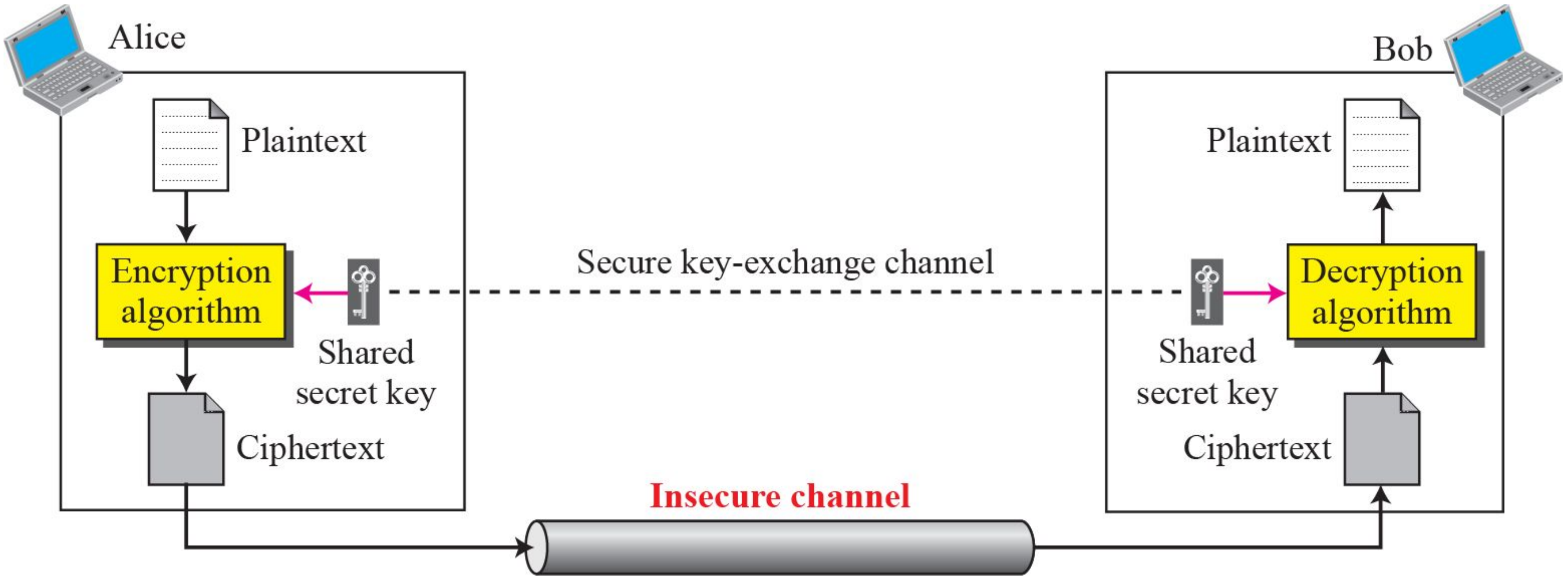
Traditional ciphers

- Traditional ciphers are called symmetric-key ciphers (or secret-key ciphers)
- because the same key is used for encryption and decryption and
- the key can be used for bidirectional communication.

Topics Discussed in the Section

- ✔ Key
- ✔ Substitution Ciphers
- ✔ Transposition Ciphers
- ✔ Stream and Block Ciphers

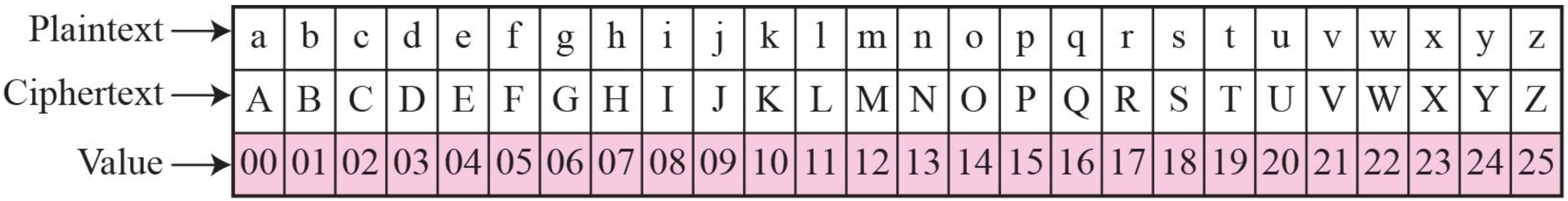
General idea of traditional cipher



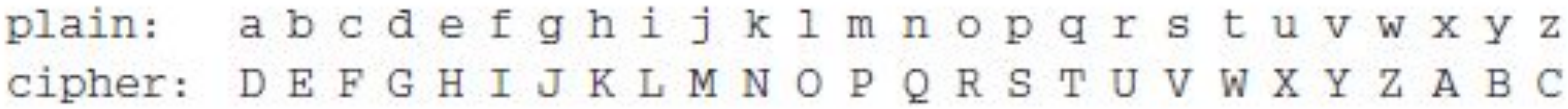
substitution cipher

- A substitution cipher replaces one symbol with another

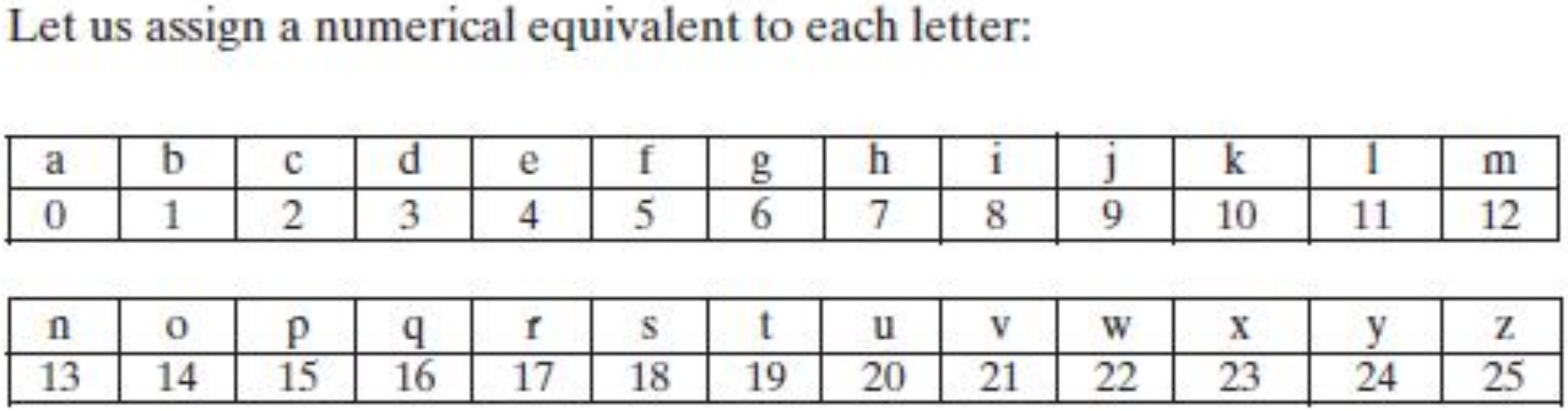
Representation of characters in modulo 26



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
Ciphertext →	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
Value →	00	01	02	03	04	05	06	07	08	09	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25



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



Let us assign a numerical equivalent to each letter:

a	b	c	d	e	f	g	h	i	j	k	l	m
0	1	2	3	4	5	6	7	8	9	10	11	12

n	o	p	q	r	s	t	u	v	w	x	y	z
13	14	15	16	17	18	19	20	21	22	23	24	25

Contd.

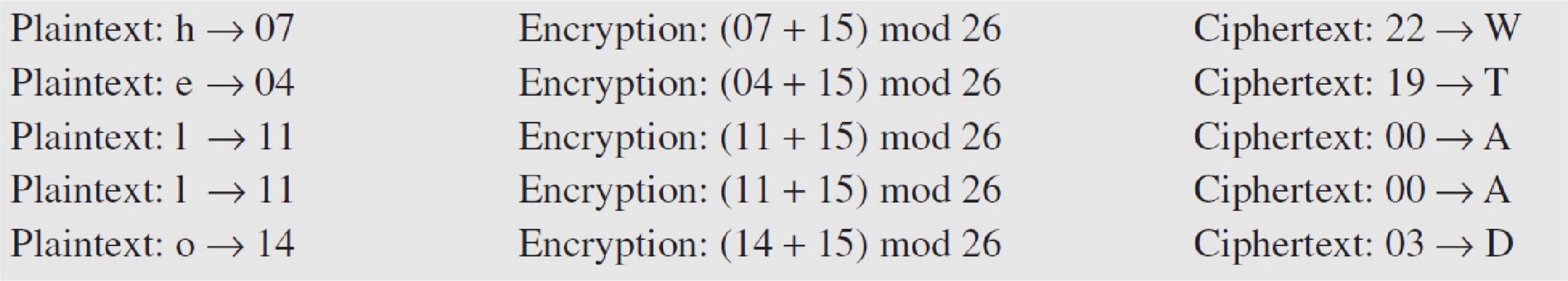
- In additive cipher, the plaintext, ciphertext, and key are integers in modulo 26.
- $C = (P+K) \mod 26$
- $P = (C-K) \mod 26$

Example 01

Use the additive cipher with key = 15 to encrypt the message “hello”.

Solution

We apply the encryption algorithm to the plaintext, character by character. The result is “WTAAD”. Note that the cipher is mono alphabetic because two instances of the same plaintext character (ls) are encrypted as the same character (A).



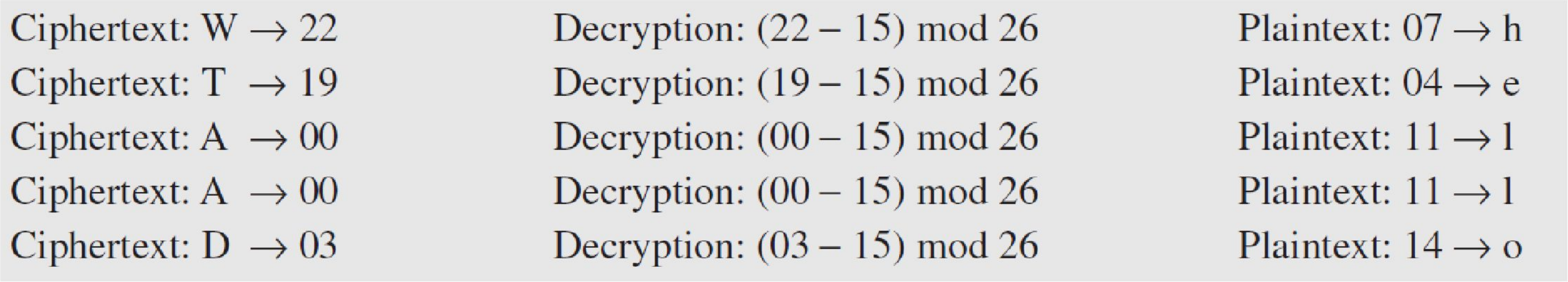
Plaintext: h → 07	Encryption: (07 + 15) mod 26	Ciphertext: 22 → W
Plaintext: e → 04	Encryption: (04 + 15) mod 26	Ciphertext: 19 → T
Plaintext: l → 11	Encryption: (11 + 15) mod 26	Ciphertext: 00 → A
Plaintext: l → 11	Encryption: (11 + 15) mod 26	Ciphertext: 00 → A
Plaintext: o → 14	Encryption: (14 + 15) mod 26	Ciphertext: 03 → D

Example 01

Use the additive cipher with key = 15 to decrypt the message “WTAAD”.

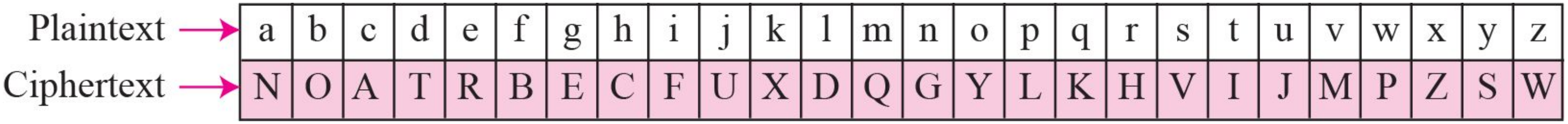
Solution

We apply the decryption algorithm to the plaintext character by character. The result is “hello”. Note that the operation is in modulo 26, which means that we need to add 26 to a negative result (for example −15 becomes 11).



Ciphertext: W → 22	Decryption: (22 – 15) mod 26	Plaintext: 07 → h
Ciphertext: T → 19	Decryption: (19 – 15) mod 26	Plaintext: 04 → e
Ciphertext: A → 00	Decryption: (00 – 15) mod 26	Plaintext: 11 → l
Ciphertext: A → 00	Decryption: (00 – 15) mod 26	Plaintext: 11 → l
Ciphertext: D → 03	Decryption: (03 – 15) mod 26	Plaintext: 14 → o

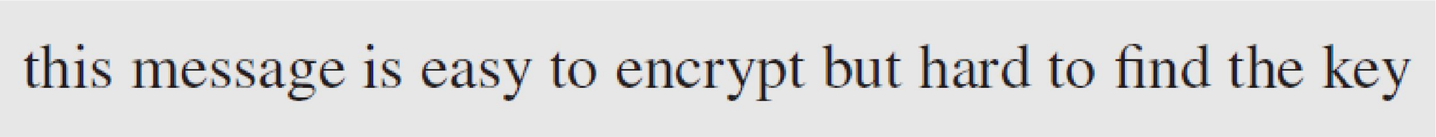
An example key for mono-alphabetic substitution cipher



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

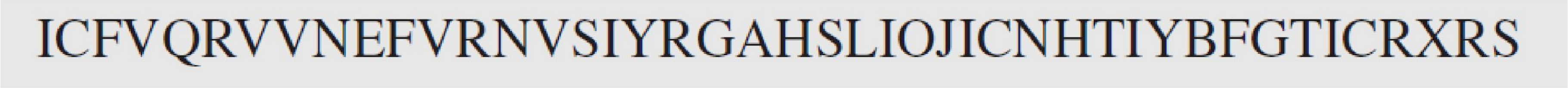
Example

- We can use the key to encrypt the message



this message is easy to encrypt but hard to find the key

The ciphertext is

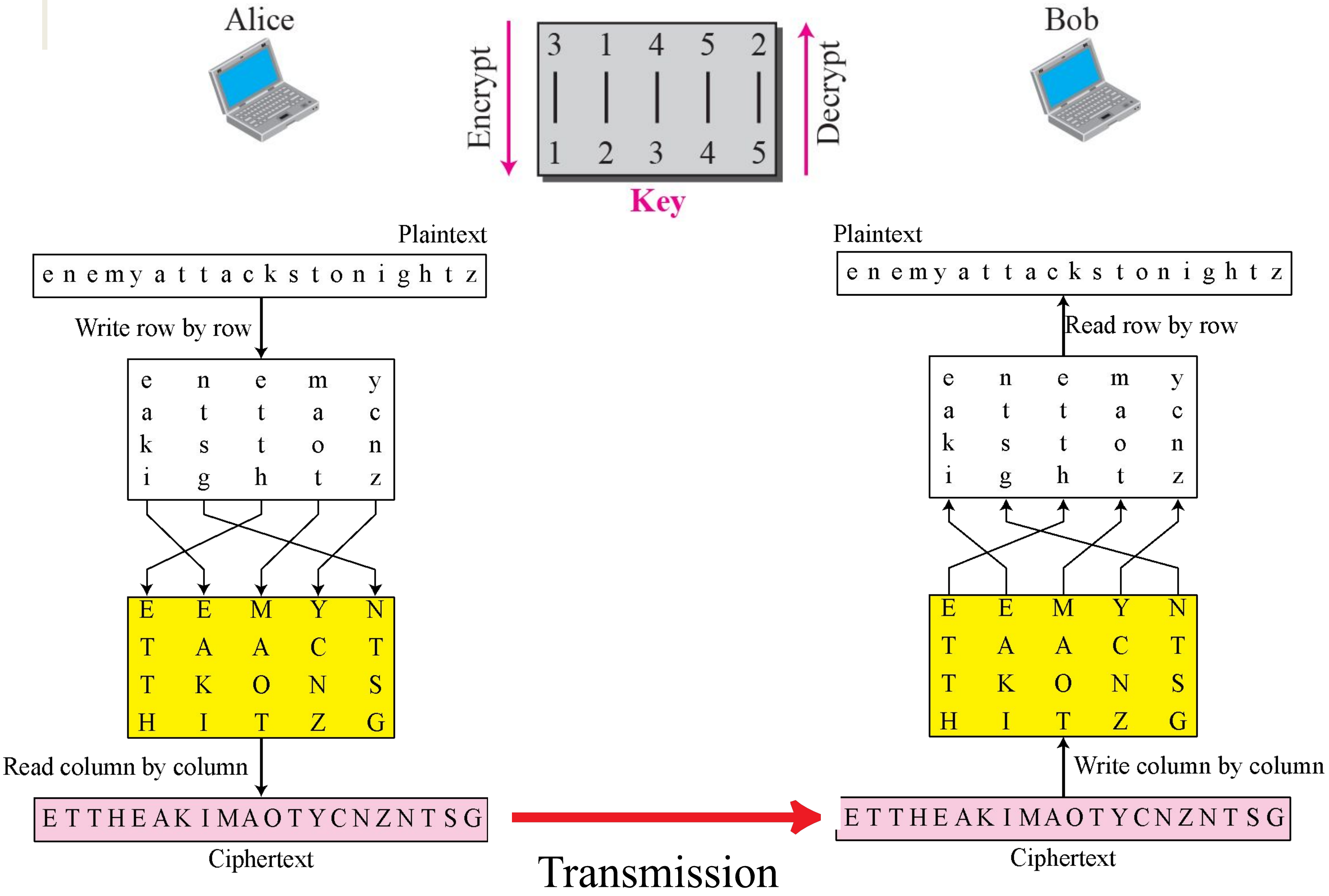


ICFVQRVVNEFVRNVSIYRGAHSLIOJICNHTIYBFGTICRXRS

Transposition Cipher

- A transposition cipher reorders symbols

Transposition cipher



Alice

Bob

Encrypt

3	1	4	5	2
1	2	3	4	5

Decrypt

Key

Plaintext

enemyattackstonightz

Write row by row

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

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

Plaintext

enemyattackstonightz

Read row by row

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

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

Write column by column

ETTHEAKIMAOTYCNZNTSG

Ciphertext

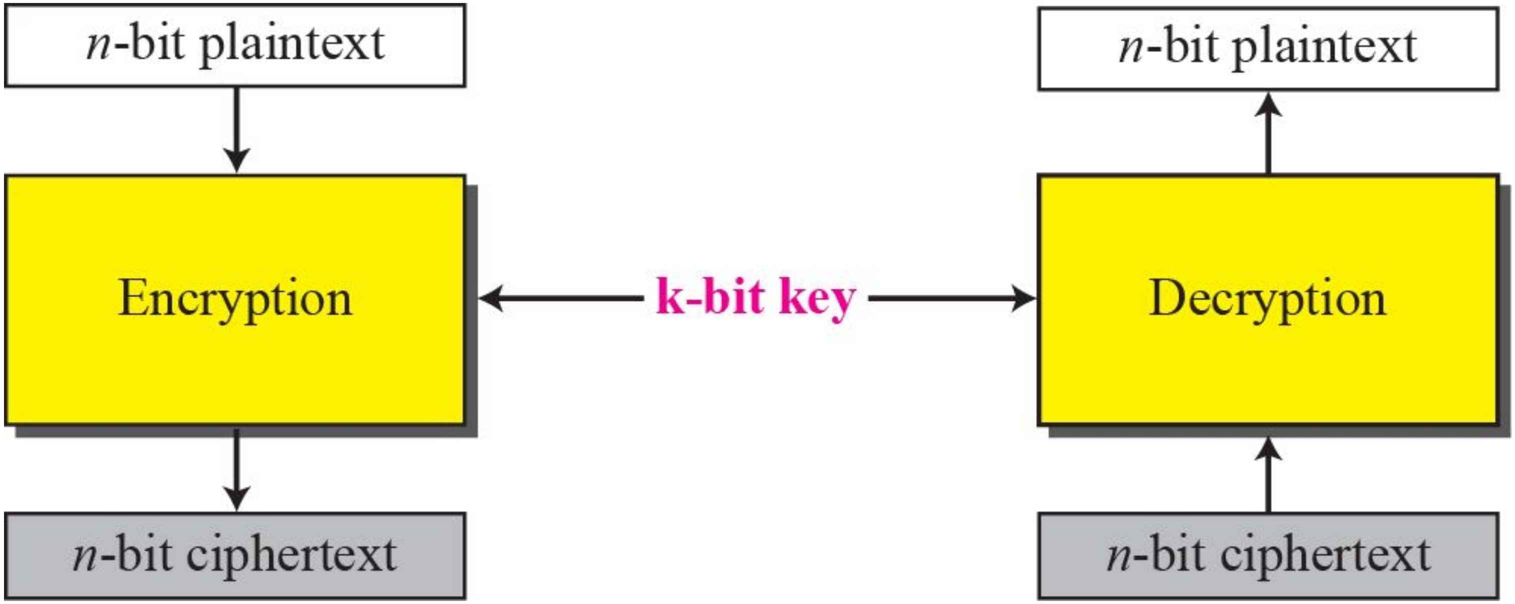
Modern ciphers

- The traditional symmetric-key ciphers that we have studied so far are character-oriented ciphers.
- With the advent of the computer, we need bit-oriented ciphers.
- This is because the information to be encrypted is not just text; it can also consist of numbers, graphics, audio, and video data.
- It is convenient to convert these types of data into a stream of bits, to encrypt the stream, and then to send the encrypted stream.
- A modern block cipher can be either a block cipher or a stream cipher.

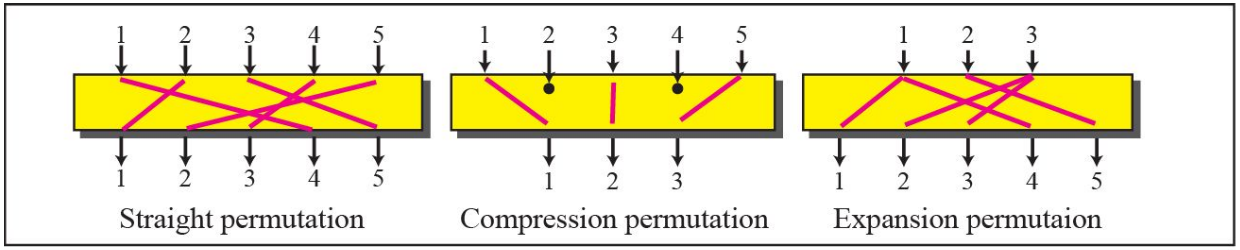
Topics Discussed in the Section

- Modern Block Ciphers
- Data Encryption Standard (DES)
- Modern Stream Ciphers

A modern block cipher



Components of a modern block cipher

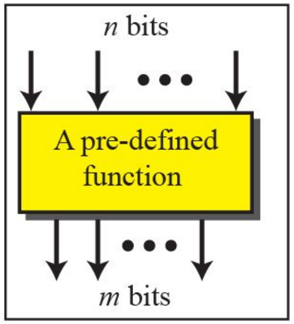


Straight permutation

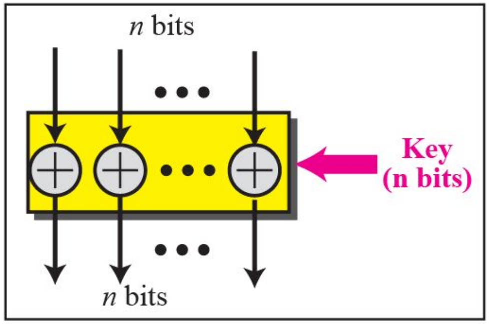
Compression permutation

Expansion permutaion

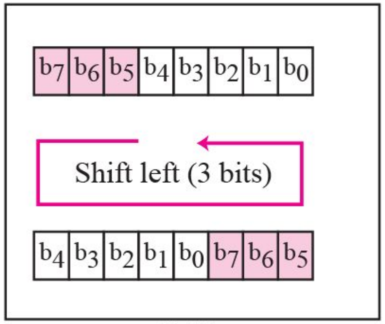
Transposition



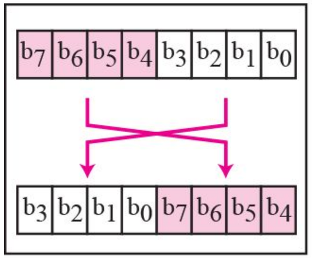
Substitution



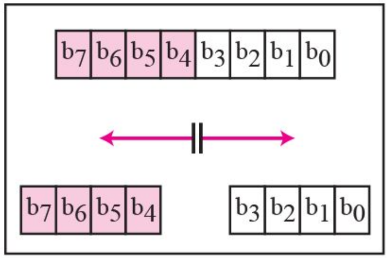
Exclusive-Or


b_7 b_6 b_5 b_4 b_3 b_2 b_1 b_0
Shift left (3 bits)
b_4 b_3 b_2 b_1 b_0 b_7 b_6 b_5

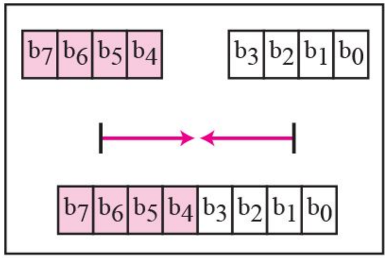
Shift


b_7 b_6 b_5 b_4 b_3 b_2 b_1 b_0
b_3 b_2 b_1 b_0 b_7 b_6 b_5 b_4

Swap

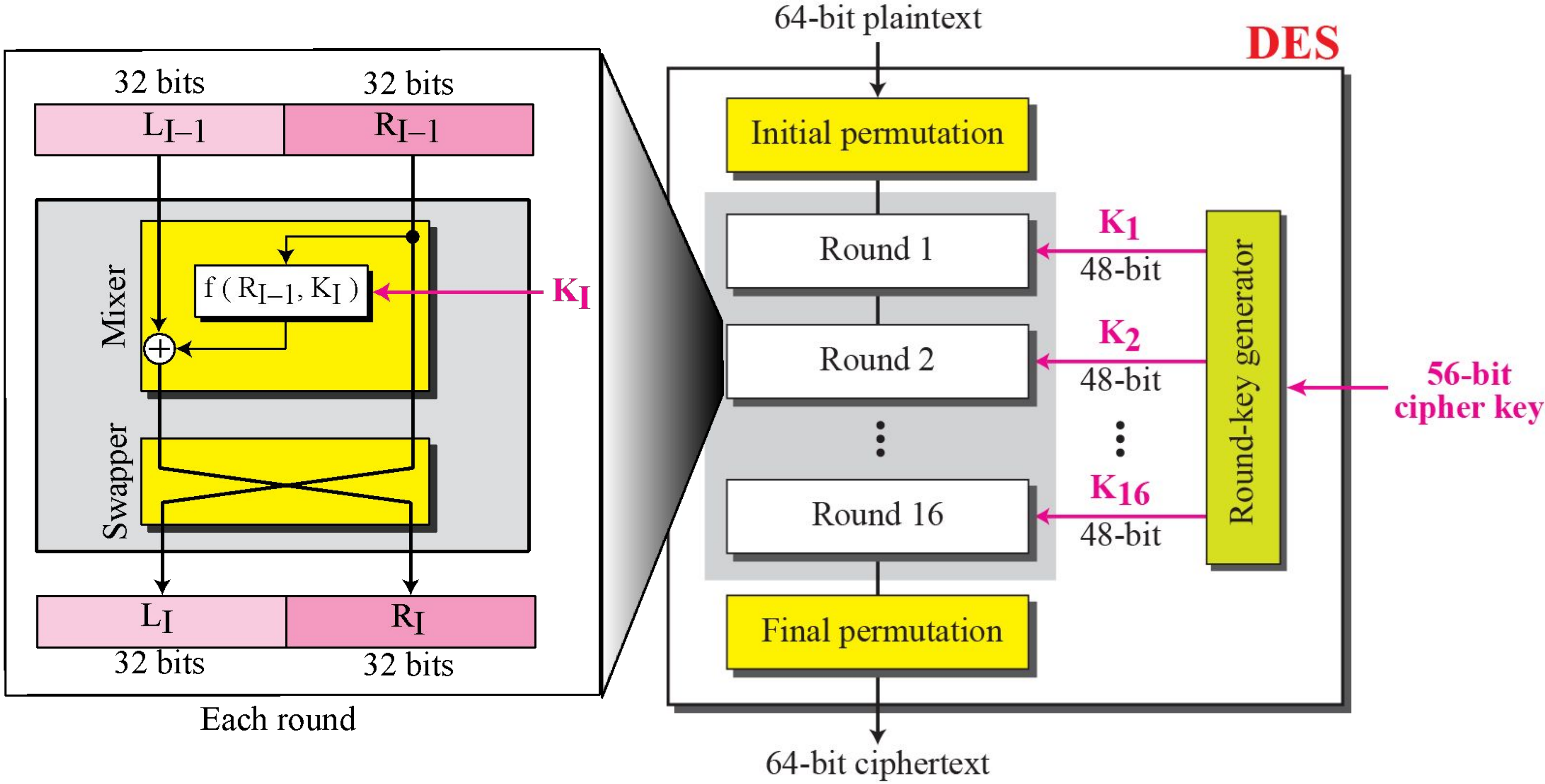


Split

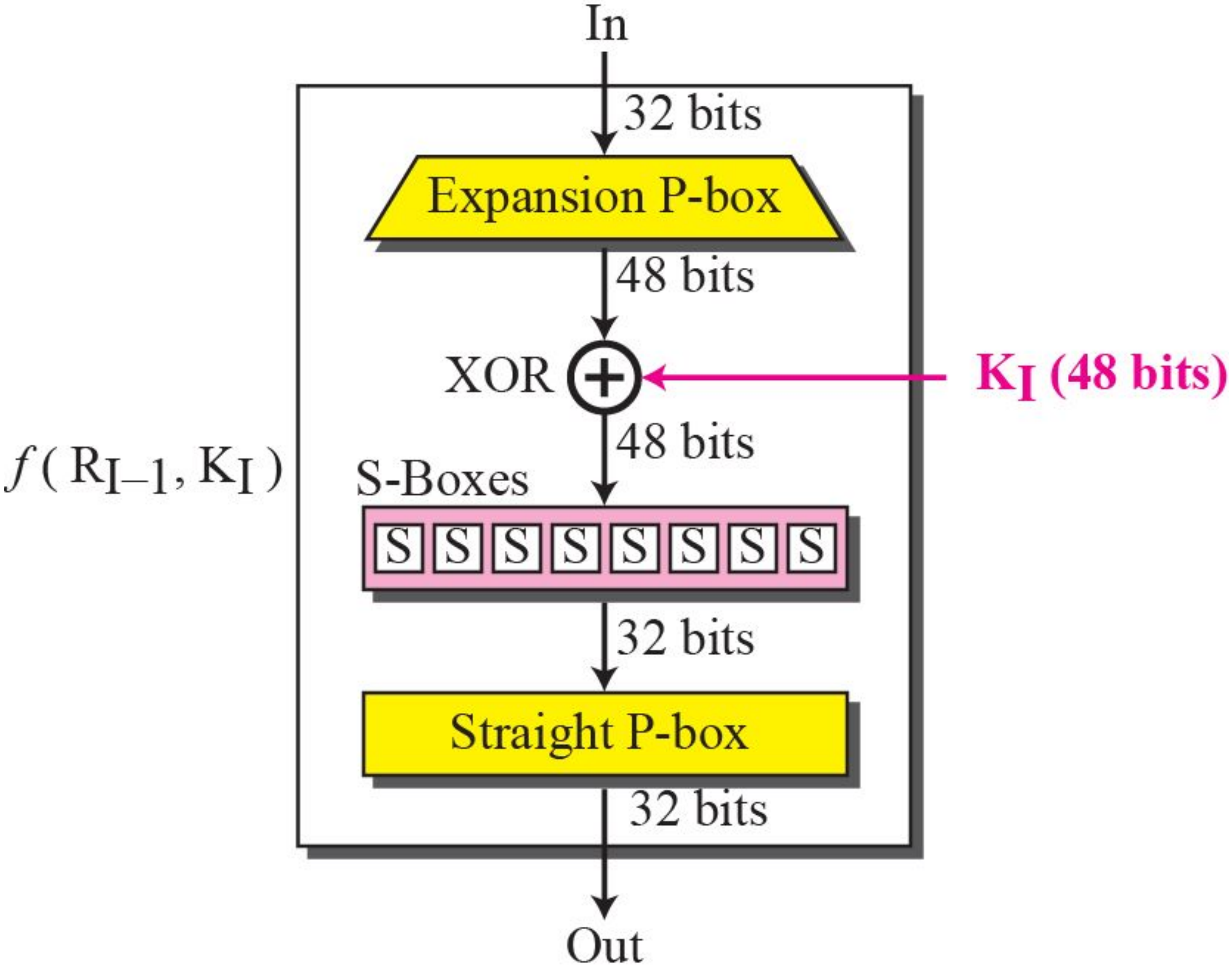


Combine

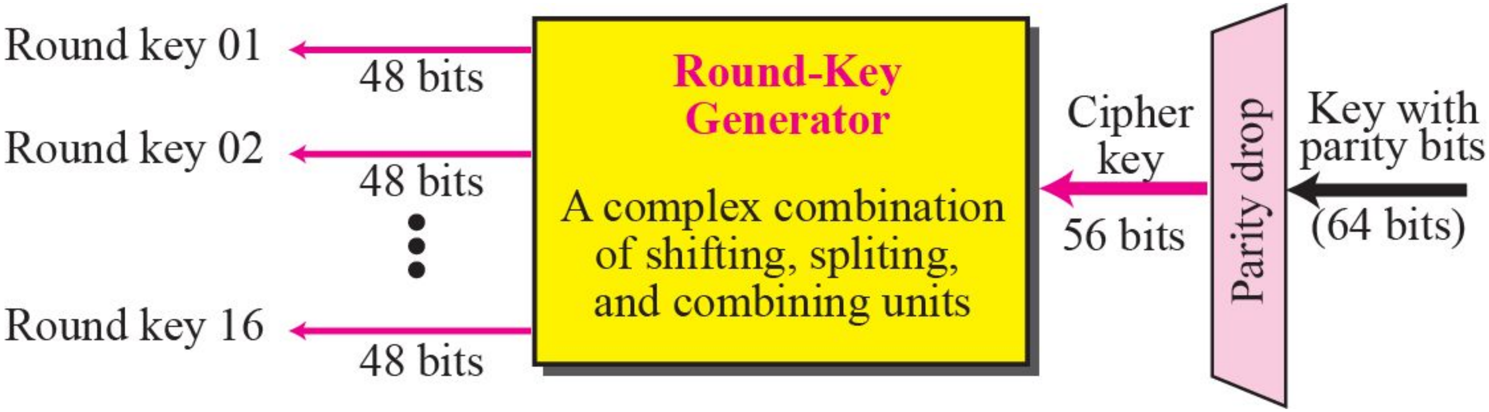
General structure of DES



DES function

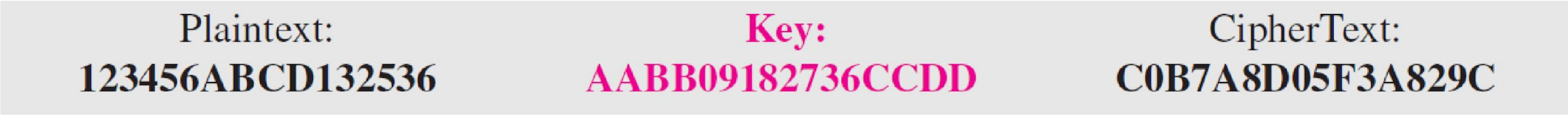


Key generation



Example 04

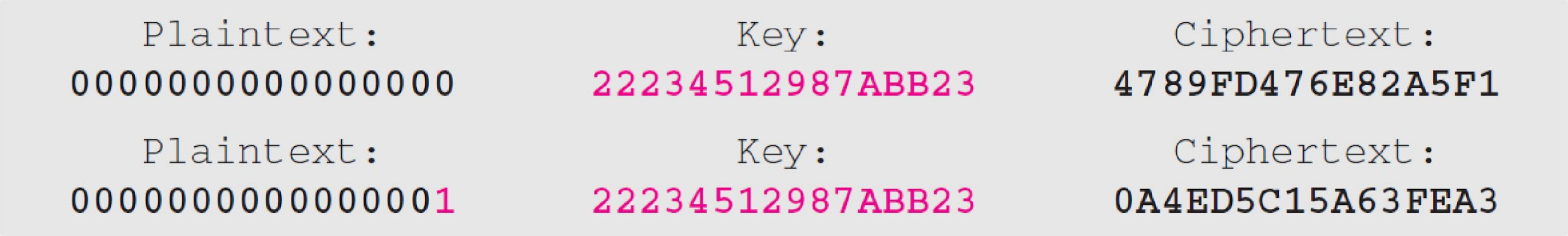
- We choose a random plaintext block, a random key, and a computer program to determine what the cipher text block would be (all in hexadecimal):



Plaintext:	**Key:**	CipherText:
123456ABCD132536	**AABB09182736CCDD**	**C0B7A8D05F3A829C**

Example 05

- To check the effectiveness of DES, when a single bit is changed in the input, let us use two different plaintexts with only one single bit difference.
- The two cipher texts are completely different without even changing the key:



Plaintext:	Key:	Ciphertext:
0000000000000000	22234512987ABB23	4789FD476E82A5F1
Plaintext:	Key:	Ciphertext:
0000000000000001	22234512987ABB23	0A4ED5C15A63FEA3

Although the two plaintext blocks differ only in the rightmost bit, the ciphertext blocks differ in 29 bits.

End Chapter 2

- Questions?