



**TRƯỜNG ĐẠI HỌC BÁCH KHOA HÀ NỘI**  
**VIỆN ĐIỆN TỬ - VIỄN THÔNG**

---

**BỘ MÔN ĐIỆN TỬ HÀNG KHÔNG VŨ TRỤ**

**Môn học:**


# LÝ THUYẾT MẬT MÃ

Giảng viên: TS. Hán Trọng Thanh  
 Email: [httbkhn@gmail.com](mailto:httbkhn@gmail.com)

---

4/7/2016

1



## Mục tiêu học phần

---

Cung cấp kiến thức cơ bản về mật mã đảm bảo an toàn và bảo mật thông tin:

- ✓ Các phương pháp mật mã khóa đối xứng; Phương pháp mật mã khóa công khai;
- ✓ Các hệ mật dòng và vấn đề tạo dãy giả ngẫu nhiên;
- ✓ Lược đồ chữ ký số Elgamal và chuẩn chữ ký số ECDSA;
- ✓ Độ phức tạp xử lý và độ phức tạp dữ liệu của một tấn công cụ thể vào hệ thống mật mã;
- ✓ Đặc trưng an toàn của phương thức mã hóa;
- ✓ Thăm mã tuyến tính, thăm mã vi sai và các vấn đề về xây dựng hệ mã bảo mật cho các ứng dụng.

---

2



## Nội Dung

---

1. Chương 1. Tổng quan
2. Chương 2. Mật mã khóa đối xứng
3. Chương 3. Mật mã khóa công khai
4. Chương 4. Hàm băm và chữ ký số
5. Chương 5. Dây giả ngẫu nhiên và hệ mật dòng
6. Chương 6. Kỹ thuật quản lý khóa

4/7/2016

3



## Tài liệu tham khảo

---

1. A. J. Menezes, P. C. Van Oorschot, S. A. Vanstone, *Handbook of applied cryptography*, CRC Press 1998.
2. B. Schneier, *Applied Cryptography*. John Wiley Press 1996.
3. M. R. A. Huth, *Secure Communicating Systems*, Cambridge University Press 2001.
4. W. Stallings, *Network Security Essentials, Applications and Standards*, Prentice Hall. 2000.

4



## Nhiệm vụ của Sinh viên

---

1. Chấp hành nội quy lớp học
2. Thực hiện đầy đủ bài tập
3. Nắm vững ngôn ngữ lập trình Matlab




---

5



## Chương 2. Mật mã khóa đối xứng

---

- 2.1. Giới thiệu sơ lược mật mã khóa đối xứng cổ điển
- 2.2. Một số hệ mật mã khóa đối xứng cổ điển
- 2.3. Sơ lược hệ mật mã dòng và hệ mật mã khối
- 2.4. Cơ sở toán học cho hệ mật mã khóa đối xứng hiện đại.
- 2.5 Sơ lược hệ mật mã đối xứng hiện đại

---

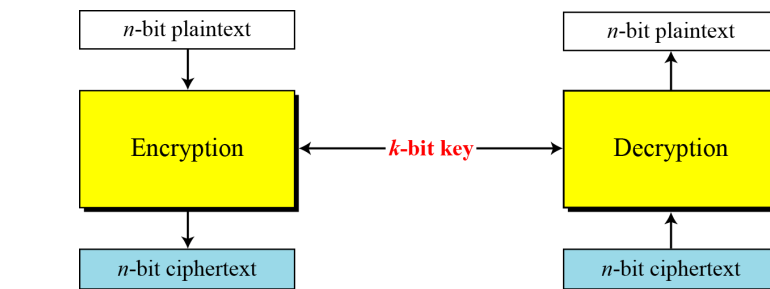
6



## 2.5. Sơ lược hệ mật mã đối xứng hiện đại

### 2.5.1. Hệ mật mã khối hiện đại

*A symmetric-key modern block cipher encrypts an  $n$ -bit block of plaintext or decrypts an  $n$ -bit block of ciphertext. The encryption or decryption algorithm uses a  $k$ -bit key.*



7



## 2.5. Sơ lược hệ mật mã đối xứng hiện đại

### 2.5.1. Hệ mật mã khối hiện đại

A modern block cipher can be designed to act as a substitution cipher or a transposition cipher.

**To be resistant to exhaustive-search attack,  
a modern block cipher needs to be  
designed as a substitution cipher.**

8



## 2.5. Sơ lược hệ mật mã đối xứng hiện đại

### 2.5.1. Hệ mật mã khối hiện đại

#### *Full-Size Key Substitution Block Ciphers*

*A full-size key substitution cipher does not transpose bits; it substitutes bits. We can model the substitution cipher as a permutation if we can decode the input and encode the output.*



*A substitution block cipher model as a permutation*

9



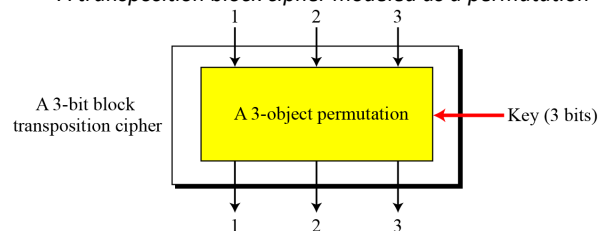
## 2.5. Sơ lược hệ mật mã đối xứng hiện đại

### 2.5.1. Hệ mật mã khối hiện đại

#### *Full-Size Key Transposition Block Ciphers*

*In a full-size key transposition cipher we need to have  $n!$  possible keys, so the key should have  $\text{Log}_2 n!$  bits.*


*A transposition block cipher modeled as a permutation*



$\{[1\ 2\ 3], [1\ 3\ 2], [2\ 1\ 3], [2\ 3\ 1], [3\ 1\ 2], [3\ 2\ 1]\}$

The set of permutation tables with  $3! = 6$  elements

10



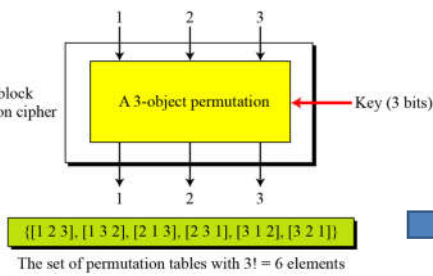
## 2.5. Sơ lược hệ mật mã đối xứng hiện đại

---

### 2.5.1. Hệ mật mã khối hiện đại

*A substitution block cipher model as a permutation*

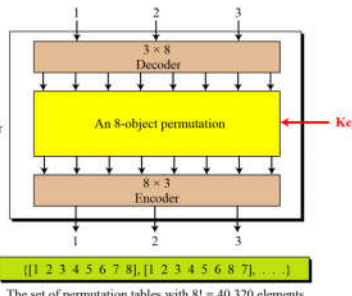
A 3-bit block transposition cipher



The set of permutation tables with  $3! = 6$  elements


➔

A 3-bit block substitution cipher



The set of permutation tables with  $8! = 40,320$  elements

11




## 2.5. Sơ lược hệ mật mã đối xứng hiện đại

---

### 2.5.1. Hệ mật mã khối hiện đại

**Show the model and the set of permutation tables for a 3-bit block substitution cipher.**




**The model and the set of permutation table?**

**-> Using decoder before permutation and coder after permutation!**

**The key is also much longer,  $\lceil \log_2 40,320 \rceil = 16$  bits.**

12

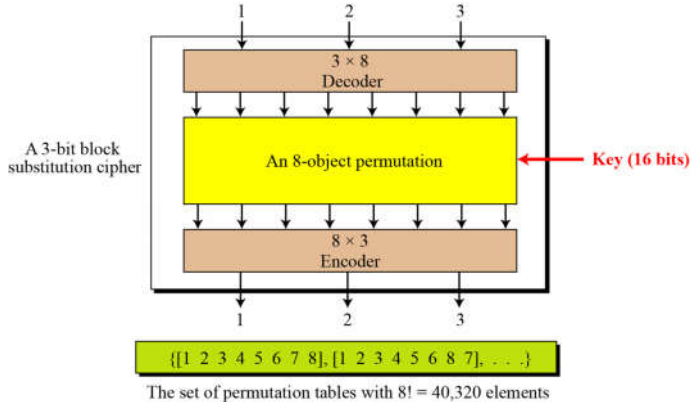


## 2.5. Sơ lược hệ mật mã đối xứng hiện đại

---


### 2.5.1. Hệ mật mã khối hiện đại

*A substitution block cipher model as a permutation*



The set of permutation tables with  $8! = 40,320$  elements

13



## 2.5. Sơ lược hệ mật mã đối xứng hiện đại

---

### 2.5.1. Hệ mật mã khối hiện đại

*Full-Size Key Substitution Block Ciphers*

A partial-key cipher is a group under the composition operation if it is a subgroup of the corresponding full-size key cipher.

A full-size key  $n$ -bit transposition cipher or a substitution block cipher can be modeled as a permutation, but their key sizes are different:

- ☐ Transposition: the key is  $\lceil \log_2 n! \rceil$  bits long.
- ☐ Substitution: the key is  $\lceil \log_2(2^n)! \rceil$  bits long.

14



## 2.5. Sơ lược hệ mật mã đối xứng hiện đại

### 2.5.1. Hệ mật mã khối hiện đại

#### Components of a Modern Block Cipher

*Modern block ciphers normally are keyed substitution ciphers in which the key allows only partial mappings from the possible inputs to the possible outputs.*

#### P-Boxes

*A P-box (**P**ermutation **B**ox) parallels the traditional transposition cipher for characters. It **transposes bits**.*

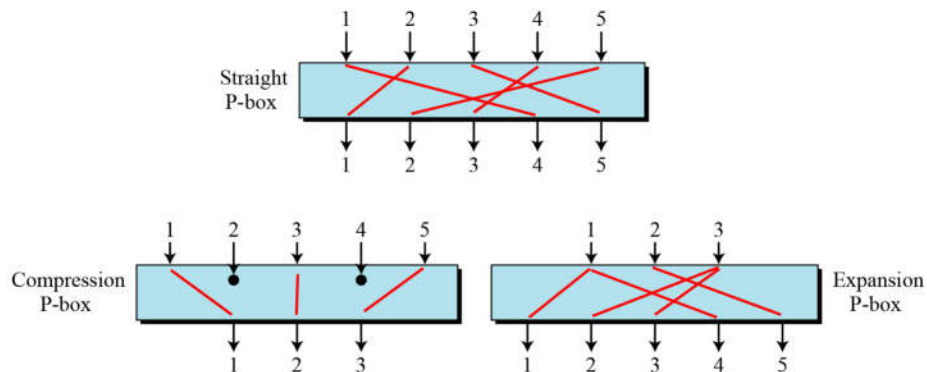
15



## 2.5. Sơ lược hệ mật mã đối xứng hiện đại

### 2.5.1. Hệ mật mã khối hiện đại

#### Three types of P-boxes



16

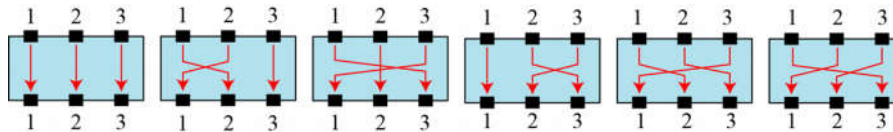




## 2.5. Sơ lược hệ mật mã đối xứng hiện đại

### 2.5.1. Hệ mật mã khối hiện đại

Shows all 6 possible mappings of a  $3 \times 3$  P-Box ?



17



## 2.5. Sơ lược hệ mật mã đối xứng hiện đại

### 2.5.1. Hệ mật mã khối hiện đại

Example of a permutation table for a straight P-box

58	50	42	34	26	18	10	02	60	52	44	36	28	20	12	04
62	54	46	38	30	22	14	06	64	56	48	40	32	24	16	08
57	49	41	33	25	17	09	01	59	51	43	35	27	19	11	03
61	53	45	37	29	21	13	05	63	55	47	39	31	23	15	07

18



## 2.5. Sơ lược hệ mật mã đối xứng hiện đại

### 2.5.1. Hệ mật mã khối hiện đại

#### Compression P-Boxes

A compression P-box is a P-box with  $n$  inputs and  $m$  outputs where  $m < n$ .

01	02	03	21	22	26	27	28	29	13	14	17
18	19	20	04	05	06	10	11	12	30	31	32

*Example of a  $32 \times 24$  permutation table*

19



## 2.5. Sơ lược hệ mật mã đối xứng hiện đại

### 2.5.1. Hệ mật mã khối hiện đại

#### Expansion P-Boxes

An expansion P-box is a P-box with  $n$  inputs and  $m$  outputs where  $m > n$ .

01	09	10	11	12	01	02	03	03	04	05	06	07	08	09	12
----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----

*Example of a  $12 \times 16$  permutation table*

20



## 2.5. Sơ lược hệ mật mã đối xứng hiện đại

### 2.5.1. Hệ mật mã khối hiện đại

Lưu ý

**A straight P-box is invertible, but compression and expansion P-boxes are not.**

21



## 2.5. Sơ lược hệ mật mã đối xứng hiện đại

### 2.5.1. Hệ mật mã khối hiện đại

**How to invert a permutation table represented as a one-dimensional table?**

1. Original table 

6	3	4	5	2	1
---	---	---	---	---	---
2. Add indices 

6	3	4	5	2	1
1	2	3	4	5	6
3. Swap contents and indices 

1	2	3	4	5	6
6	3	4	5	2	1
4. Sort based on indices 

6	5	2	3	4	1
1	2	3	4	5	6
5. Inverted table 

6	5	2	3	4	1
---	---	---	---	---	---

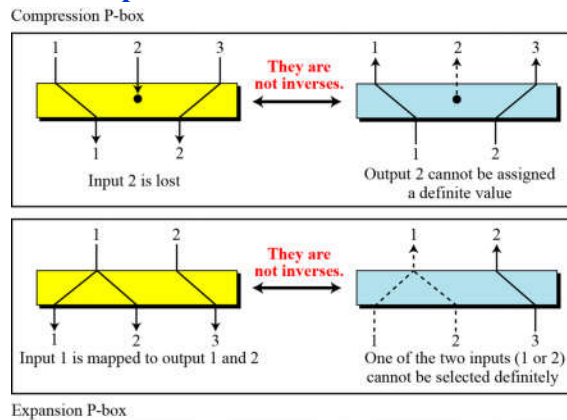
22



## 2.5. Sơ lược hệ mật mã đối xứng hiện đại

### 2.5.1. Hệ mật mã khối hiện đại

Compression and expansion P-boxes are non-invertible



23



## 2.5. Sơ lược hệ mật mã đối xứng hiện đại

### 2.5.1. Hệ mật mã khối hiện đại

#### **S-Box**

An *S-box* (**S**ubstitution **B**ox) can be thought of as a miniature substitution cipher.

Lưu ý

An S-box is an  $m \times n$  substitution unit, where  $m$  and  $n$  are not necessarily the same.

24



## 2.5. Sơ lược hệ mật mã đối xứng hiện đại

### 2.5.1. Hệ mật mã khối hiện đại

In an S-box with three inputs and two outputs, we have

$$y_1 = x_1 \oplus x_2 \oplus x_3 \quad y_2 = x_1$$



$$\begin{bmatrix} y_1 \\ y_2 \end{bmatrix} = \begin{bmatrix} 1 & 1 & 1 \\ 1 & 0 & 0 \end{bmatrix} \times \begin{bmatrix} x_1 \\ x_2 \\ x_3 \end{bmatrix}$$

This S-Box is **linear** because  $a_{1,1} = a_{1,2} = a_{1,3} = a_{2,1} = 1$  and  $a_{2,2} = a_{2,3} = 0$ .

25



## 2.5. Sơ lược hệ mật mã đối xứng hiện đại

### 2.5.1. Hệ mật mã khối hiện đại

In an S-box with three inputs and two outputs, we have

$$y_1 = (x_1)^3 + x_2 \quad y_2 = (x_1)^2 + x_1x_2 + x_3$$

where multiplication and addition is in GF(2). The S-box is **nonlinear** because there is no linear relationship between the inputs and the outputs.

26



## 2.5. Sơ lược hệ mật mã đối xứng hiện đại

### 2.5.1. Hệ mật mã khối hiện đại

The following table defines the input/output relationship for an S-box of size  $3 \times 2$ . The leftmost bit of the input defines the row; the two rightmost bits of the input define the column. The two output bits are values on the cross section of the selected row and column.

	Leftmost bit		00	01	10	11	
							Rightmost bits
Input: 010 – output: 01	↓	0	00	10	01	11	
Input: 101 – output: 00		1	10	00	11	01	
			Output bits				

27




## 2.5. Sơ lược hệ mật mã đối xứng hiện đại

### 2.5.1. Hệ mật mã khối hiện đại

#### Lưu ý

*An S-box may or may not be invertible. In an invertible S-box, the number of input bits should be the same as the number of output bits.*

28



## 2.5. Sơ lược hệ mật mã đối xứng hiện đại

---

### 2.5.1. Hệ mật mã khối hiện đại

#### An example of an invertible S-box

3 bits  
↓

	00	01	10	11
0	011	101	111	100
1	000	010	001	110

Table used for encryption  
↓  
3 bits

3 bits  
↓

	00	01	10	11
0	100	110	101	000
1	011	001	111	010


Table used for decryption  
↓  
3 bits

Encryption: input: 001 -> **output ?**

Decryption: input: 101 -> **output ?**

---

29



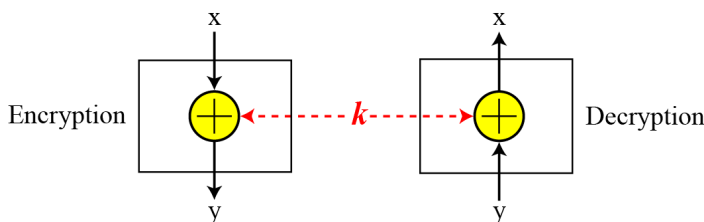
## 2.5. Sơ lược hệ mật mã đối xứng hiện đại

---

### 2.5.1. Hệ mật mã khối hiện đại

#### Exclusive-Or

*An important component in most block ciphers is the exclusive-or operation.*



*Invertibility of the exclusive-or operation*

---

30



## 2.5. Sơ lược hệ mật mã đối xứng hiện đại

### 2.5.1. Hệ mật mã khối hiện đại

*Addition and subtraction operations in the  $GF(2^n)$  field are performed by a single operation called the exclusive-or (XOR).*

*The five properties of the exclusive-or operation in the  $GF(2^n)$  field makes this operation a very interesting component for use in a block cipher: **closure**, **associativity**, **commutativity**, **existence of identity**, and **existence of inverse**.*

31

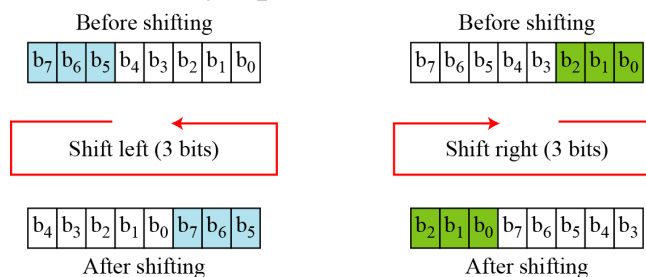


## 2.5. Sơ lược hệ mật mã đối xứng hiện đại

### 2.5.1. Hệ mật mã khối hiện đại

#### Circular Shift

*Another component found in some modern block ciphers is the circular shift operation.*



*Circular shifting an 8-bit word to the left or right*

32



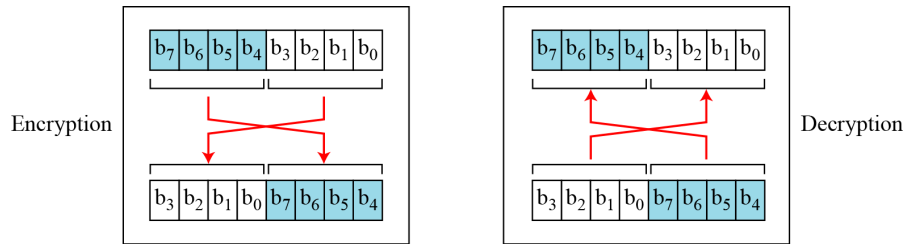


## 2.5. Sơ lược hệ mật mã đối xứng hiện đại

### 2.5.1. Hệ mật mã khối hiện đại

#### Swap

*The swap operation is a special case of the circular shift operation where  $k = n/2$ .*



*Swap operation on an 8-bit word*

33

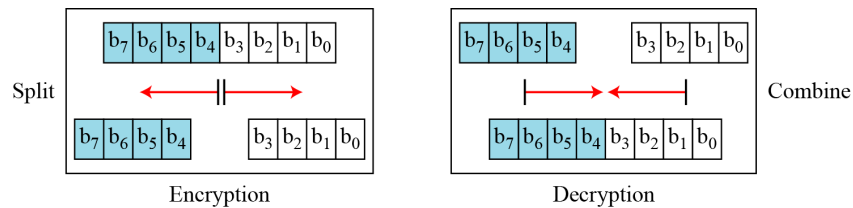


## 2.5. Sơ lược hệ mật mã đối xứng hiện đại

### 2.5.1. Hệ mật mã khối hiện đại

#### Split and Combine

*Two other operations found in some block ciphers are split and combine.*



*Split and combine operations on an 8-bit word*

34



## 2.5. Sơ lược hệ mật mã đối xứng hiện đại

### 2.5.1. Hệ mật mã khối hiện đại

#### Product Ciphers

*Shannon introduced the concept of a product cipher. A product cipher is a complex cipher combining substitution, permutation, and other components discussed in previous sections.*

35



## 2.5. Sơ lược hệ mật mã đối xứng hiện đại

### 2.5.1. Hệ mật mã khối hiện đại

#### Diffusion

*The idea of diffusion is to hide the relationship between the ciphertext and the plaintext.*

#### Lưu ý

**Diffusion hides the relationship between the ciphertext and the plaintext.**

36



## 2.5. Sơ lược hệ mật mã đối xứng hiện đại

### 2.5.1. Hệ mật mã khối hiện đại

#### *Confusion*

*The idea of confusion is to hide the relationship between the ciphertext and the key.*

#### Lưu ý

**Confusion hides the relationship between the ciphertext and the key.**

37



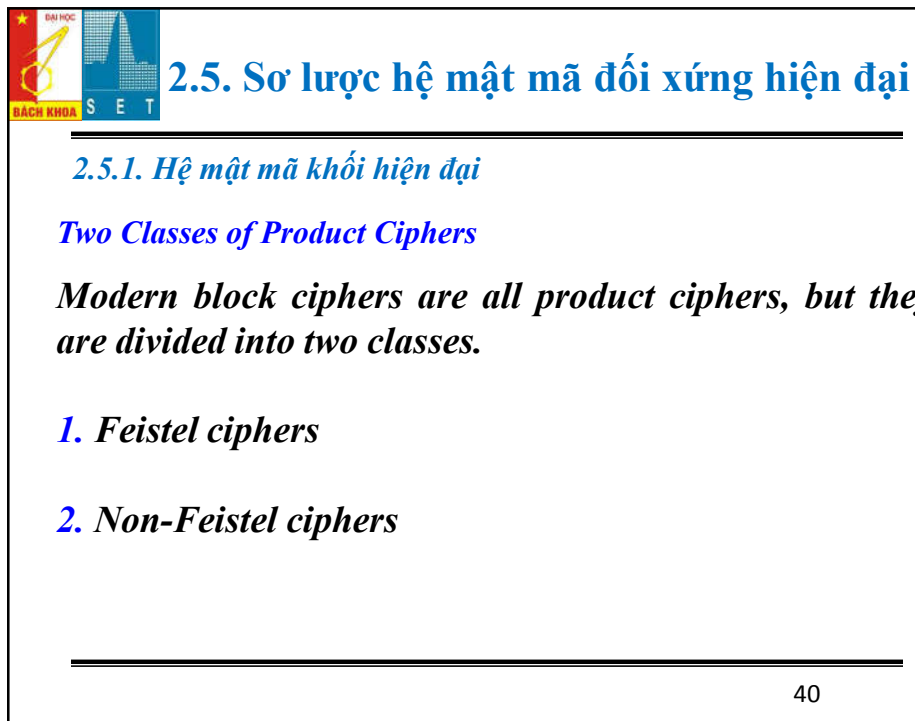
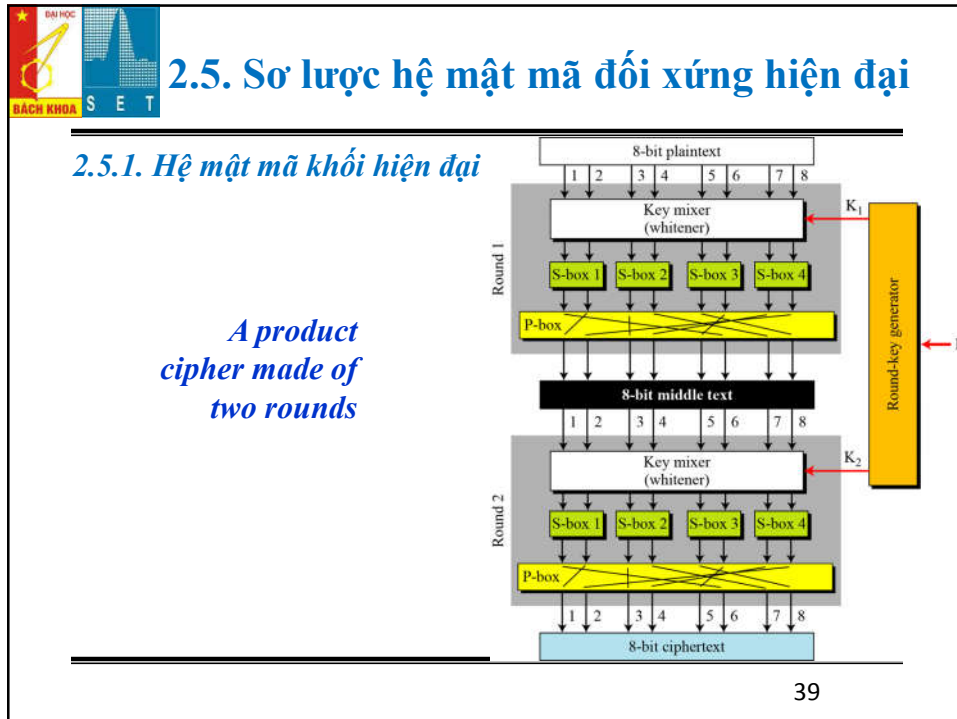
## 2.5. Sơ lược hệ mật mã đối xứng hiện đại

### 2.5.1. Hệ mật mã khối hiện đại

#### *Rounds*

*Diffusion and confusion can be achieved using **iterated product ciphers** where each iteration is a combination of S-boxes, P-boxes, and other components.*

38





## 2.5. Sơ lược hệ mật mã đối xứng hiện đại

### 2.5.1. Hệ mật mã khối hiện đại

#### *Feistel Ciphers*

*Feistel designed a very intelligent and interesting cipher that has been used for decades. A Feistel cipher can have three types of components: self-invertible, invertible, and noninvertible.*

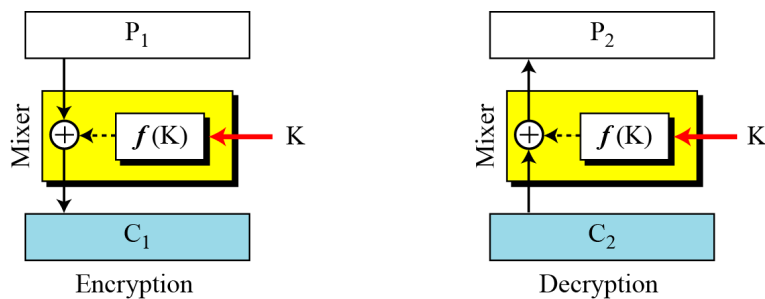
41



## 2.5. Sơ lược hệ mật mã đối xứng hiện đại

### 2.5.1. Hệ mật mã khối hiện đại

#### *The first thought in Feistel cipher design*



**Diffusion hides the relationship between the ciphertext and the plaintext.**

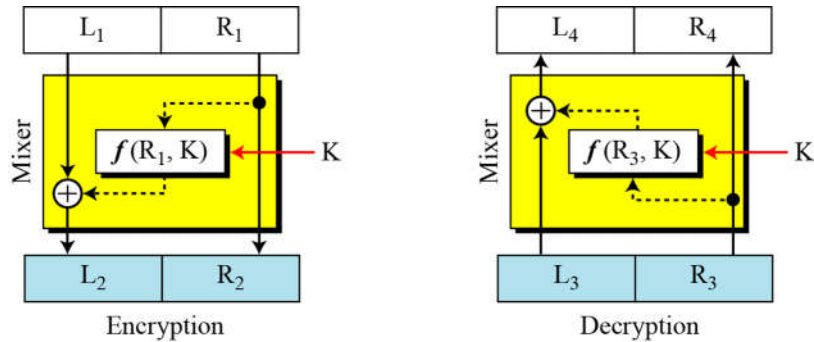
42



## 2.5. Sơ lược hệ mật mã đối xứng hiện đại

### 2.5.1. Hệ mật mã khối hiện đại

#### Improvement of the previous Feistel design



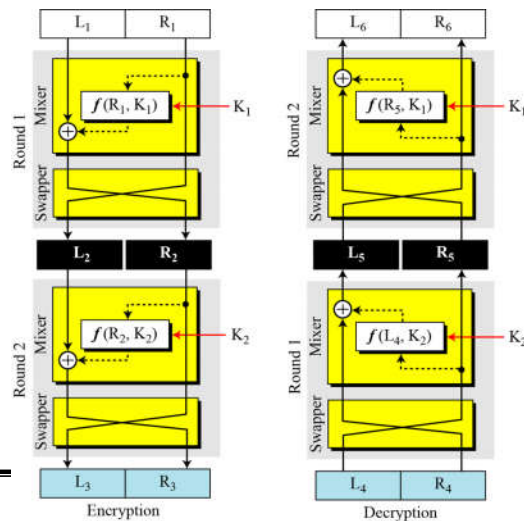
43



## 2.5. Sơ lược hệ mật mã đối xứng hiện đại

### 2.5.1. Hệ mật mã khối hiện đại

*Final design  
of a Feistel  
cipher with  
two rounds*



44



## 2.5. Sơ lược hệ mật mã đối xứng hiện đại

### 2.5.1. Hệ mật mã khối hiện đại

#### *Non-Feistel Ciphers*

*A non-Feistel cipher uses only invertible components. A component in the encryption cipher has the corresponding component in the decryption cipher.*

45

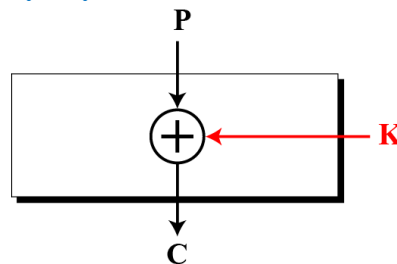


## 2.5. Sơ lược hệ mật mã đối xứng hiện đại

### 2.5.2. Thăm mã hệ mật mã khối hiện đại


#### *Differential Cryptanalysis*

*Eli Biham and Adi Shamir introduced the idea of differential cryptanalysis. This is a chosen-plaintext attack.*



Assume that the cipher is made only of one exclusive-or operation. Without knowing the value of the key, Eve can easily find the relationship between plaintext differences and ciphertext differences if by plaintext difference  $P1 \oplus P2$  and by ciphertext difference,  $C1 \oplus C2 \Rightarrow C1 \oplus C2 = P1 \oplus P2$

46



## 2.5. Sơ lược hệ mật mã đối xứng hiện đại

---

**2.5.2. Thám mã hệ mật mã khối hiện đại**

*Ví dụ:*  
 Hãy tìm khóa **K** của hệ mật như sau

P (3 bits) ↓

$\oplus$

X (3 bits) ↓

$3 \times 2$   
S-box


C (2 bits) ↓

← **K (3 bits)**

X	000	001	010	011	100	101	110	111
C	11	00	10	10	01	00	11	00

S-box table

47



## 2.5. Sơ lược hệ mật mã đối xứng hiện đại

---


**2.5.2. Thám mã hệ mật mã khối hiện đại**

**Differential cryptanalysis is based on a nonuniform differential distribution table of the S-boxes in a block cipher.**

***Linear Cryptanalysis***  
*Linear cryptanalysis was presented by Mitsuru Matsui in 1993. The analysis uses known plaintext attacks.*

48



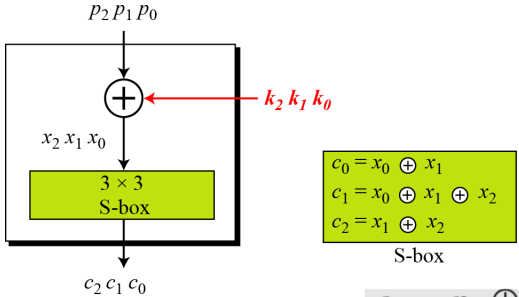


## 2.5. Sơ lược hệ mật mã đối xứng hiện đại

---

### 2.5.2. Thăm mã hệ mật mã khối hiện đại

*A simple cipher with a linear S-box*




$$\begin{aligned} c_0 &= x_0 \oplus k_0 \\ c_1 &= x_0 \oplus x_1 \oplus k_1 \\ c_2 &= x_1 \oplus k_2 \end{aligned}$$

S-box

$$\begin{aligned} c_0 &= p_0 \oplus k_0 \oplus p_1 \oplus k_1 \\ c_1 &= p_0 \oplus k_0 \oplus p_1 \oplus k_1 \oplus p_2 \oplus k_2 \\ c_2 &= p_1 \oplus k_1 \oplus p_2 \oplus k_2 \end{aligned}$$

49




## 2.5. Sơ lược hệ mật mã đối xứng hiện đại

---

### 2.5.2. Thăm mã hệ mật mã khối hiện đại

*A simple cipher with a linear S-box*

$$\begin{aligned} c_0 &= p_0 \oplus k_0 \oplus p_1 \oplus k_1 \\ c_1 &= p_0 \oplus k_0 \oplus p_1 \oplus k_1 \oplus p_2 \oplus k_2 \\ c_2 &= p_1 \oplus k_1 \oplus p_2 \oplus k_2 \end{aligned}$$



$$\begin{aligned} k_1 &= (p_1) \oplus (c_0 \oplus c_1 \oplus c_2) \\ k_2 &= (p_2) \oplus (c_0 \oplus c_1) \\ k_0 &= (p_0) \oplus (c_1 \oplus c_2) \end{aligned}$$

*This means that three known-plaintext attacks can find the values of  $k_0$ ,  $k_1$ , and  $k_2$ .*

50



## 2.5. Sơ lược hệ mật mã đối xứng hiện đại

### 2.5.2. Thăm mã hệ mật mã khối hiện đại

*In some modern block ciphers, it may happen that some S-boxes are not totally nonlinear; they can be approximated, probabilistically, by some linear functions.*

$$(k_0 \oplus k_1 \oplus \dots \oplus k_x) = (p_0 \oplus p_1 \oplus \dots \oplus p_y) \oplus (c_0 \oplus c_1 \oplus \dots \oplus c_z)$$

*where  $1 \leq x \leq m$ ,  $1 \leq y \leq n$ , and  $1 \leq z \leq n$ .*

51



## 2.5. Sơ lược hệ mật mã đối xứng hiện đại

### 2.5.3. Hệ mật mã dòng hiện đại

*In a modern stream cipher, encryption and decryption are done  $r$  bits at a time. We have a plaintext bit stream  $P = p_n \dots p_2 p_1$ , a ciphertext bit stream  $C = c_n \dots c_2 c_1$ , and a key bit stream  $K = k_n \dots k_2 k_1$ , in which  $p_i$ ,  $c_i$ , and  $k_i$  are  $r$ -bit words.*

- **Synchronous Stream Ciphers**
- **Nonsynchronous Stream Ciphers**

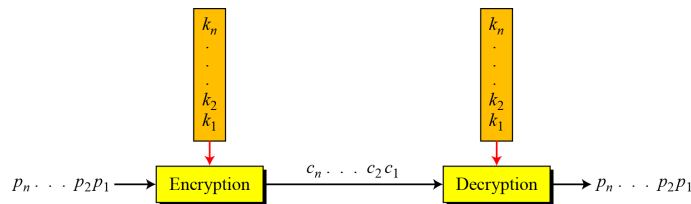
52



## 2.5. Sơ lược hệ mật mã đối xứng hiện đại

### 2.5.3. Hệ mật mã dòng hiện đại

In a modern stream cipher, each  $r$ -bit word in the plaintext stream is enciphered using an  $r$ -bit word in the key stream to create the corresponding  $r$ -bit word in the ciphertext stream.



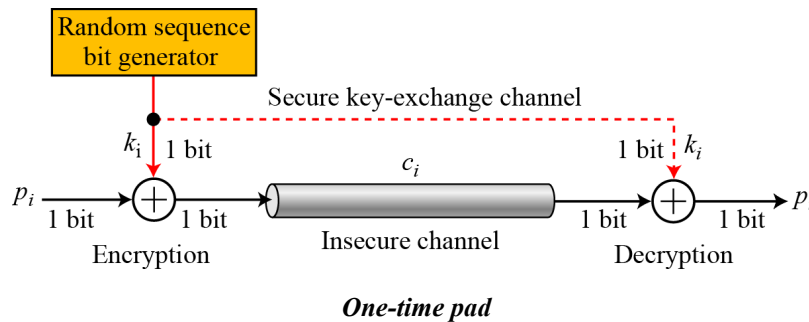
53



## 2.5. Sơ lược hệ mật mã đối xứng hiện đại

### 2.5.3. Hệ mật mã dòng hiện đại

In a synchronous stream cipher the key is independent of the plaintext or ciphertext.



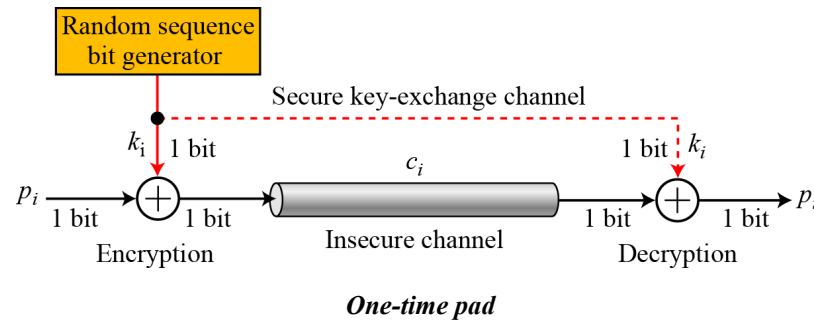
54



## 2.5. Sơ lược hệ mật mã đối xứng hiện đại

### 2.5.3. Hệ mật mã dòng hiện đại

**In a synchronous stream cipher the key is independent of the plaintext or ciphertext.**



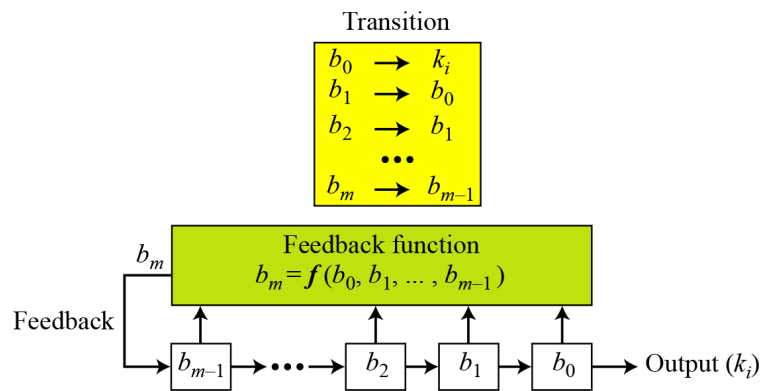
55



## 2.5. Sơ lược hệ mật mã đối xứng hiện đại

### 2.5.3. Hệ mật mã dòng hiện đại

#### Feedback shift register (FSR)



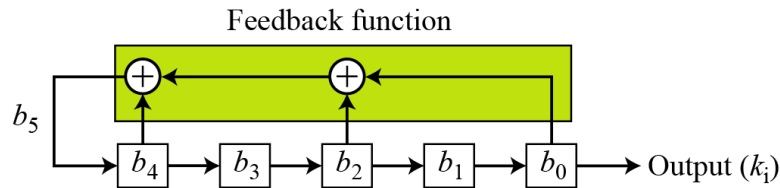
56



## 2.5. Sơ lược hệ mật mã đối xứng hiện đại

### 2.5.3. Hệ mật mã dòng hiện đại

*Ví dụ:* Create a linear feedback shift register with 5 cells in which  $b_5 = b_4 \oplus b_2 \oplus b_0$ .



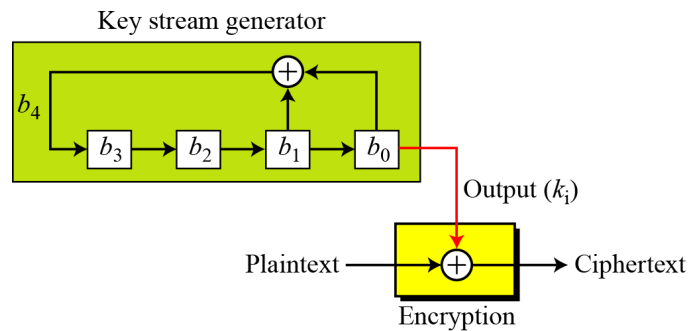
57



## 2.5. Sơ lược hệ mật mã đối xứng hiện đại

### 2.5.3. Hệ mật mã dòng hiện đại

*Ví dụ:* Create a linear feedback shift register with 4 cells in which  $b_4 = b_1 \oplus b_0$ . Show the value of output for 20 transitions (shifts) if the seed is  $(0001)_2$ .



58



## 2.5. Sơ lược hệ mật mã đối xứng hiện đại

### 2.5.3. Hệ mật mã dòng hiện đại

States	$b_4$	$b_3$	$b_2$	$b_1$	$b_0$	$k_j$
Initial	1	0	0	0	1	
1	0	1	0	0	0	1
2	0	0	1	0	0	0
3	1	0	0	1	0	0
4	1	1	0	0	1	0
5	0	1	1	0	0	1
6	1	0	1	1	0	0
7	0	1	0	1	1	0
8	1	0	1	0	1	1
9	1	1	0	1	0	1
10	1	1	1	0	1	0

11	1	1	1	1	0	1
12	0	1	1	1	1	0
13	0	0	1	1	1	1
14	0	0	0	1	1	1
15	1	0	0	0	1	1
16	0	1	0	0	0	1
17	0	0	1	0	0	0
18	1	0	0	1	0	0
19	1	1	0	0	1	0
20	1	1	1	0	0	1

100010011010111 100010011010111 100010011010111 100010011010111 ...

The key stream generated from a LFSR is a pseudorandom sequence in which the sequence is repeated after  $N$  bits.

**The maximum period of an LFSR is to  $2^m - 1$ .**

59



## 2.5. Sơ lược hệ mật mã đối xứng hiện đại

### 2.5.3. Hệ mật mã dòng hiện đại

**In a nonsynchronous stream cipher, the key depends on either the plaintext or ciphertext.**

60