

# **Chương 3**

# **Traditional Symmetric-Key Ciphers**

**Mật mã khóa đối xứng  
cổ điển**

## Objectives

- Xác định các thuật ngữ và khái niệm về mật mã khóa đối xứng
- Nhấn mạnh hai loại mật mã truyền thống: mật mã thay thế (substitution) và chuyển vị (transposition)
- Mô tả các loại phân tích mật mã (thám mã) được sử dụng để phá vỡ hệ mật mã đối xứng
- Giới thiệu các khái niệm về mật mã dòng và mật mã khối
- Thảo luận về một số mật mã nổi trội được sử dụng trong quá khứ, chẳng hạn như máy Enigma

## Objectives

- To define the terms and the concepts of symmetric key ciphers**
- To emphasize the two categories of traditional ciphers: substitution and transposition ciphers**
- To describe the categories of cryptanalysis used to break the symmetric ciphers**
- To introduce the concepts of the stream ciphers and block ciphers**
- To discuss some very dominant ciphers used in the past, such as the Enigma machine**

## 3-1 INTRODUCTION

*Hình 3.1 sau đây cho thấy ý tưởng chung đằng sau một mật mã khóa đối xứng. Thông điệp gốc từ Alice đến Bob được gọi là bản rõ; thông điệp được gửi qua kênh được gọi là bản mã. Để tạo bản mã từ bản rõ, Alice sử dụng một thuật toán mã hóa và một khóa bí mật được chia sẻ. Để tạo bản rõ từ bản mã, Bob sử dụng một thuật toán giải mã và cùng một khóa bí mật.*

### Topics discussed in this section:

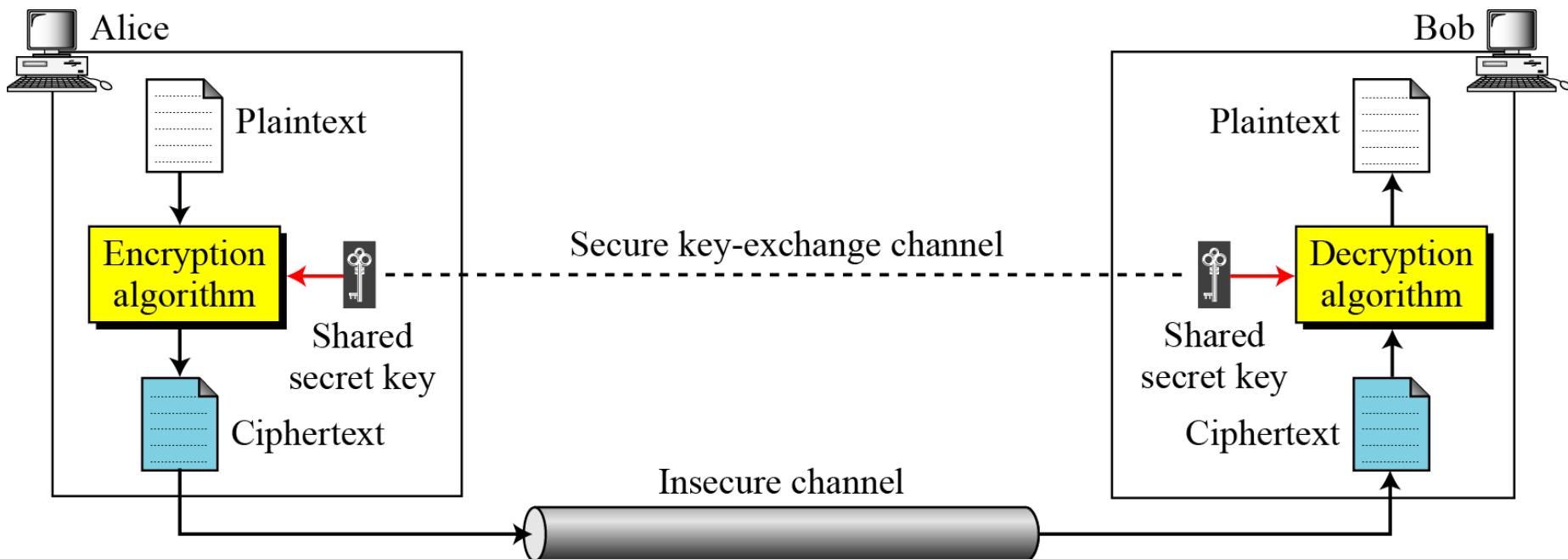
3.1.1 Kerckhoff's Principle

3.1.2 Cryptanalysis

3.1.3 Categories of Traditional Ciphers

### 3.1 *Continued*

**Figure 3.1 General idea of symmetric-key cipher**  
**Hình 3.1 Ý tưởng chung về mật mã khóa đối xứng**



### 3.1 *Continued*

*If  $P$  is the plaintext,  $C$  is the ciphertext, and  $K$  is the key,  
Nếu  $P$  là bản rõ,  $C$  là bản mã và  $K$  là khóa,*

Encryption:  $C = E_k(P)$

Decryption:  $P = D_k(C)$

In which,  $D_k(E_k(x)) = E_k(D_k(x)) = x$

*We assume that Bob creates  $P_1$ ; we prove that  $P_1 = P$ :  
Chúng ta giả định rằng Bob tạo  $P_1$ ; chúng tôi chứng minh  
rằng  $P_1 = P$ :*

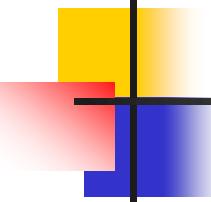
**Alice:**  $C = E_k(P)$

**Bob:**  $P_1 = D_k(C) = D_k(E_k(P)) = P$

### 3.1 *Continued*

**Figure 3.2** Locking and unlocking with the same key  
*Hình 3.2 Khóa và mở khóa bằng cùng một chìa khóa*





### **3.1.1 *Kerckhoff's Principle***

Based on **Kerckhoff's principle**, one should always assume that the adversary, Eve, knows the encryption/decryption algorithm. The resistance of the cipher to attack must be based only on the secrecy of the key.

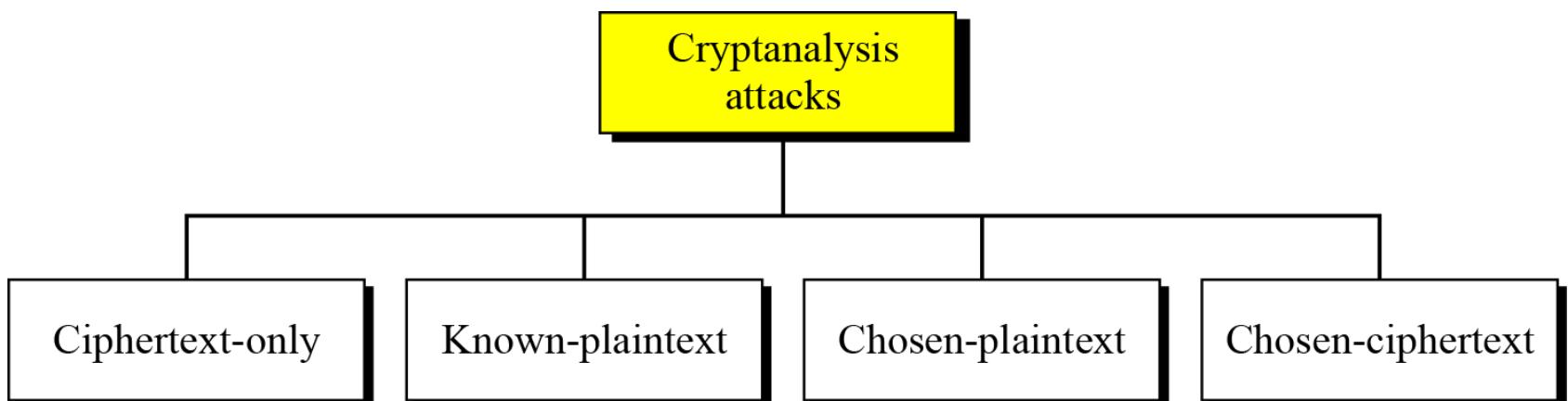
Dựa trên nguyên tắc của Kerckhoff, người ta nên luôn giả định rằng đối thủ, gọi là Eve, biết thuật toán mã hóa / giải mã. Khả năng chống lại sự tấn công của mật mã chỉ được dựa vào tính bí mật của khóa.

### 3.1.2 Cryptanalysis

As cryptography is the science and art of creating secret codes, **cryptanalysis** is the science and art of breaking those codes.

Vì mật mã là khoa học và nghệ thuật tạo ra các mã bí mật, nên phá mã là khoa học và nghệ thuật để phá các mã đó.

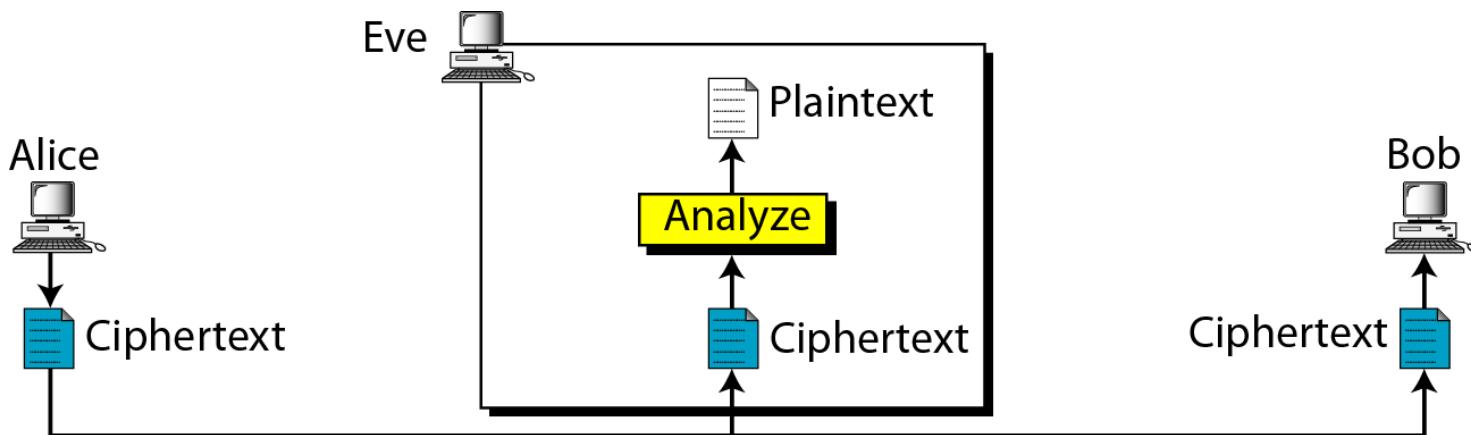
**Figure 3.3** *Cryptanalysis attacks*



## 3.1.2 *Continued*

### Ciphertext-Only Attack

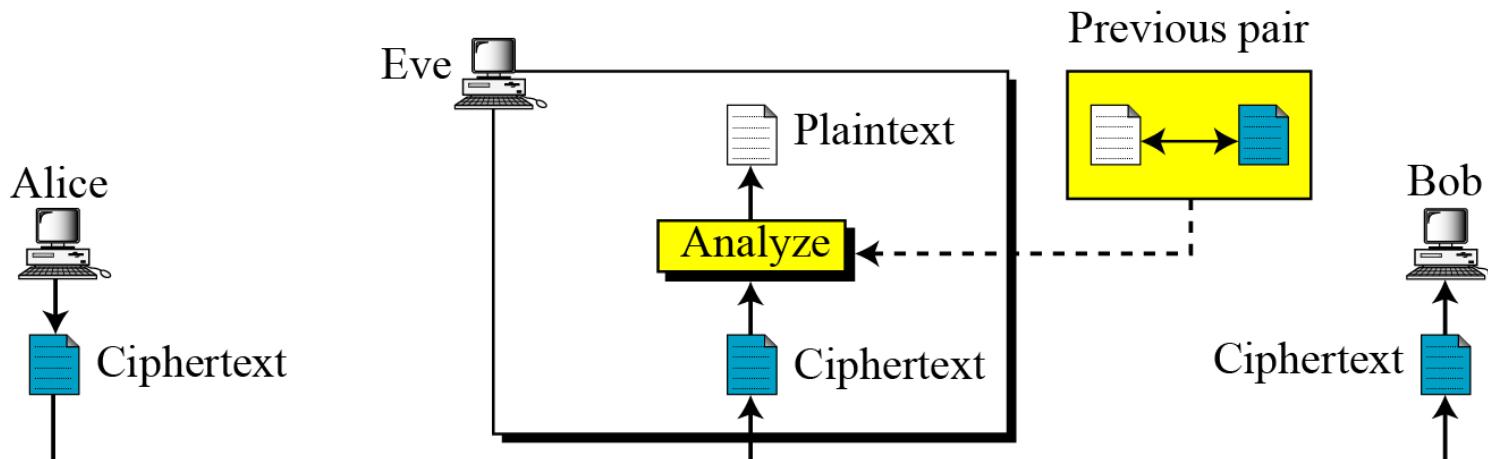
**Figure 3.4 Ciphertext-only attack**  
*Tấn công chỉ bằng văn bản mã*



## 3.1.2 *Continued*

### Known-Plaintext Attack

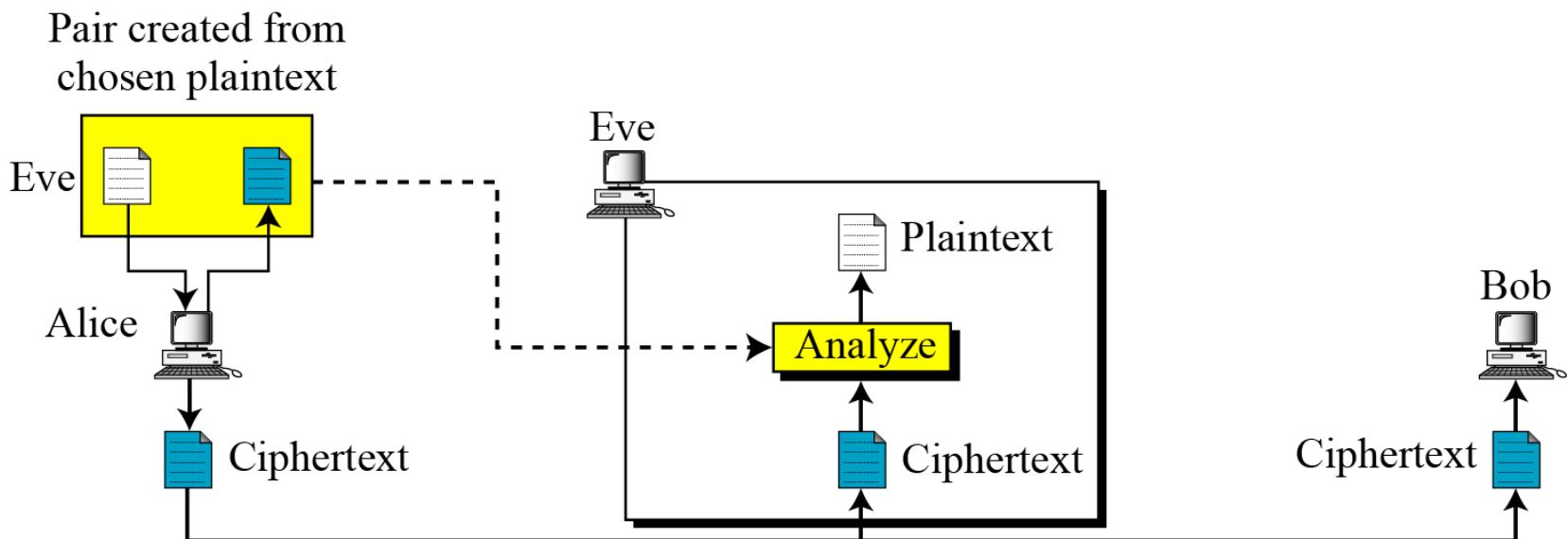
**Figure 3.5 Known-plaintext attack**  
*Tấn công văn bản rõ đã biết*



## 3.1.2 *Continued*

### Chosen-Plaintext Attack

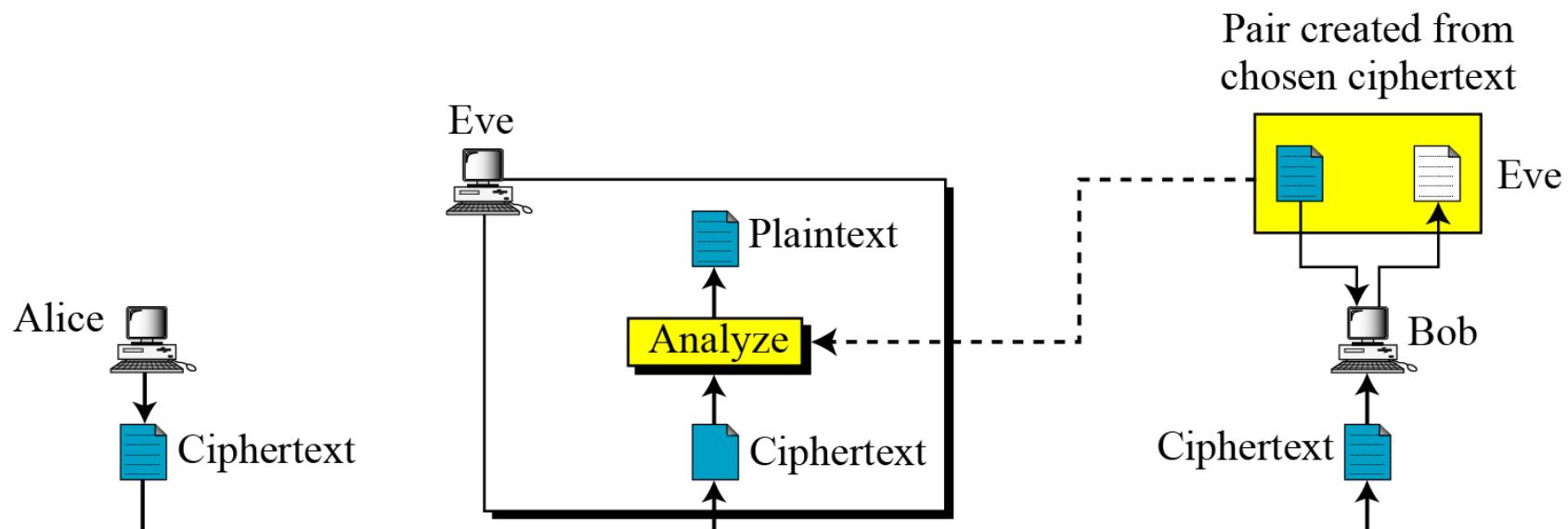
**Figure 3.6 Chosen-plaintext attack**  
*Cuộc tấn công plaintext được chọn*



## 3.1.2 *Continued*

### Chosen-Ciphertext Attack

**Figure 3.7 Chosen-ciphertext attack**  
*Tấn công bản mã được chọn*



## 3-2 SUBSTITUTION CIPHERS: MÃ THAY THẾ

A substitution cipher replaces one symbol with another. Substitution ciphers can be categorized as either monoalphabetic ciphers or polyalphabetic ciphers.

Một mật mã thay thế thay thế một ký hiệu bằng một ký hiệu khác. Mật mã thay thế có thể được phân loại là mật mã đơn ký tự hoặc mật mã đa ký tự.

**Note**

**A substitution cipher replaces one symbol with another.**

**Topics discussed in this section:**

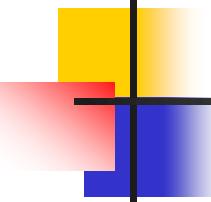
- 3.2.1 Monoalphabetic Ciphers: Hệ mật thay thế đơn ký tự**
- 3.2.2 Polyalphabetic Ciphers: Hệ mật thay thế đa ký tự**

### *3.2.1 Monoalphabetic Ciphers: Mã đơn ký tự*

#### *Note*

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

*Trong phép thay thế đơn ký tự, mối quan hệ giữa một ký hiệu trong bản rõ với một ký hiệu trong bản mã luôn là một-một.*



### 3.2.1 *Continued*

#### Example 3.1

The following shows a plaintext and its corresponding ciphertext. The cipher is probably monoalphabetic because both *l*'s (els) are encrypted as *O*'s.

**Plaintext:** hello

**Ciphertext:** KHOOR

#### Example 3.2

The following shows a plaintext and its corresponding ciphertext. The cipher is not monoalphabetic because each *l* (el) is encrypted by a different character.

### 3.2.1 *Continued*

#### Additive Cipher

The simplest monoalphabetic cipher is the additive cipher. This cipher is sometimes called a **shift cipher** and sometimes a **Caesar cipher**, but the term **additive cipher** better reveals its mathematical nature.

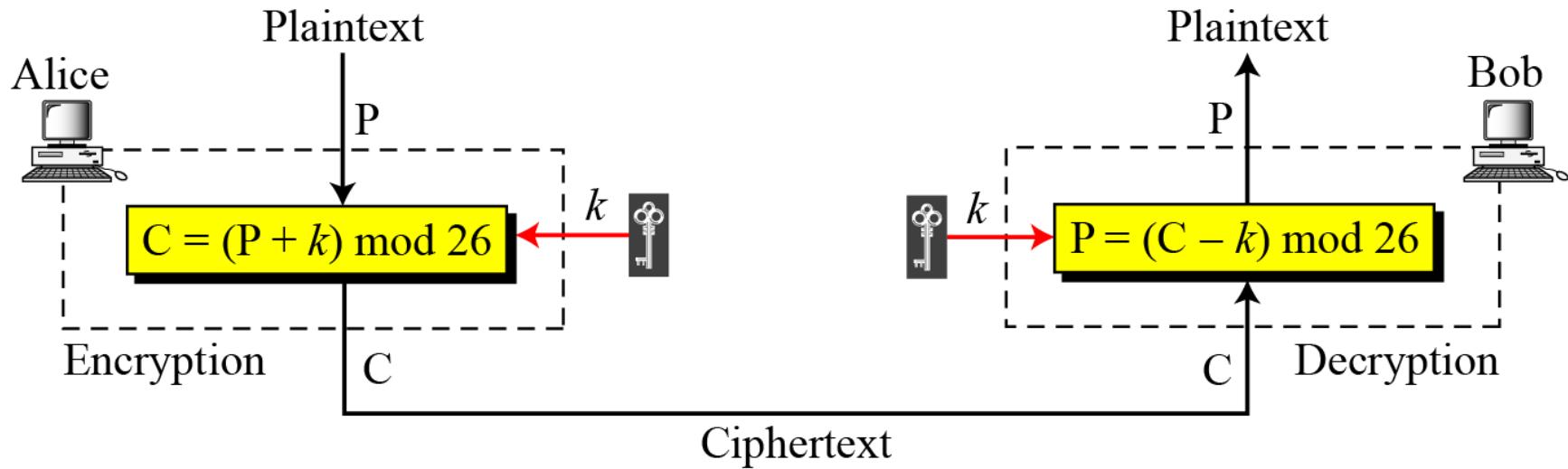
*Mật mã đơn pha đơn giản nhất là mật mã cộng. Mật mã này đôi khi được gọi là mật mã dịch chuyển và đôi khi là mật mã Caesar, nhưng thuật ngữ mật mã cộng thêm tiết lộ rõ hơn bản chất toán học của nó.*

**Figure 3.8 Plaintext and Ciphertext in  $Z_{26}$**

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

### 3.2.1 *Continued*

**Figure 3.9 Additive cipher: Mã cộng**



Hai quá trình mã hóa và giải mã hóa là thuận nghịch với nhau?  
 $P = (C - k) \text{ mod } 26 = (P + k - k) \text{ mod } 26 = P$

**Note**

**When the cipher is additive, the plaintext, ciphertext, and key are integers in  $\mathbb{Z}_{26}$ .**

### 3.2.1 *Continued*

#### Example 3.3

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

#### Solution

Chúng ta áp dụng thuật toán mã hóa cho bản rõ, từng ký tự một:

Plaintext: h → 07

Encryption:  $(07 + 15) \text{ mod } 26$

Ciphertext: 22 → W

Plaintext: e → 04

Encryption:  $(04 + 15) \text{ mod } 26$

Ciphertext: 19 → T

Plaintext: l → 11

Encryption:  $(11 + 15) \text{ mod } 26$

Ciphertext: 00 → A

Plaintext: l → 11

Encryption:  $(11 + 15) \text{ mod } 26$

Ciphertext: 00 → A

Plaintext: o → 14

Encryption:  $(14 + 15) \text{ mod } 26$

Ciphertext: 03 → D

### 3.2.1 *Continued*

#### Example 3.4

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

#### Solution

We apply the decryption algorithm to the plaintext character by character:

Ciphertext: W → 22

Decryption:  $(22 - 15) \bmod 26$

Plaintext: 07 → h

Ciphertext: T → 19

Decryption:  $(19 - 15) \bmod 26$

Plaintext: 04 → e

Ciphertext: A → 00

Decryption:  $(00 - 15) \bmod 26$

Plaintext: 11 → l

Ciphertext: A → 00

Decryption:  $(00 - 15) \bmod 26$

Plaintext: 11 → l

Ciphertext: D → 03

Decryption:  $(03 - 15) \bmod 26$

Plaintext: 14 → o

### 3.2.1 *Continued*

#### Shift Cipher and Caesar Cipher

Historically, additive ciphers are called **shift ciphers**. Julius Caesar used an additive cipher to communicate with his officers. For this reason, additive ciphers are sometimes referred to as the Caesar cipher. Caesar used a key of 3 for his communications.

##### **Note**

**Additive ciphers are sometimes referred to as shift ciphers or Caesar cipher.**

*Về mặt lịch sử, mật mã cộng được gọi là mật mã dịch chuyển. Julius Caesar đã sử dụng một mật mã cộng để liên lạc với các sĩ quan của mình. Vì lý do này, mật mã cộng đôi khi được gọi là mật mã Caesar. Caesar đã sử dụng khóa 3 để liên lạc thông tin.*

## 3.2.1 *Continued*

### Example 3.5

Eve has intercepted the ciphertext “UVACLYFZLJBYL”. Show how she can use a brute-force attack to break the cipher.

Eve đã chặn bản mã “UVACLYFZLJBYL”. Chỉ ra cách cô ấy có thể sử dụng một cuộc tấn công bạo lực để phá vỡ mật mã.

### Solution

Eve tries keys from 1 to 7. With a key of 7, the plaintext is “not very secure”, which makes sense.

Eve thử các khóa từ 1 đến 7. Với khóa 7, bản rõ là "không an toàn lắm", điều này có lý.

Ciphertext: UVACLYFZLJBYL

<b>K = 1</b>	→	<b>Plaintext:</b> tuzbkxeykiaxk
<b>K = 2</b>	→	<b>Plaintext:</b> styajwdxjhwj
<b>K = 3</b>	→	<b>Plaintext:</b> rsxzivcwigyvi
<b>K = 4</b>	→	<b>Plaintext:</b> qrwyhubvhfxuh
<b>K = 5</b>	→	<b>Plaintext:</b> pqvxgtaugewtg
<b>K = 6</b>	→	<b>Plaintext:</b> opuwfsztfdvsf
<b>K = 7</b>	→	<b>Plaintext:</b> notverysecure

### 3.2.1 *Continued*

**Bảng 3.1 Tần suất của các ký tự trong tiếng Anh**

Letter	Frequency	Letter	Frequency	Letter	Frequency	Letter	Frequency
E	12.7	H	6.1	W	2.3	K	0.08
T	9.1	R	6.0	F	2.2	J	0.02
A	8.2	D	4.3	G	2.0	Q	0.01
O	7.5	L	4.0	Y	2.0	X	0.01
I	7.0	C	2.8	P	1.9	Z	0.01
N	6.7	U	2.8	B	1.5		
S	6.3	M	2.4	V	1.0		

**Table 3.2 tần suất xuất của diagrams and trigrams**

Digram	TH, HE, IN, ER, AN, RE, ED, ON, ES, ST, EN, AT, TO, NT, HA, ND, OU, EA, NG, AS, OR, TI, IS, ET, IT, AR, TE, SE, HI, OF
Trigram	THE, ING, AND, HER, ERE, ENT, THA, NTH, WAS, ETH, FOR, DTH

### 3.2.1 *Continued*

#### Example 3.6

Eve đã chặn đoạn mã sau đây. Sử dụng một cuộc tấn công thống kê, tìm ra bản rõ.

XLILSYWIMWRSAJSVWEPIJSVJSYVQMPPMSRHSPEVWMXMWASVX-LQSVILY-  
VVCFIJSVIXLIWIPPIVIGIMZIWQSVISJJIVW

#### Solution

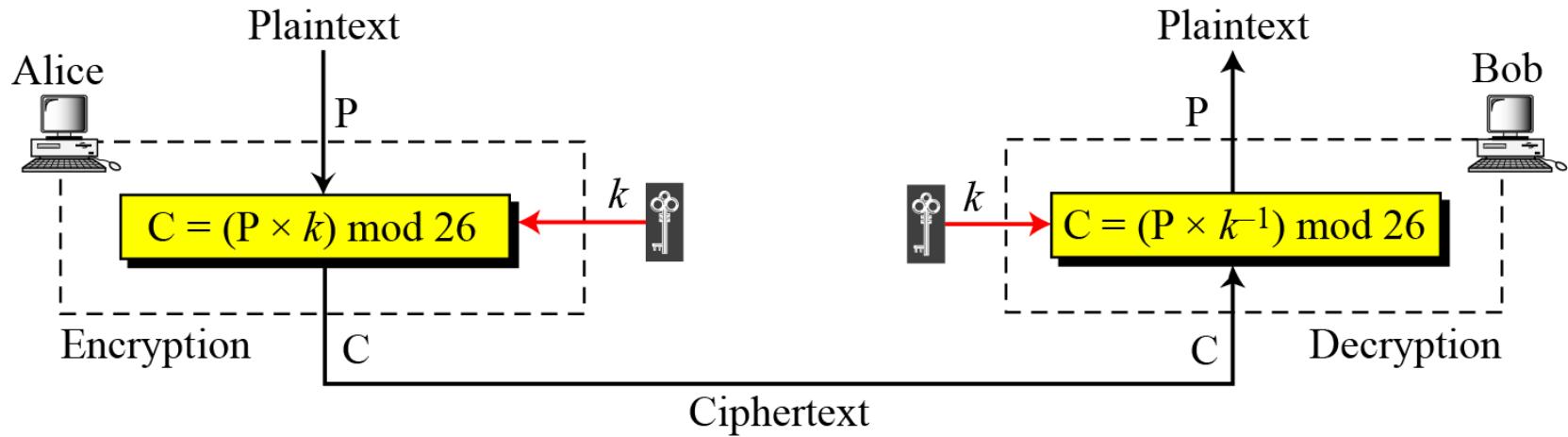
Khi Eve lập bảng tần số của các chữ cái trong bản mã này, cô ấy nhận được: I = 14, V = 13, S = 12, v.v. Ký tự phổ biến nhất là I với 14 lần xuất hiện. Điều này có nghĩa là key = 4.

the house is now for sale for four million dollars it is worth more hurry before the seller receives more offers

### 3.2.1 *Continued*

#### Multiplicative Ciphers: Mã nhân

Figure 3.10 lược đồ mã nhân (*Multiplicative cipher*)



**Note**

In a multiplicative cipher, the plaintext and ciphertext are integers in  $Z_{26}$ ; the key is an integer in  $Z_{26}^*$ .

### 3.2.1 *Continued*

#### Example 3.7

Miền khóa (key domain) đối với bất kỳ mã nhân (multiplicative cipher) nào là gì, gồm những số nào?

#### Solution

Khóa cần tìm phải thuộc tập  $Z_{26}^*$ . Tập này có 12 số như sau: **1, 3, 5, 7, 9, 11, 15, 17, 19, 21, 23, 25**.

#### Example 3.8

Chúng ta sử dụng mã nhân để mã hóa bản tin “hello” với khóa là 7. Khi đó, bản mã là “XCZZU”.

Plaintext: h → 07

Encryption:  $(07 \times 07) \bmod 26$

ciphertext: 23 → X

Plaintext: e → 04

Encryption:  $(04 \times 07) \bmod 26$

ciphertext: 02 → C

Plaintext: l → 11

Encryption:  $(11 \times 07) \bmod 26$

ciphertext: 25 → Z

Plaintext: l → 11

Encryption:  $(11 \times 07) \bmod 26$

ciphertext: 25 → Z

Plaintext: o → 14

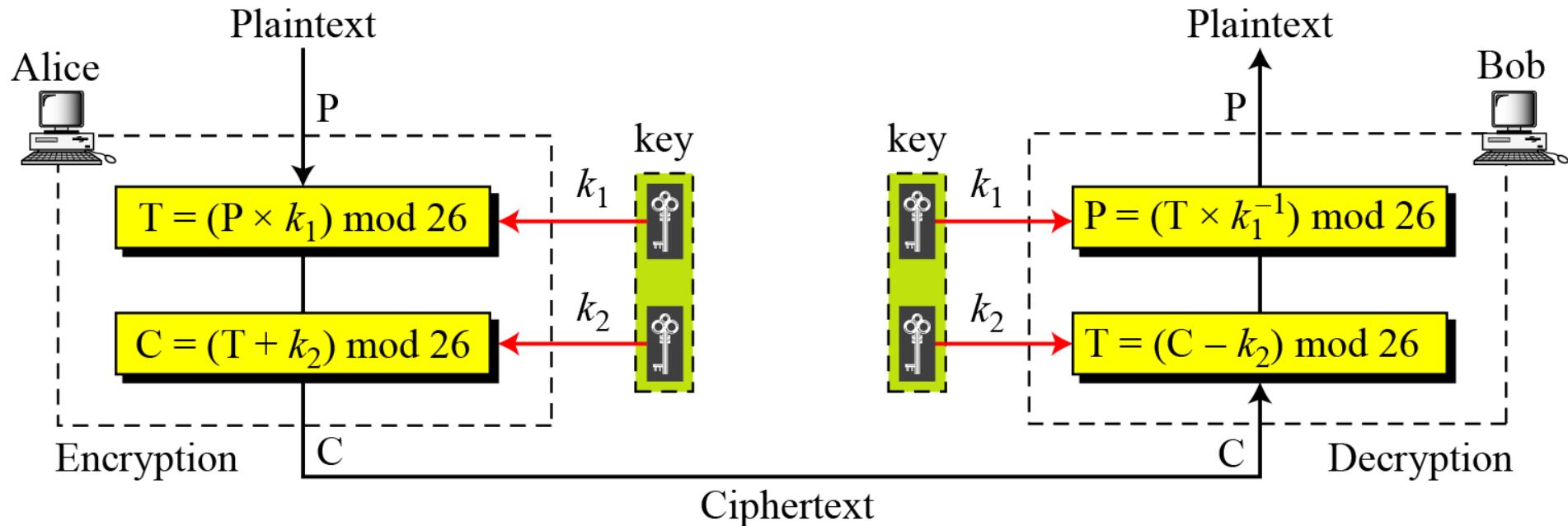
Encryption:  $(14 \times 07) \bmod 26$

ciphertext: 20 → U

### 3.2.1 *Continued*

#### Affine Ciphers: Mā Affine

**Figure 3.11** *Affine cipher*



$$C = (P \times k_1 + k_2) \bmod 26$$

$$P = ((C - k_2) \times k_1^{-1}) \bmod 26$$

where  $k_1^{-1}$  is the multiplicative inverse of  $k_1$  and  $-k_2$  is the additive inverse of  $k_2$

### 3.2.1 *Continued*

#### Example 3.09

The affine cipher uses a pair of keys in which the first key is from  $Z_{26}^*$  and the second is from  $Z_{26}$ . The size of the key domain is  $12 \times 26 = 312$ .

Mật mã affine sử dụng một cặp khóa, trong đó khóa đầu tiên là từ  $Z_{26}^*$  và khóa thứ hai là từ  $Z_{26}$ . Kích thước của miền khóa là  $12 \times 26 = 312$ .

#### Example 3.10

Use an affine cipher to encrypt the message “hello” with the key pair  $(7, 2)$ .

Sử dụng mật mã affine để mã hóa thông báo “hello” bằng cặp khóa  $(7, 2)$ .

$$P: h \rightarrow 07$$

$$\text{Encryption: } (07 \times 7 + 2) \bmod 26$$

$$C: 25 \rightarrow Z$$

$$P: e \rightarrow 04$$

$$\text{Encryption: } (04 \times 7 + 2) \bmod 26$$

$$C: 04 \rightarrow E$$

$$P: l \rightarrow 11$$

$$\text{Encryption: } (11 \times 7 + 2) \bmod 26$$

$$C: 01 \rightarrow B$$

$$P: l \rightarrow 11$$

$$\text{Encryption: } (11 \times 7 + 2) \bmod 26$$

$$C: 01 \rightarrow B$$

$$P: o \rightarrow 14$$

$$\text{Encryption: } (14 \times 7 + 2) \bmod 26$$

$$C: 22 \rightarrow W$$

## 3.2.1 *Continued*

### Example 3.11

Use the affine cipher to decrypt the message “ZEBBW” with the key pair  $(7, 2)$  in modulus 26.

Sử dụng mật mã affine để giải mã thông báo “ZEBBW” bằng cặp khóa  $(7, 2)$  trong mô-đun 26.

### Solution

C: Z  $\rightarrow$  25

Decryption:  $((25 - 2) \times 7^{-1}) \bmod 26$

P:07  $\rightarrow$  h

C: E  $\rightarrow$  04

Decryption:  $((04 - 2) \times 7^{-1}) \bmod 26$

P:04  $\rightarrow$  e

C: B  $\rightarrow$  01

Decryption:  $((01 - 2) \times 7^{-1}) \bmod 26$

P:11  $\rightarrow$  l

C: B  $\rightarrow$  01

Decryption:  $((01 - 2) \times 7^{-1}) \bmod 26$

P:11  $\rightarrow$  l

C: W  $\rightarrow$  22

Decryption:  $((22 - 2) \times 7^{-1}) \bmod 26$

P:14  $\rightarrow$  o

### Example 3.12

The additive cipher is a special case of an affine cipher in which  $k_1 = 1$ . The multiplicative cipher is a special case of affine cipher in which  $k_2 = 0$ .

Mật mã cộng là một trường hợp đặc biệt của mật mã affine, trong đó  $k_1 = 1$ .

Mật mã nhân là một trường hợp đặc biệt của mật mã affine trong đó  $k_2 = 0$ .

### 3.2.1 *Continued*

#### Monoalphabetic Substitution Cipher

Because additive, multiplicative, and affine ciphers have small key domains, they are very vulnerable to brute-force attack.

*Do mật mã cộng, nhân và mã Affine có miền khóa nhỏ, chúng rất dễ bị tấn công cực mạnh (brute-force).*

A better solution is to create a mapping between each plaintext character and the corresponding ciphertext character. Alice and Bob can agree on a table showing the mapping for each character.

*Một giải pháp tốt hơn là tạo một ánh xạ giữa mỗi ký tự bản rõ và ký tự bản mã tương ứng. Alice và Bob có thể đồng ý về một bảng hiển thị ánh xạ cho mỗi ký tự.*

**Figure 3.12** An example key for monoalphabetic 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

### 3.2.1 *Continued*

#### Example 3.13

We can use the key in Figure 3.12 to encrypt the message  
Chúng ta có thể sử dụng khóa trong hình 3.12 để mã hóa thông  
điệp sau đây:

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

The ciphertext is

ICFVQRVVNEFVRNVSIYRGAHSLIOJICNHTIYBFGTICRXRS

### 3.2.2 Polyalphabetic Ciphers: Mã đa ký tự

In polyalphabetic substitution, each occurrence of a character may have a different substitute. The relationship between a character in the plaintext to a character in the ciphertext is one-to-many.

Trong thay thế đa chữ cái, mỗi lần xuất hiện của một ký tự có thể có một thay thế khác nhau. Mỗi quan hệ giữa một ký tự trong bản rõ với một ký tự trong bản mã là một-nhiều.

#### Autokey Cipher

$$P = P_1 P_2 P_3 \dots$$

$$C = C_1 C_2 C_3 \dots$$

$$k = (k_1, P_1, P_2, \dots)$$

Encryption:  $C_i = (P_i + k_i) \bmod 26$

Decryption:  $P_i = (C_i - k_i) \bmod 26$

## 3.2.2 *Continued*

### Example 3.14

Assume that Alice and Bob agreed to use an autokey cipher with initial key value  $k_1 = 12$ . Now Alice wants to send Bob the message “Attack is today”. Enciphering is done character by character.

*Giả sử rằng Alice và Bob đã đồng ý sử dụng một mật mã autokey với giá trị khóa ban đầu là  $k_1 = 12$ . Nay giờ, Alice muốn gửi cho Bob thông báo “Attack is today”. Mã hóa được thực hiện theo từng ký tự.*

Plaintext:	a	t	t	a	c	k	i	s	t	o	d	a	y
P's Values:	00	19	19	00	02	10	08	18	19	14	03	00	24
Key stream:	12	00	19	19	00	02	10	08	18	19	14	03	00
C's Values:	12	19	12	19	02	12	18	00	11	7	17	03	24
Ciphertext:	M	T	M	T	C	M	S	A	L	H	R	D	Y

$$P = P_1 P_2 P_3 \dots$$

$$C = C_1 C_2 C_3 \dots$$

$$k = (k_1, P_1, P_2, \dots)$$

$$\text{Encryption: } C_i = (P_i + k_i) \bmod 26$$

$$\text{Decryption: } P_i = (C_i - k_i) \bmod 26$$

## 3.2.2 *Continued*

### Playfair Cipher: Mã Playfair → hệ đa ký tự

Figure 3.13 Ví dụ về khóa bí mật trong mật mã Playfair

Secret Key =  
 $5 \times 5$

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

1) Nếu cặp 2 chữ nằm cùng hàng → thay bởi các chữ cái bên phải

2) Nếu cặp 2 chữ nằm cùng cột → thay bởi các chữ cái bên dưới

3) Các trường hợp khác còn lại → mỗi chữ cái được thay thế bởi chữ cái khác cùng hàng, nhưng trên cùng cái cột IX → LU mà chữ cái cùng cặp)

$$P = \textcolor{red}{B} \textcolor{blue}{A} \textcolor{blue}{C} \textcolor{yellow}{H} \textcolor{orange}{K} \textcolor{blue}{O} \textcolor{red}{A} \textcolor{red}{H} \textcolor{blue}{A} \textcolor{blue}{N} \textcolor{blue}{O} \textcolor{red}{I} \textcolor{blue}{X}$$
$$K = \textcolor{red}{D} \textcolor{blue}{T} \textcolor{blue}{V} \textcolor{blue}{T} \textcolor{blue}{A}$$

P      C      Ma trận khóa  $5 \times 5$   
 $\textcolor{red}{B} \textcolor{blue}{A} \rightarrow \textcolor{red}{G} \textcolor{blue}{D}$   
 $\textcolor{red}{C} \textcolor{blue}{H} \rightarrow \textcolor{red}{B} \textcolor{blue}{I}$   
 $\textcolor{red}{K} \textcolor{blue}{H} \rightarrow \textcolor{red}{L} \textcolor{blue}{I}$   
 $\textcolor{red}{O} \textcolor{blue}{A} \rightarrow \textcolor{red}{R} \textcolor{blue}{T}$   
 $\textcolor{red}{H} \textcolor{blue}{A} \rightarrow \textcolor{red}{M} \textcolor{blue}{D}$   
 $\textcolor{red}{N} \textcolor{blue}{O} \rightarrow \textcolor{red}{O} \textcolor{blue}{P}$   
 $\textcolor{red}{I} \textcolor{blue}{X} \rightarrow \textcolor{red}{L} \textcolor{blue}{U}$

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

### Example 3.15

Let us encrypt the plaintext “hello” using the key in Figure 3.13.

he → EC

Plaintext: hello

lx → QZ

Ciphertext: ECQZBX

## 3.2.2 *Continued*

### Vigenere Cipher

$$P = P_1 P_2 P_3 \dots$$

$$C = C_1 C_2 C_3 \dots$$

$$K = [(k_1, k_2, \dots, k_m), (k_1, k_2, \dots, k_m), \dots]$$

$$\text{Encryption: } C_i = P_i + k_i$$

$$\text{Decryption: } P_i = C_i - k_i$$

#### Example 3.16

We can encrypt the message “She is listening” using the 6-character keyword “PASCAL”.

Plaintext:	s	h	e	i	s	l	i	s	t	e	n	i	n	g
P's values:	18	07	04	08	18	11	08	18	19	04	13	08	13	06
Key stream:	15	00	18	02	00	11	15	00	18	02	00	11	15	00
C's values:	07	07	22	10	18	22	23	18	11	6	13	19	02	06
Ciphertext:	H	H	W	K	S	W	X	S	L	G	N	T	C	G

## 3.2.2 *Continued*

### Example 3.16

Let us see how we can encrypt the message “She is listening” using the 6-character keyword “PASCAL”. The initial key stream is (15, 0, 18, 2, 0, 11). The key stream is the repetition of this initial key stream (as many times as needed).

Xem cách có thể mã hóa thông điệp “She is listening” bằng cách sử dụng từ khóa 6 ký tự “PASCAL”. Luồng khóa ban đầu là (15, 0, 18, 2, 0, 11). Luồng khóa là sự lặp lại của luồng khóa ban đầu này (dùng nhiều lần nếu cần).

Plaintext:	s	h	e	i	s	l	i	s	t	e	n	i	n	g
P's values:	18	07	04	08	18	11	08	18	19	04	13	08	13	06
Key stream:	15	00	18	02	00	11	15	00	18	02	00	11	15	00
C's values:	07	07	22	10	18	22	23	18	11	6	13	19	02	06
Ciphertext:	H	H	W	K	S	W	X	S	L	G	N	T	C	G

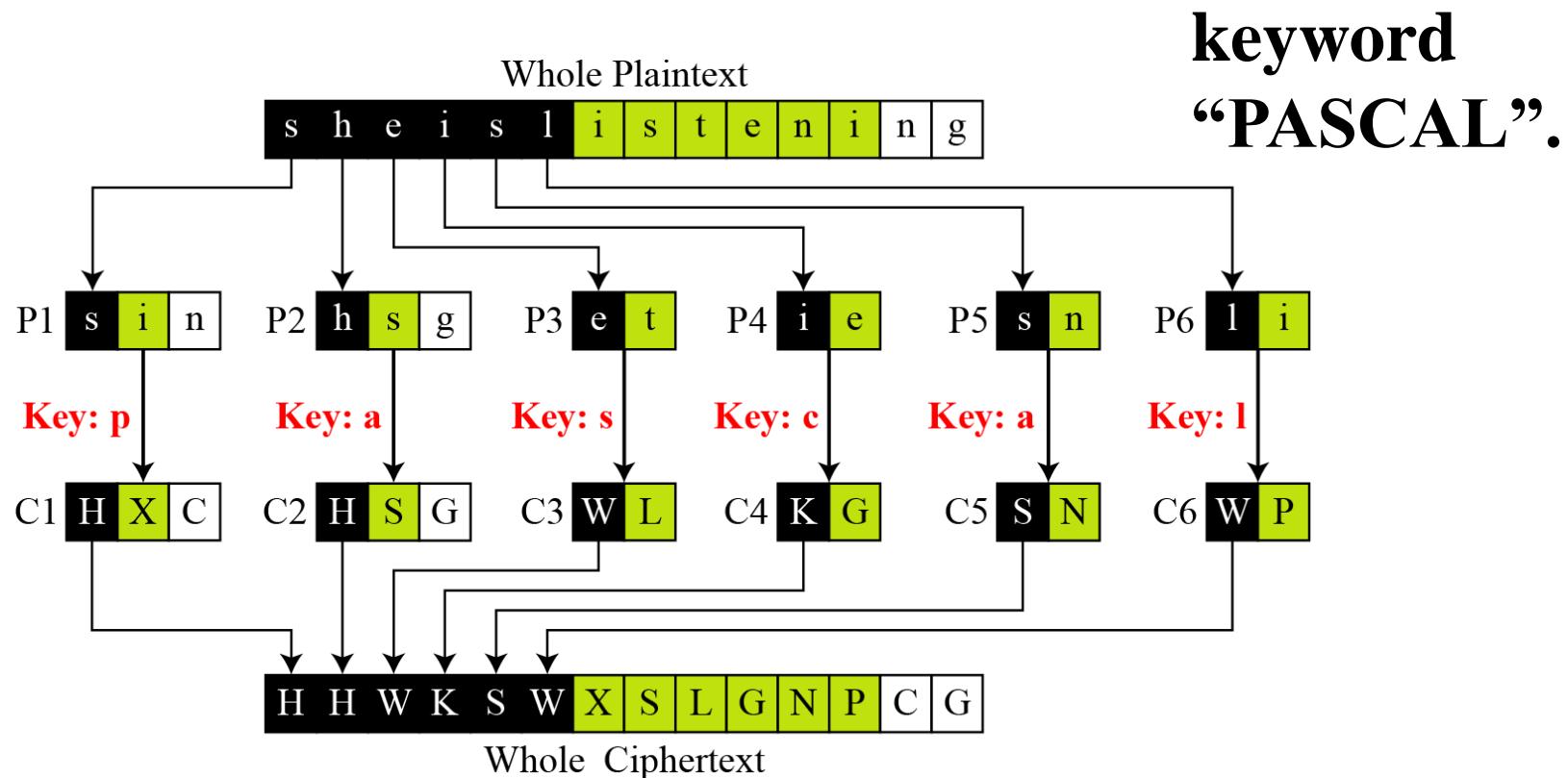
## 3.2.2 *Continued*

### Example 3.17

Mật mã Vigenere có thể được xem là sự kết hợp của m mật mã cộng.

**Figure 3.14** A Vigenere cipher as a combination of m additive ciphers

Mật mã Vigenere là sự kết hợp của m mật mã cộng



## 3.2.2 *Continued*

### Example 3.18

Using Example 3.18, we can say that the additive cipher is a special case of Vigenere cipher in which  $m = 1$ .

	a	b	c	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t	v	v	w	x	y	z
A	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
B	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	A
C	C	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
D	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
E	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	D
F	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E
G	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F
H	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G
I	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H
J	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I
K	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J
L	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K
M	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L
N	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M
O	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N
P	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O
Q	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P
R	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q
S	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R
T	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S
U	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T
V	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U
W	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V
X	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W
Y	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X
Z	Z	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

**Table 3.3**  
*A Vigenere Table*

## 3.2.2 *Continued*

### Vigenere Cipher (Crypanalysis)

#### Example 3.19

Giả sử chúng tôi đã chặn đoạn mã sau:

LIOMWGFEGGDVWGHHCQUCRHRWAGWIOWQLKGZETKKMEVLWPCZVGTH-  
VTSGXQOVGCSVETQLTJSUMVVVEUVLXEWSLGZMVVWLGYHCUSWXQH-  
KVGSHEEVFLCFDGVSUMPHKIRZDMPHHBVWWJWIXGFWLTSHGJOUEEHH-  
VUCFVGOWICQLTJSUXGLW

Kiểm tra Kasiski về sự lặp lại của các đoạn ba ký tự cho kết quả như trong Bảng 3.4.

<i>String</i>	<i>First Index</i>	<i>Second Index</i>	<i>Difference</i>
JSU	68	168	100
SUM	69	117	48
VWV	72	132	60
MPH	119	127	8

## 3.2.2 *Continued*

### Example 3.19

Let us assume we have intercepted the following ciphertext:

LIOMWGEGGDVWGHHCQUCRHRWAGWIOWQLKGZETKKMEVLWPCZVGTH-  
VTSGXQOVGCSVETQLTJSUMVVVEUVLXEWSLGFMVVWLGYHCUSWXQH-  
KVGSHEEVFLCFDGVSUMPHKIRZDMPHHBVWVWJWIXGFWLTSHGJOUEEHH-  
VUCFVGOWICQLTJSUXGLW

The Kasiski test for repetition of three-character segments yields the results shown in Table 3.4.

<i>String</i>	<i>First Index</i>	<i>Second Index</i>	<i>Difference</i>
JSU	68	168	100
SUM	69	117	48
VWV	72	132	60
MPH	119	127	8

## 3.2.2 *Continued*

### Example 3.19 (Continued)

The greatest common divisor of differences is 4, which means that the key length is multiple of 4. First try  $m = 4$ .

*Ước chung lớn nhất của các khác biệt là 4, có nghĩa là độ dài khóa là bội số của 4. Đầu tiên hãy thử  $m = 4$ .*

C1 : LWGWCRAOKTEPGTQCTJVUEGVGUQGECVPRPVJGTJEUGCJG

P1 : jueuapymircneroarhtsthihytrahcieixsthcarrehe

C2 : IGGGQHGWGKVCTSOSQS WVWFVYSHSVF SHZHWWF SOHCOQSL

P2 : ussscts is who feaeceihcetes oecatn p nther hctecex

C3 : OFDHURWQZKLZHGVVLUVLSZWHWKHF DUKDHVIWHUHF WL UW

P3 : lcaerotnwhi wed ssirsi irhkete hretl t i ideat rairt

C4 : MEVHCWILEMWVVXGETMEXMLCXVELGMIMBWXLGEVVITX

P4 : i ardysehaisrrt capiafpwtet hecarhaesf terectpt

Trong trường hợp này, bản rõ có ý nghĩa.

---

Julius Caesar used a cryptosystem in his wars, which is now referred to as Caesar cipher.

It is an additive cipher with the key set to three. Each character in the plaintext is shifted three characters to create ciphertext.

---

## 3.2.2 *Continued*

### Hill Cipher: Mă Hill

Figure 3.15 Key in the Hill cipher

$$K = \begin{bmatrix} k_{11} & k_{12} & \dots & k_{1m} \\ k_{21} & k_{22} & \dots & k_{2m} \\ \vdots & \vdots & & \vdots \\ k_{m1} & k_{m2} & \dots & k_{mm} \end{bmatrix}$$

$$\begin{aligned} C_1 &= P_1 k_{11} + P_2 k_{21} + \dots + P_m k_{m1} \\ C_2 &= P_1 k_{12} + P_2 k_{22} + \dots + P_m k_{m2} \\ &\dots \\ C_m &= P_1 k_{1m} + P_2 k_{2m} + \dots + P_m k_{mm} \end{aligned}$$

**Note**

*Ma trận khóa trong mật mã Hill cần có một nghịch đảo nhân.*

The key matrix in the Hill cipher needs to have a multiplicative inverse.

## 3.2.2 *Continued*

### Example 3.20

For example, the plaintext “code is ready” can make a  $3 \times 4$  matrix when adding extra bogus character “z” to the last block and removing the spaces. The ciphertext is “OHKNIHGKLSS”.

*Ví dụ, bản rõ “code is ready” có thể tạo ma trận  $3 \times 4$  khi thêm ký tự không có thật “z” vào khối cuối cùng và loại bỏ khoảng trắng. Bản mã là “OHKNIHGKLSS”.*

**Figure 3.16 Example 3.20**

$$\begin{bmatrix} 14 & 07 & 10 & 13 \\ 08 & 07 & 06 & 11 \\ 11 & 08 & 18 & 18 \end{bmatrix}^C = \begin{bmatrix} 02 & 14 & 03 & 04 \\ 08 & 18 & 17 & 04 \\ 00 & 03 & 24 & 25 \end{bmatrix}^P \begin{bmatrix} 09 & 07 & 11 & 13 \\ 04 & 07 & 05 & 06 \\ 02 & 21 & 14 & 09 \\ 03 & 23 & 21 & 08 \end{bmatrix}^K$$

a. Encryption

$$\begin{bmatrix} 02 & 14 & 03 & 04 \\ 08 & 18 & 17 & 04 \\ 00 & 03 & 24 & 25 \end{bmatrix}^P = \begin{bmatrix} 14 & 07 & 10 & 13 \\ 08 & 07 & 06 & 11 \\ 11 & 08 & 18 & 18 \end{bmatrix}^C \begin{bmatrix} 02 & 15 & 22 & 03 \\ 15 & 00 & 19 & 03 \\ 09 & 09 & 03 & 11 \\ 17 & 00 & 04 & 07 \end{bmatrix}^{K^{-1}}$$

b. Decryption

## 3.2.2 *Continued*

### Example 3.21

Assume that Eve knows that  $m = 3$ . She has intercepted three plaintext/ciphertext pair blocks (not necessarily from the same message) as shown in Figure 3.17.

*Giả sử rằng Eve biết rằng  $m = 3$ . Cô ấy đã chặn ba khối cặp bản rõ / bản mã (không nhất thiết phải từ cùng một thông điệp) như trong Hình 3.17.*

**Figure 3.17 Example 3.21**

$$\begin{bmatrix} 05 & 07 & 10 \end{bmatrix} \longleftrightarrow \begin{bmatrix} 03 & 06 & 00 \end{bmatrix}$$

$$\begin{bmatrix} 13 & 17 & 07 \end{bmatrix} \longleftrightarrow \begin{bmatrix} 14 & 16 & 09 \end{bmatrix}$$

$$\begin{bmatrix} 00 & 05 & 04 \end{bmatrix} \longleftrightarrow \begin{bmatrix} 03 & 17 & 11 \end{bmatrix}$$

P

C

## 3.2.2 *Continued*

### Example 3.21 (Continued)

She makes matrices P and C from these pairs. Because P is invertible, she inverts the P matrix and multiplies it by C to get the K matrix as shown in Figure 3.18.

Cô ấy tạo ma trận P và C từ các cặp này. Vì P khả nghịch nên cô ấy đảo ngược ma trận P và nhân nó với C để được ma trận K như trong hình 3.18.

**Figure 3.18 Example 3.21**

$$\begin{bmatrix} 02 & 03 & 07 \\ 05 & 07 & 09 \\ 01 & 02 & 11 \end{bmatrix} = \begin{bmatrix} 21 & 14 & 01 \\ 00 & 08 & 25 \\ 13 & 03 & 08 \end{bmatrix} \begin{bmatrix} 03 & 06 & 00 \\ 14 & 16 & 09 \\ 03 & 17 & 11 \end{bmatrix}$$

**K**                    **P<sup>-1</sup>**                    **C**

Now she has the key and can break any ciphertext encrypted with that key.

### 3.2.2 *Continued*

#### One-Time Pad: Bảng dùng một lần

One of the goals of cryptography is perfect secrecy. A study by Shannon has shown that perfect secrecy can be achieved if each plaintext symbol is encrypted with a key randomly chosen from a key domain. This idea is used in a cipher called one-time pad, invented by **Vernam**.

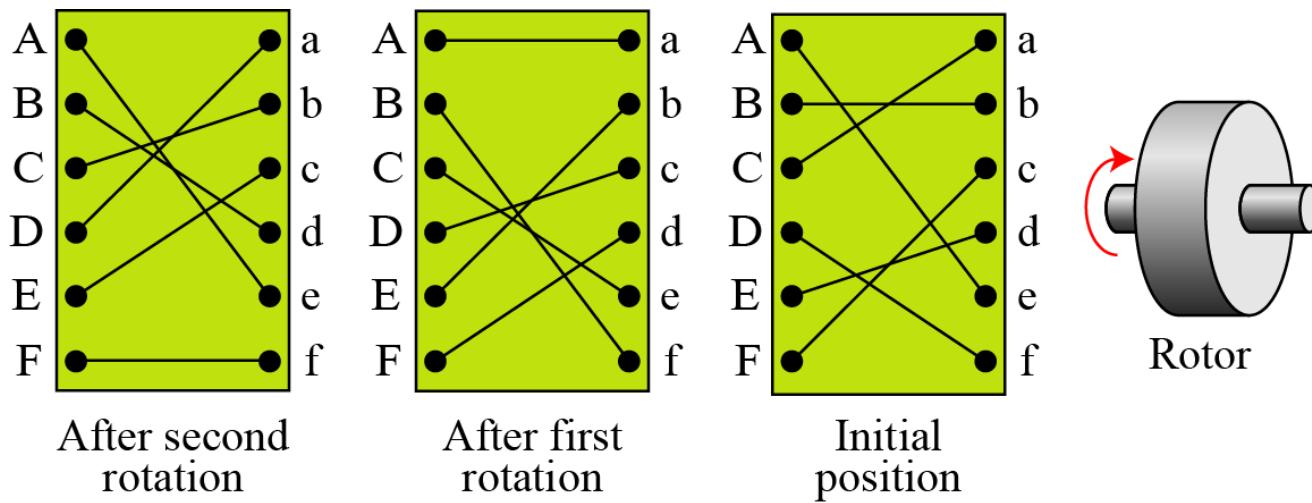
*Một trong những mục tiêu của mật mã là bí mật hoàn hảo. Một nghiên cứu của Shannon đã chỉ ra rằng có thể đạt được sự bí mật hoàn hảo nếu mỗi ký hiệu bản rõ được mã hóa bằng một khóa được chọn ngẫu nhiên từ một miền khóa.*

*Ý tưởng này được sử dụng trong một mật mã được gọi là bảng một lần, do Vernam phát minh.*

## 3.2.2 *Continued*

### Rotor Cipher

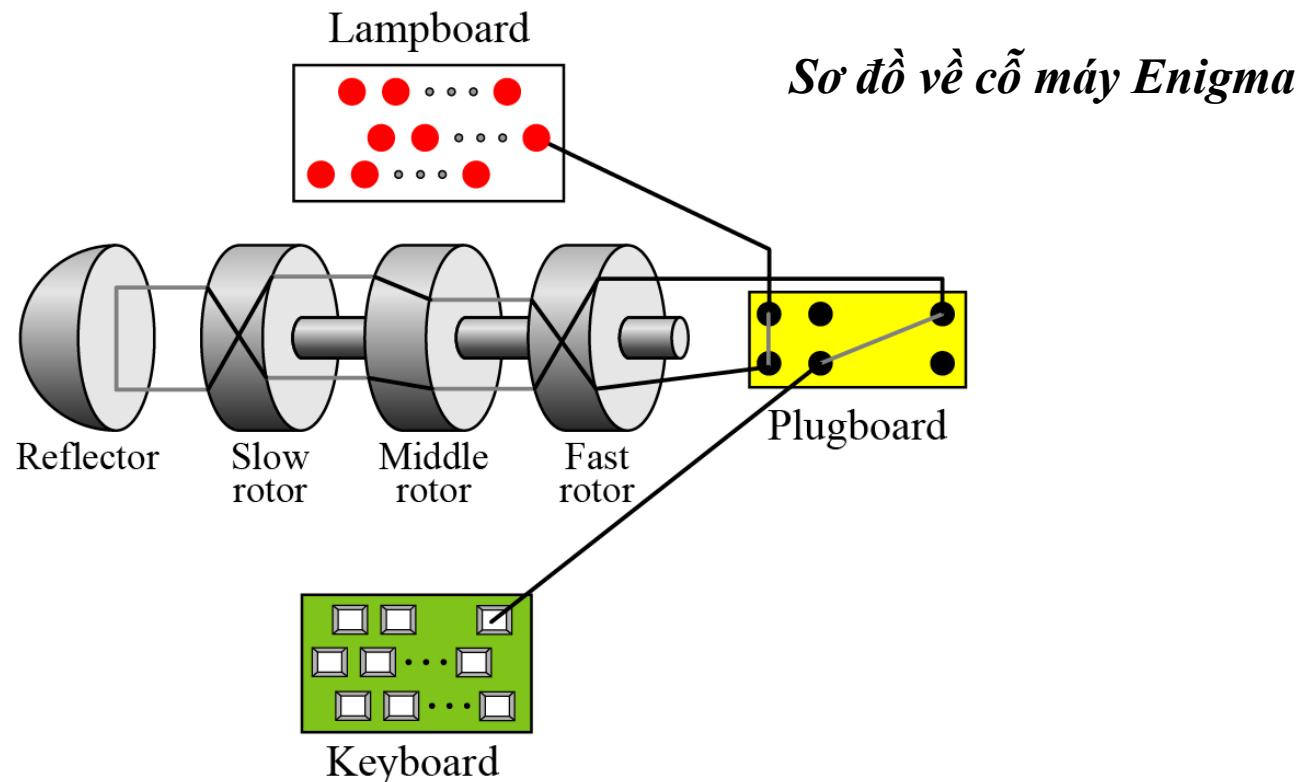
**Figure 3.19 A rotor cipher**



## 3.2.2 *Continued*

### Enigma Machine

**Figure 3.20** *A schematic of the Enigma machine*



## 3-3 TRANSPOSITION CIPHERS: MÃ CHUYỂN VỊ

*A transposition cipher does not substitute one symbol for another, instead it changes the location of the symbols.*

*Mật mã chuyển vị không thay thế một ký hiệu này cho một ký hiệu khác, thay vào đó nó thay đổi vị trí của các ký hiệu.*

**Note**

→ Mật mã chuyển vị sắp xếp lại các ký hiệu.

**A transposition cipher reorders symbols.**

**Topics discussed in this section:**

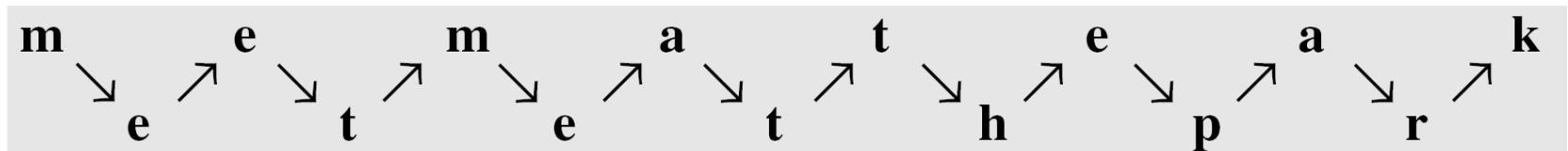
- 3.3.1 Keyless Transposition Ciphers**
- 3.3.2 Keyed Transposition Ciphers**
- 3.3.3 Combining Two Approaches**

### 3.3.1 Keyless Transposition Ciphers: *Mã chuyển vị không khóa*

Simple transposition ciphers, which were used in the past, are keyless.

#### Example 3.22

Một ví dụ điển hình về mật mã không khóa sử dụng phương pháp đầu tiên là mật mã hàng rào đường sắt (**rail fence cipher**). Bản mã được tạo để đọc từng dòng mẫu. Ví dụ: để gửi tin nhắn “Meet me at the park” cho Bob, Alice viết



She then creates the ciphertext “**MEMATEAKETETHPR**”.

### 3.3.1 *Continued*

#### Example 3.23

Alice and Bob can agree on the number of columns and use the second method. Alice writes the same plaintext, row by row, in a table of four columns.

m	e	e	t
m	e	a	t
t	h	e	p
a	r	k	

She then creates the ciphertext “MMTAEEHREAEKTP”.

### 3.3.1 *Continued*

#### Example 3.24

The cipher in Example 3.23 is actually a transposition cipher. The following shows the **permutation** of each character in the plaintext into the ciphertext based on the positions.

01	02	03	04	05	06	07	08	09	10	11	12	13	14	15
↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓
01	05	09	13	02	06	10	13	03	07	11	15	04	08	12

The second character in the plaintext has moved to the fifth position in the ciphertext; the third character has moved to the ninth position; and so on. Although the characters are permuted, there is a pattern in the permutation: (01, 05, 09, 13), (02, 06, 10, 13), (03, 07, 11, 15), and (08, 12). In each section, the difference between the two adjacent numbers is 4.

### 3.3.2 *Keyed Transposition Ciphers:* *Mã chuyển vị có khóa*

The keyless ciphers permute the characters by using writing plaintext in one way and reading it in another way. The permutation is done on the whole plaintext to create the whole ciphertext. Another method is to *divide the plaintext into groups of predetermined size, called blocks*, and then use a key to permute the characters in each block separately.

*Các mật mã không khóa hoán vị các ký tự bằng cách viết bản rõ theo cách này và đọc theo cách khác. Hoán vị được thực hiện trên toàn bộ bản rõ để tạo ra toàn bộ bản mã.*

*Một phương pháp khác là chia bản rõ thành các nhóm có kích thước xác định trước, được gọi là các khối, sau đó sử dụng một khóa để hoán vị các ký tự trong mỗi khối riêng biệt.*

## 3.3.2 *Continued*

### Example 3.25

Alice needs to send the message “Enemy attacks tonight” to Bob..

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

The key used for encryption and decryption is a *permutation key*, which shows how the characters are permuted.

Encryption ↓

3	1	4	5	2
1	2	3	4	5

↑ Decryption

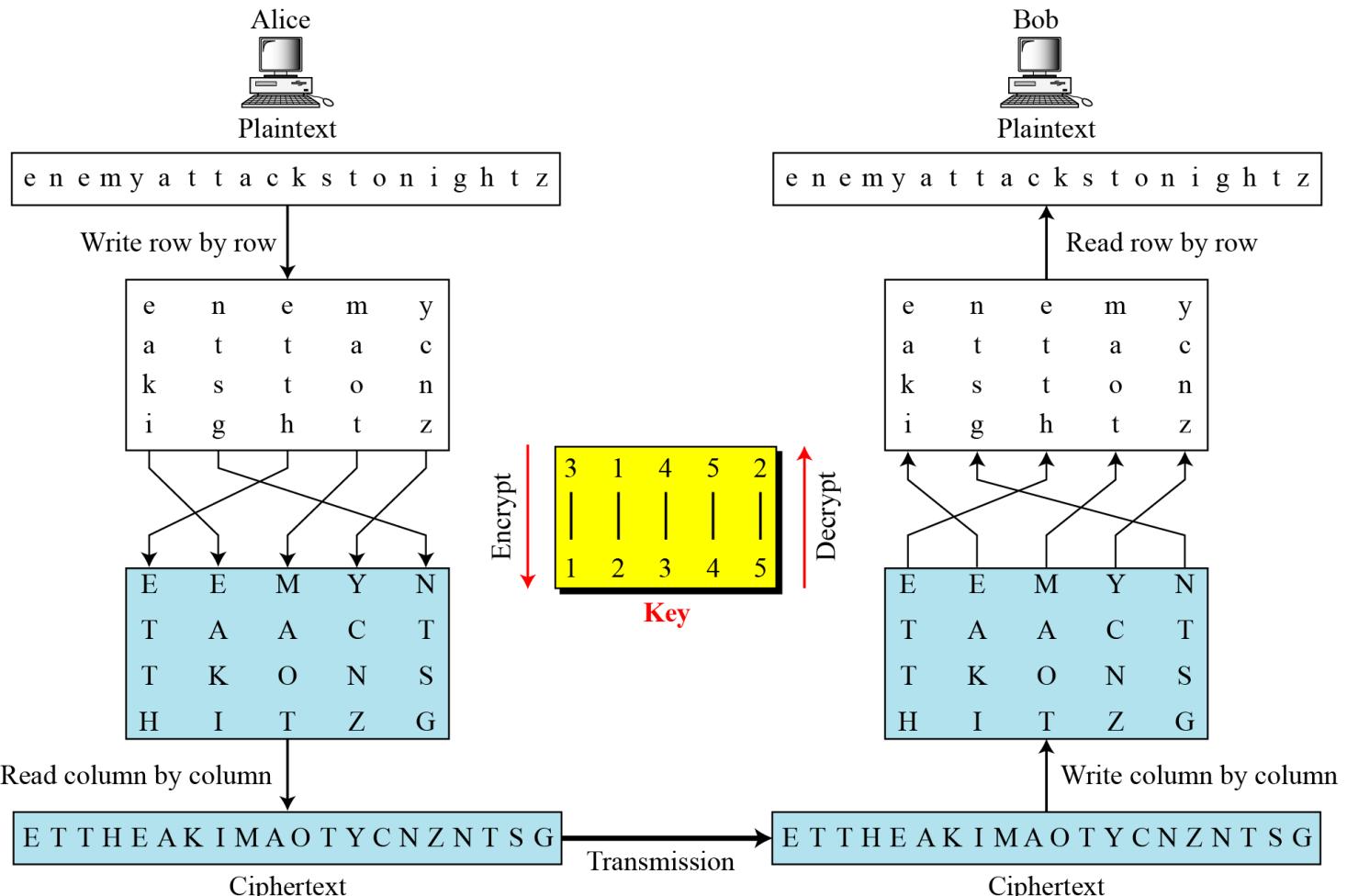
The permutation yields

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

### 3.3.3 Combining Two Approaches: Mã kết hợp chuyển vị có/không có khóa

Example 3.26

Figure 3.21



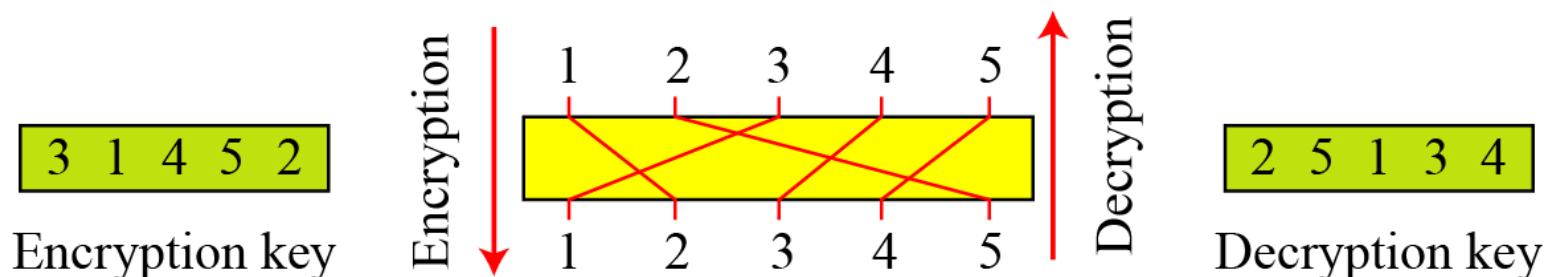
### 3.3.3 *Continued*

#### Keys

In Example 3.21, a single key was used in two directions for the column exchange: downward for encryption, upward for decryption. It is customary to create two keys.

*Một khóa duy nhất đã được sử dụng theo hai hướng để trao đổi cột: hướng xuống để mã hóa, hướng lên để giải mã. Theo thông lệ, bạn nên tạo hai khóa.*

**Figure 3.22** Encryption/decryption keys in transpositional ciphers



### 3.3.3 *Continued*

**Figure 3.23 Đảo khóa trong mật mã chuyển vị**

Encryption key

2 6 3 1 4 7 5

2 6 3 1 4 7 5  
Add index

1 2 3 4 5 6 7

Swap

1 2 3 4 5 6 7  
2 6 3 1 4 7 5

Hoán  
đổi

4 1 3 5 7 2 6

4 1 3 5 7 2 6  
1 2 3 4 5 6 7

Sort  
Sắp xếp

Decryption key

a. Manual process

Given: EncKey [index]

index  $\leftarrow 1$

while (index  $\leq$  Column)

{

    DecKey[EncKey[index]]  $\leftarrow$  index  
    index  $\leftarrow$  index + 1

}

Return : DecKey [index]

b. Algorithm

### 3.3.3 *Continued*

#### Using Matrices

We can use matrices to show the encryption/decryption process for a transposition cipher.

Chúng ta có thể sử dụng ma trận để biểu thị quá trình mã hóa / giải mã cho mật mã chuyen vị.

#### Example 3.27

Figure 3.24 Biểu diễn khóa dưới dạng ma trận trong mật mã chuyen vị

$$\begin{matrix} & 3 & 1 & 4 & 5 & 2 \\ \downarrow & \downarrow & \downarrow & \downarrow & \downarrow & \downarrow \\ \left[ \begin{matrix} 04 & 13 & 04 & 12 & 24 \\ 00 & 19 & 19 & 00 & 02 \\ 10 & 18 & 19 & 14 & 13 \\ 08 & 06 & 07 & 19 & 25 \end{matrix} \right] & \times & \left[ \begin{matrix} 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 \\ 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 \end{matrix} \right] & = & \left[ \begin{matrix} 04 & 04 & 12 & 24 & 13 \\ 19 & 00 & 00 & 02 & 19 \\ 19 & 10 & 14 & 13 & 18 \\ 07 & 08 & 19 & 25 & 06 \end{matrix} \right] \\ \text{Plaintext} & & \text{Encryption key} & & \text{Ciphertext} \end{matrix}$$

### 3.3.3 *Continued*

#### Example 3.27

Figure 3.24 shows the encryption process. Multiplying the  $4 \times 5$  plaintext matrix by the  $5 \times 5$  encryption key gives the  $4 \times 5$  ciphertext matrix.

Hình 3.24 cho thấy quá trình mã hóa. Nhân ma trận bản rõ  $4 \times 5$  với khóa mã hóa  $5 \times 5$  sẽ cho ma trận mã hóa  $4 \times 5$ .

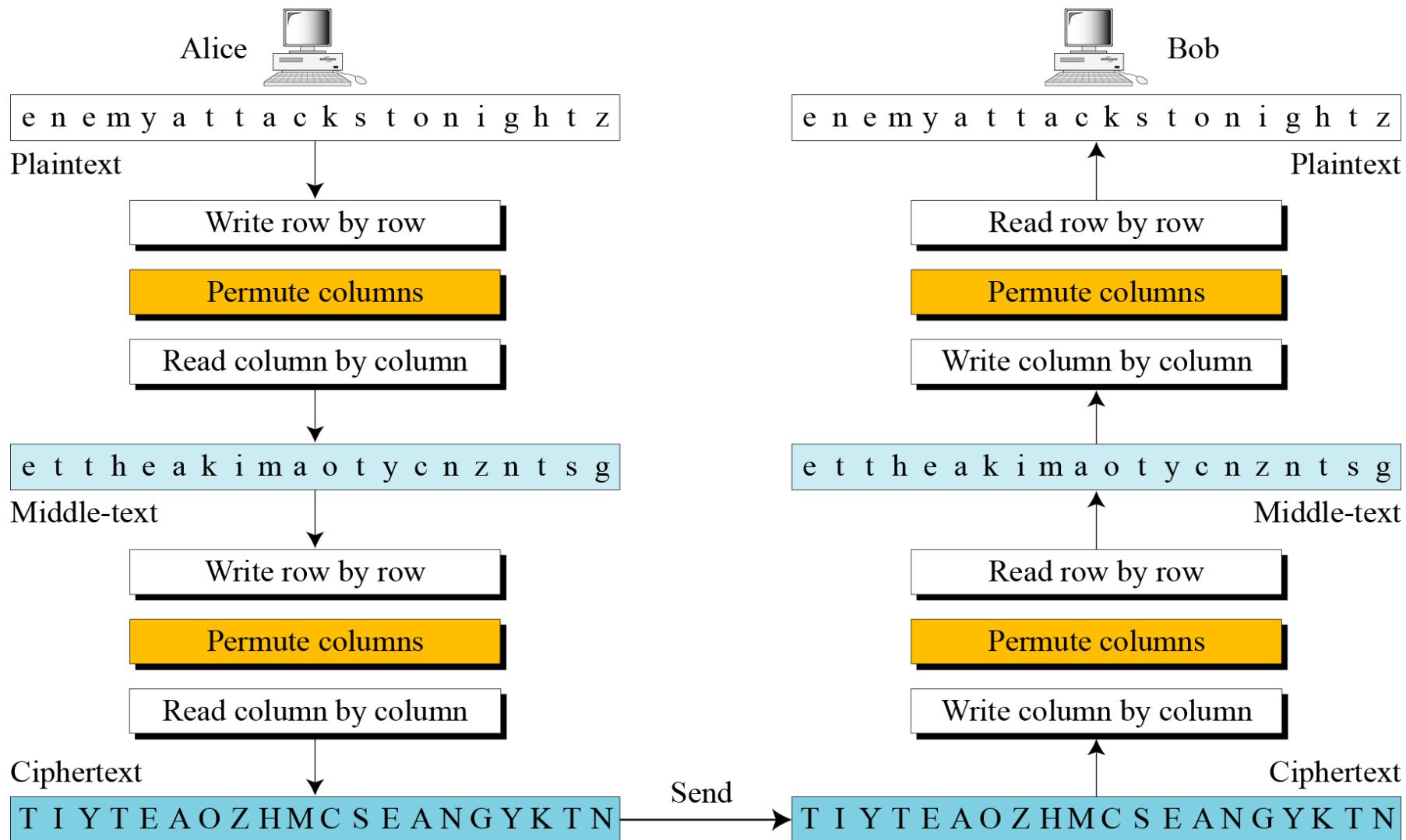
Figure 3.24 Biểu diễn khóa dưới dạng ma trận trong mật mã chuyển vị

$$\begin{bmatrix} 04 & 13 & 04 & 12 & 24 \\ 00 & 19 & 19 & 00 & 02 \\ 10 & 18 & 19 & 14 & 13 \\ 08 & 06 & 07 & 19 & 25 \end{bmatrix}_{\text{Plaintext}} \times \begin{bmatrix} 3 & 1 & 4 & 5 & 2 \\ \downarrow & \downarrow & \downarrow & \downarrow & \downarrow \\ 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 \\ 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 \end{bmatrix}_{\text{Encryption key}} = \begin{bmatrix} 04 & 04 & 12 & 24 & 13 \\ 19 & 00 & 00 & 02 & 19 \\ 19 & 10 & 14 & 13 & 18 \\ 07 & 08 & 19 & 25 & 06 \end{bmatrix}_{\text{Ciphertext}}$$

### 3.3.3 *Continued*

## Double Transposition Ciphers

Figure 3.25 Mật mã chuyển vị kép



## 3-4 STREAM AND BLOCK CIPHERS

*Tài liệu chia mật mã đối xứng thành hai loại lớn: mật mã dòng và mật mã khối. Mặc dù các định nghĩa thường được áp dụng cho mật mã hiện đại, cách phân loại này cũng áp dụng cho mật mã truyền thống.*

### *Topics discussed in this section:*

- 3.4.1 Stream Ciphers**
- 3.4.2 Block Ciphers**
- 3.4.3 Combination**

### 3.4.1 Stream Ciphers

Call the plaintext stream  $P$ , the ciphertext stream  $C$ , and the key stream  $K$ .

$$P = P_1 P_2 P_3, \dots$$

$$C = C_1 C_2 C_3, \dots$$

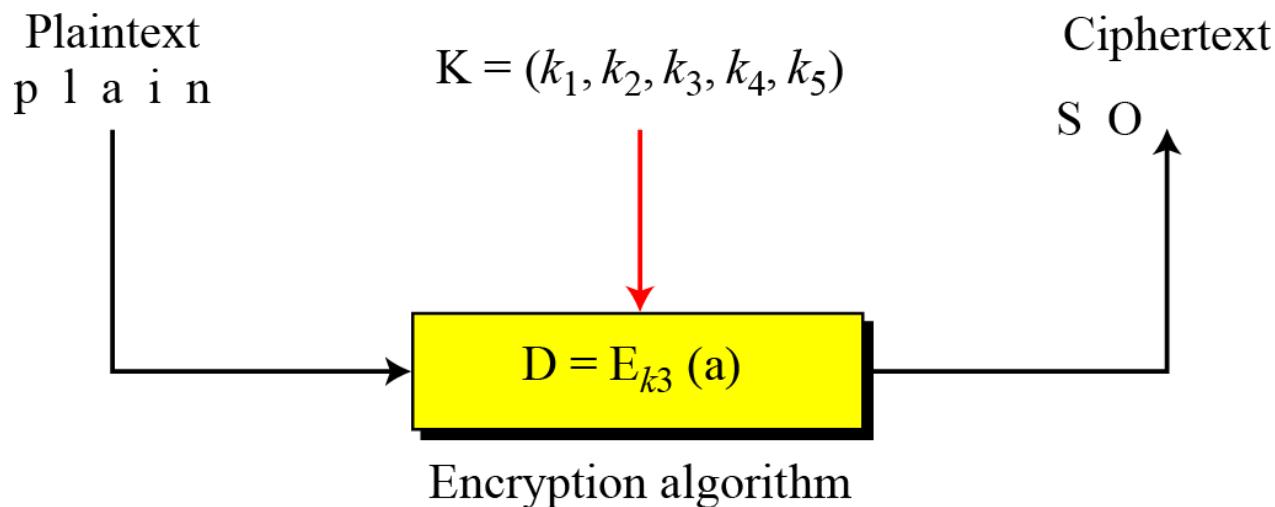
$$K = (k_1, k_2, k_3, \dots)$$

$$C_1 = E_{k1}(P_1)$$

$$C_2 = E_{k2}(P_2)$$

$$C_3 = E_{k3}(P_3) \dots$$

**Figure 3.26 Stream cipher**



### 3.4.1 *Continued*

#### Example 3.30

Mật mã cộng có thể được phân loại là mật mã dòng trong đó dòng khóa là giá trị lặp lại của khóa. Nói cách khác, dòng khóa được coi là một dòng khóa được xác định trước hoặc  $K = (k, k, \dots, k)$ . Tuy nhiên, trong mật mã này, mỗi ký tự trong bản mã chỉ phụ thuộc vào ký tự tương ứng trong bản rõ, vì dòng khóa được tạo ra một cách độc lập.

#### Example 3.31

Các mật mã thay thế đơn ký tự được thảo luận trong chương này cũng là mật mã dòng. Tuy nhiên, mỗi giá trị của dòng khóa trong trường hợp này là ánh xạ của ký tự bản rõ hiện tại với ký tự bản mã tương ứng trong bảng ánh xạ.

### 3.4.1 *Continued*

#### Example 3.32

Mật mã Vigenere cũng là mật mã dòng theo định nghĩa. Trong trường hợp này, dòng khóa là sự lặp lại của m giá trị, trong đó m là kích thước của từ khóa. Nói cách khác,

$$K = (k_1, k_2, \dots, k_m, k_1, k_2, \dots, k_m, \dots)$$

#### Example 3.33

Chúng ta có thể thiết lập một tiêu chí để phân chia mật mã dòng dựa trên các dòng chính của chúng. Chúng ta có thể nói rằng mật mã dòng là mật mã đơn ký tự nếu giá trị của ki không phụ thuộc vào vị trí của ký tự bản rõ trong dòng bản rõ; nếu không, mật mã là đa ký tự.

### 3.4.1 *Continued*

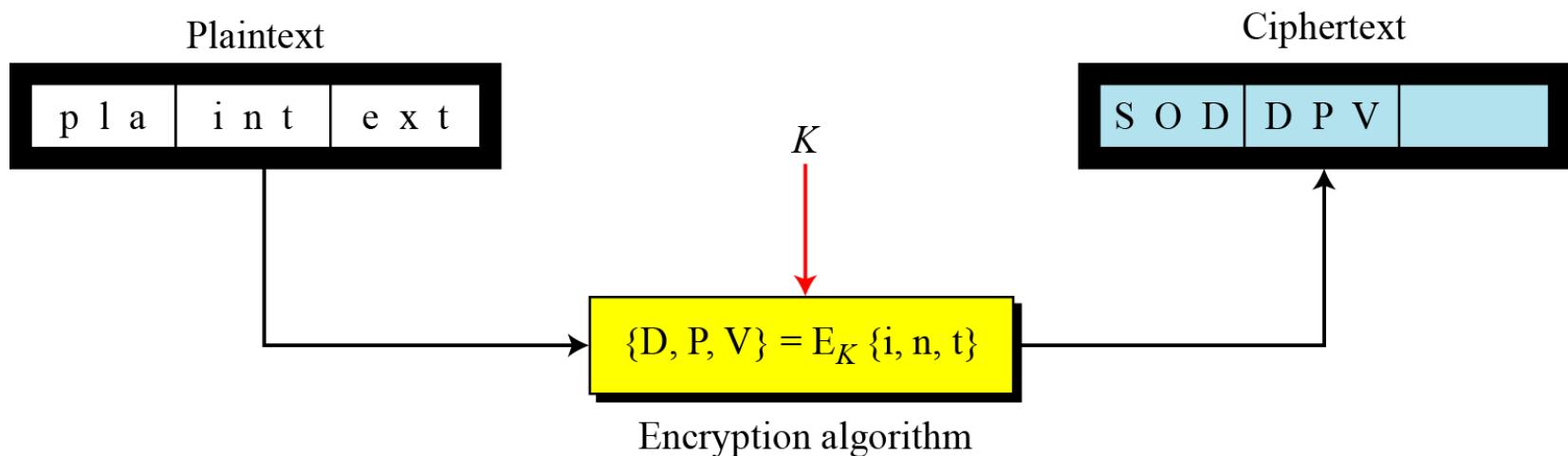
#### Example 3.33 (Continued)

- Additive ciphers are definitely monoalphabetic because  $k_i$  in the key stream is fixed; it does not depend on the position of the character in the plaintext.
- Monoalphabetic substitution ciphers are monoalphabetic because  $k_i$  does not depend on the position of the corresponding character in the plaintext stream; it depends only on the value of the plaintext character.
- Vigenere ciphers are polyalphabetic ciphers because  $k_i$  definitely depends on the position of the plaintext character. However, the dependency is cyclic. The key is the same for two characters  $m$  positions apart.

### 3.4.2 Block Ciphers

Trong mật mã khối, một nhóm các ký hiệu bản rõ có kích thước m ( $m > 1$ ) được mã hóa cùng nhau tạo ra một nhóm bản mã có cùng kích thước. Một khóa duy nhất được sử dụng để mã hóa toàn bộ khối ngay cả khi khóa được tạo từ nhiều giá trị. Hình 3.27 cho thấy khái niệm về mật mã khối.

Figure 3.27 Block cipher



## 3.4.2 *Continued*

### Example 3.34

Mật mã Playfair là mật mã khối. Kích thước của khối là  $m = 2$ . Hai ký tự được mã hóa cùng nhau.

### Example 3.35

Mật mã Hill là mật mã khối. Một khối văn bản rõ, có kích thước từ 2 trở lên được mã hóa cùng nhau bằng một khóa duy nhất (ma trận). Trong các mật mã này, giá trị của mỗi ký tự trong bản mã phụ thuộc vào tất cả các giá trị của các ký tự trong bản rõ. Mặc dù khóa được tạo ra từ các giá trị  $m \times m$ , nó được coi là một khóa duy nhất.

### Example 3.36

Từ định nghĩa về mật mã khối, rõ ràng là mọi mật mã khối đều là mật mã đa ký tự vì mỗi ký tự trong khối bản mã ( $C$ ) phụ thuộc vào tất cả các ký tự trong khối bản rõ ( $P$ ).

### *3.4.3 Combination*

In practice, blocks of plaintext are encrypted individually, but they use a stream of keys to encrypt the whole message block by block. In other words, the cipher is a block cipher when looking at the individual blocks, but it is a stream cipher when looking at the whole message considering each block as a single unit.

*Trong thực tế, các khối văn bản rõ được mã hóa riêng lẻ, nhưng chúng sử dụng một luồng các khóa để mã hóa toàn bộ thông điệp theo từng khối. Nói cách khác, mật mã là một mật mã khối khi nhìn vào các khối riêng lẻ, nhưng nó là một mật mã dòng khi xem xét toàn bộ thông điệp - coi mỗi khối là một đơn vị duy nhất.*