



# Information Security Systems (CS-408)

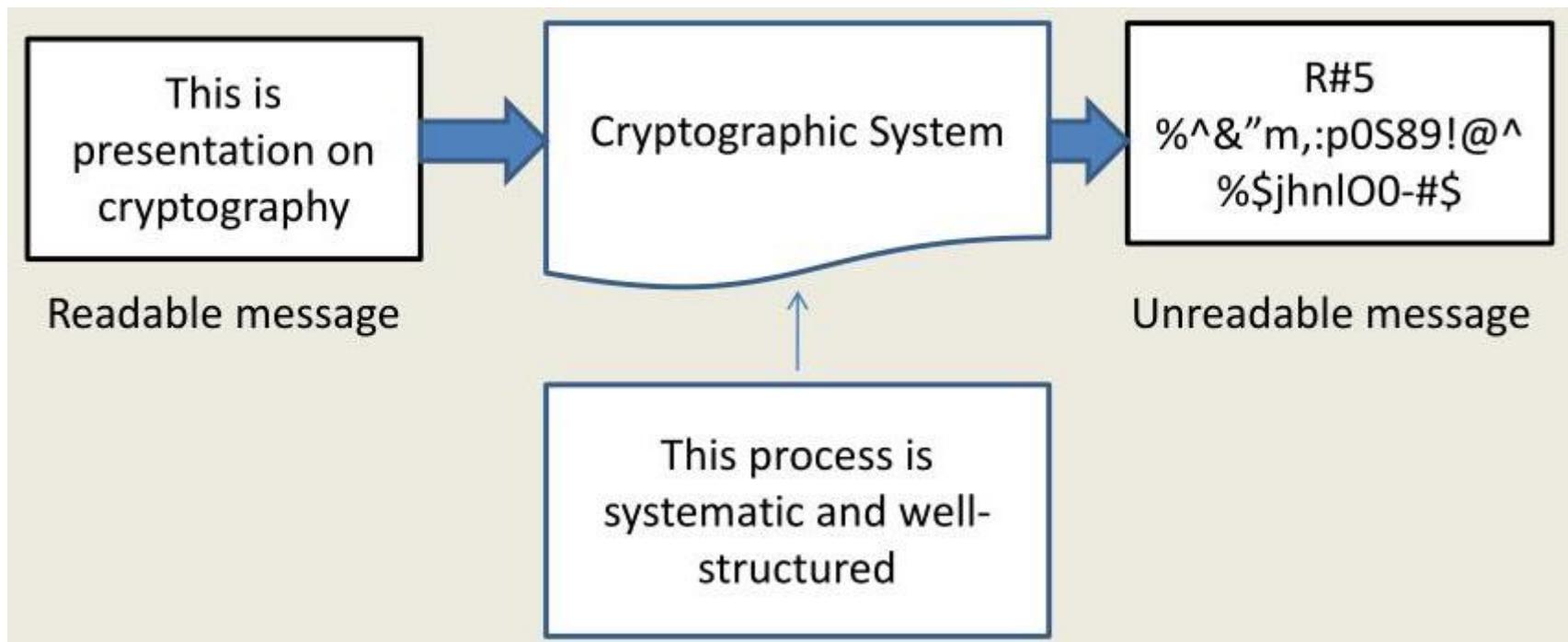
## Foundations of Cryptography & Security

*Dr Samayveer Singh  
Assistant Professor*

*Department of Computer Science & Engineering  
National Institute Technology Jalandhar, Punjab, India  
[samays@nitj.ac.in](mailto:samays@nitj.ac.in)*

# Cryptography

- ✓ Cryptography is the art and science of achieving security by encoding messages to make them impossible to understand.



# Cryptography

- ✓ Cryptography is the study of secure communications techniques that allow only the sender and intended recipient of a message to view its contents.
- ✓ The term is derived from the Greek word kryptos, which means hidden.
- ✓ It is closely associated to encryption, which is the act of scrambling ordinary text into what's known as ciphertext and then back again upon arrival.

# **Some Basic Terminology**

**Plaintext** - original message

**Ciphertext** - coded message

**Cipher** - algorithm for transforming plaintext to ciphertext

**Key** - info used in cipher known only to sender/receiver

**Encipher (encrypt)** - converting plaintext to ciphertext

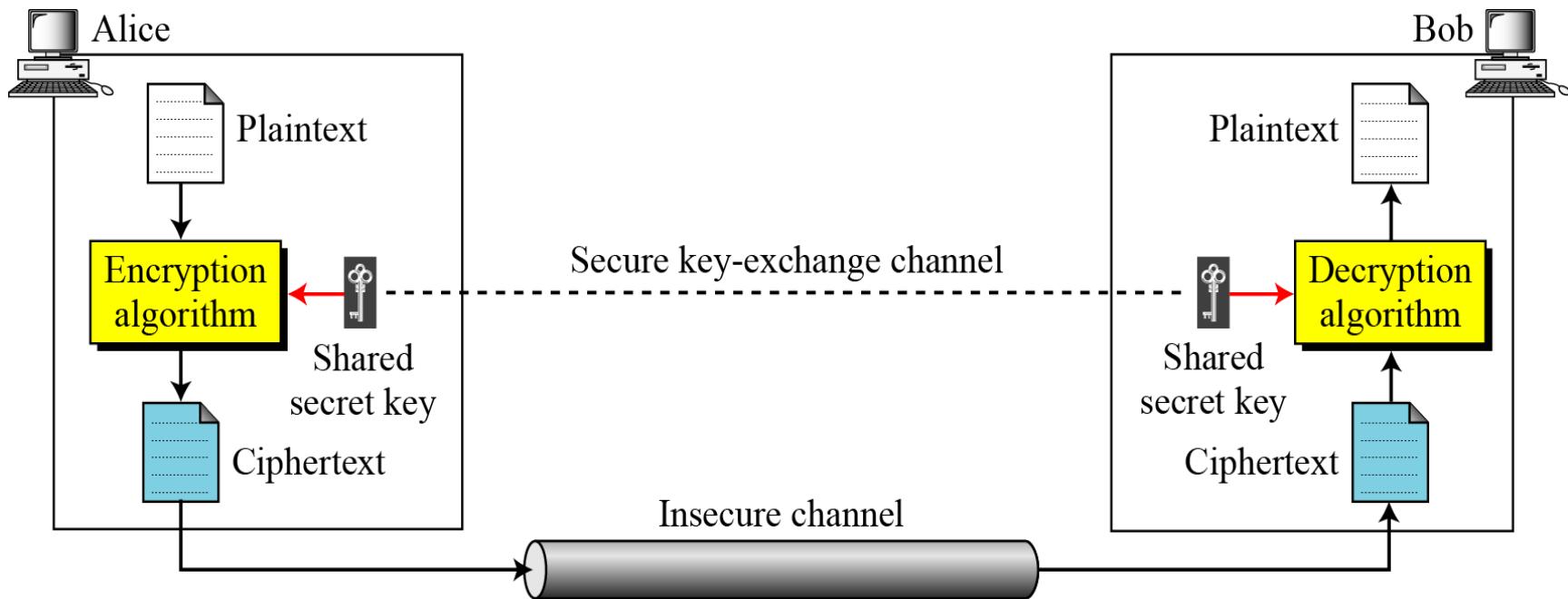
**Decipher (decrypt)** - recovering plaintext from ciphertext

**Cryptography** - study of encryption principles/methods

**Cryptanalysis (codebreaking)** - study of principles/methods of deciphering ciphertext without knowing key

**Cryptology** - field of both cryptography and cryptanalysis

# Symmetric Cipher Model



**Figure 1** General idea of symmetric-key cipher

# Continued

*If P is the plaintext, C is the ciphertext, and K is the key,*

Encryption:  $C = E_k(P)$

Decryption:  $P = D_k(C)$

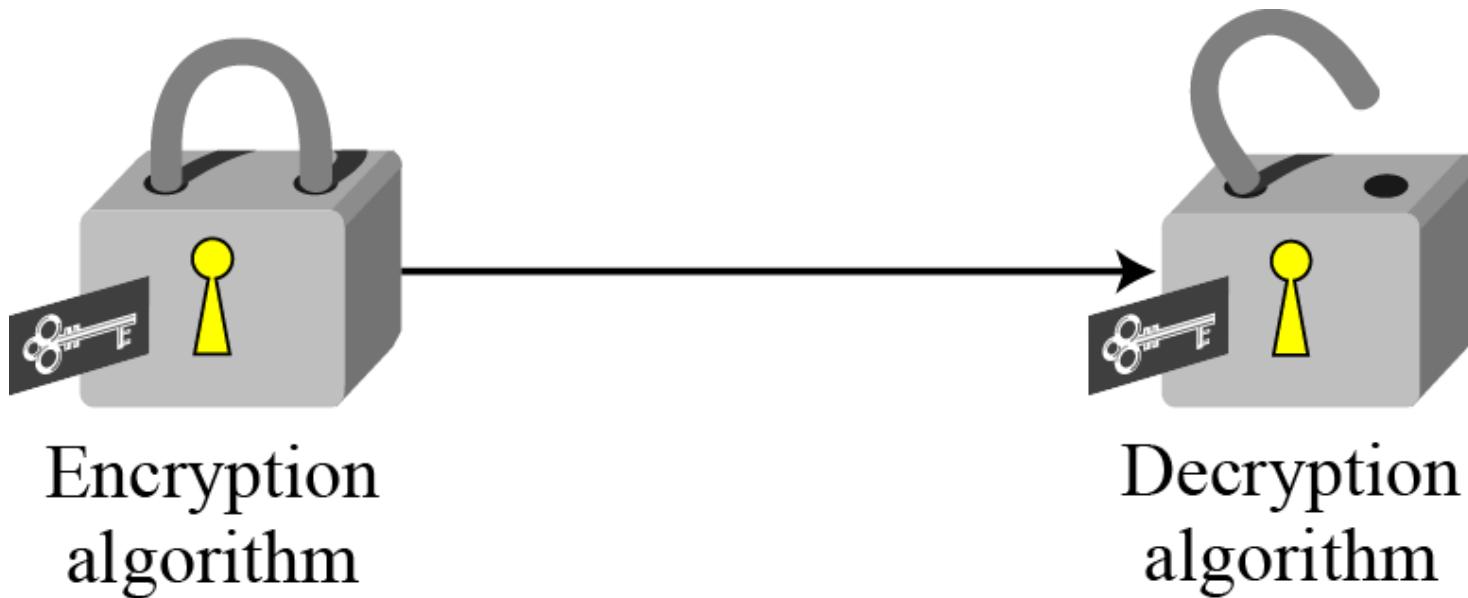
In which,  $D_k(E_k(x)) = E_k(D_k(x)) = x$

*We assume that Bob creates  $P_1$ ; we prove that  $P_1 = P$ :*

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

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

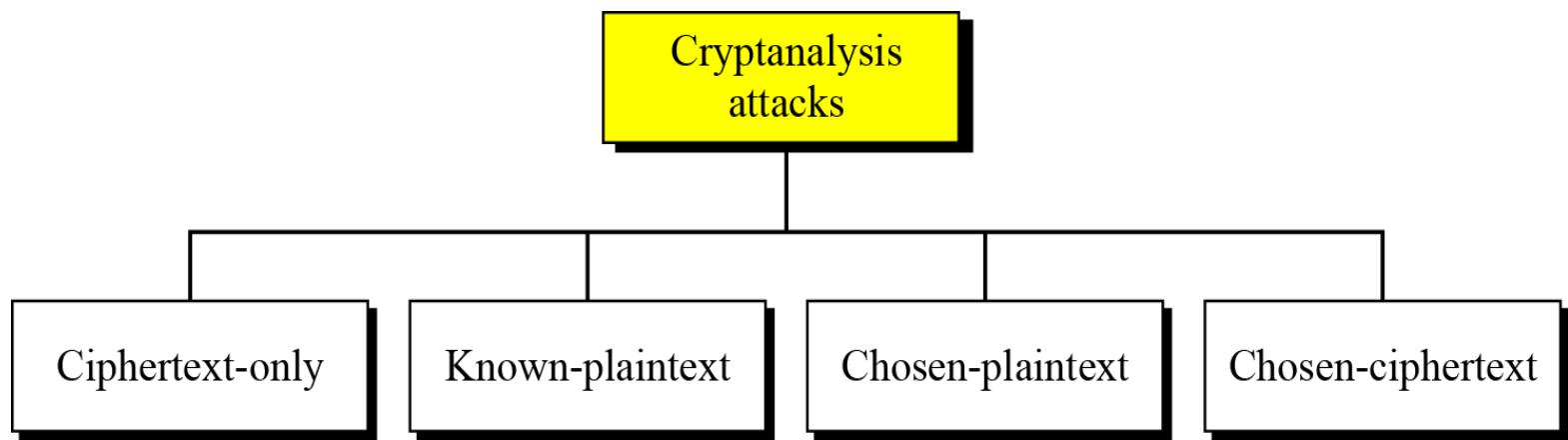
# Continued



**Figure 2** Locking and unlocking with the same key

# Cryptanalysis

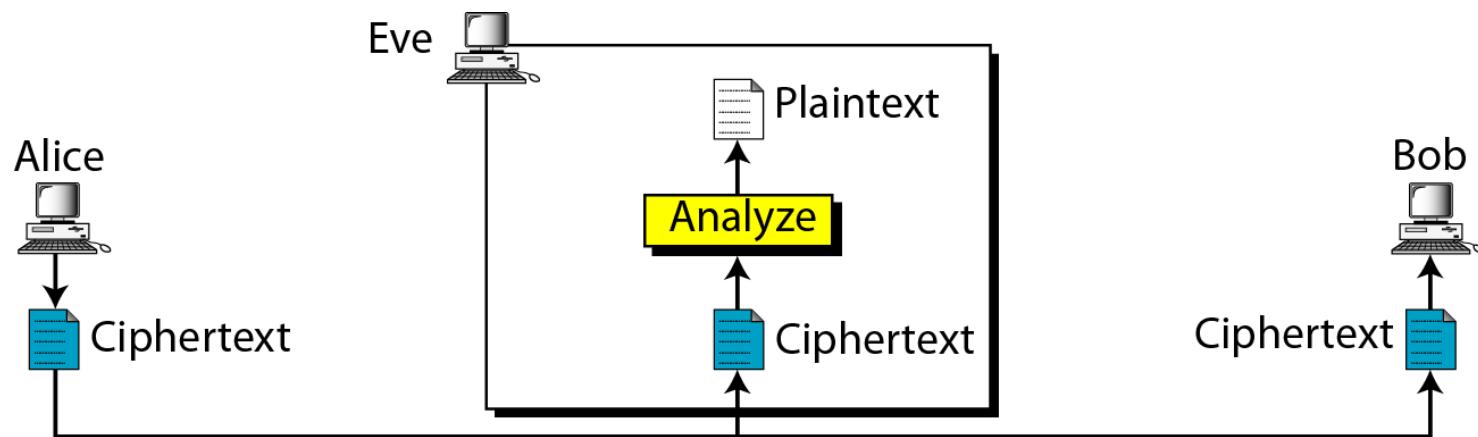
As cryptography is the science and art of creating secret codes, **cryptanalysis** is the science and art of breaking those codes.



**Figure 3** *Cryptanalysis attacks*

# Continued

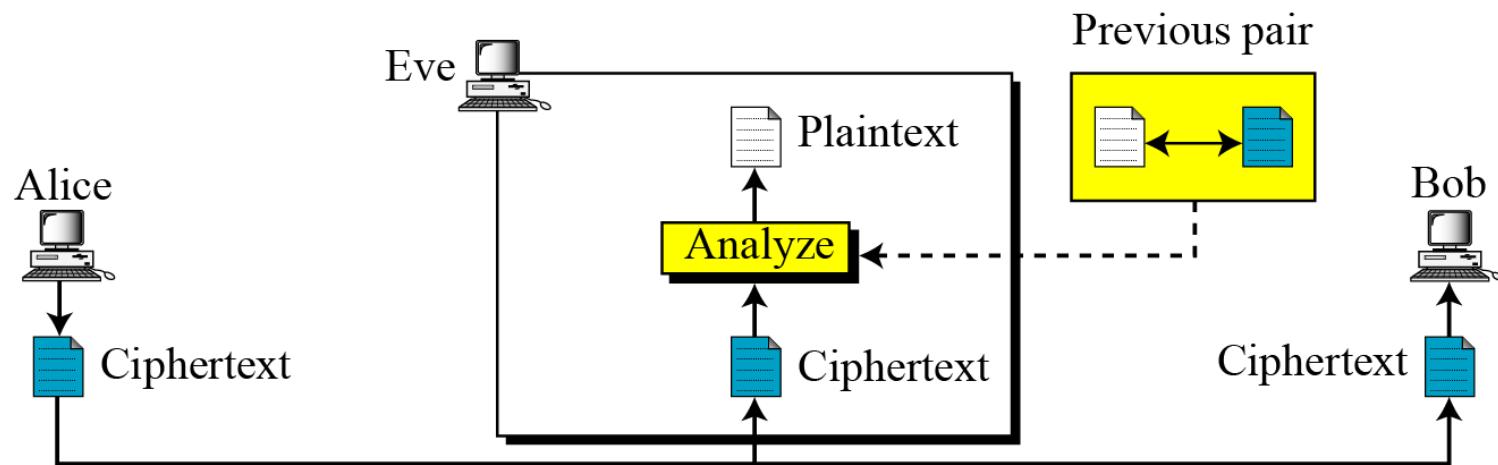
## Ciphertext-Only Attack



**Figure 4** *Ciphertext-only attack*

# Continued

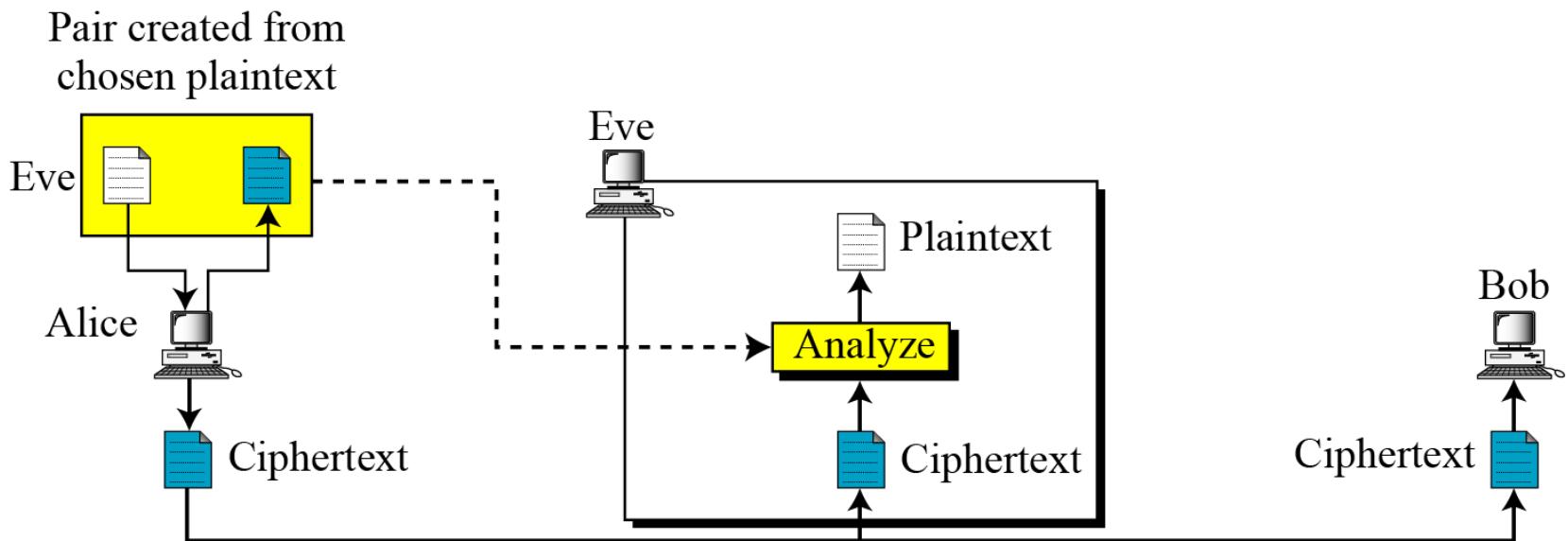
## Known-Plaintext Attack



**Figure 5** *Known-plaintext attack*

# Continued

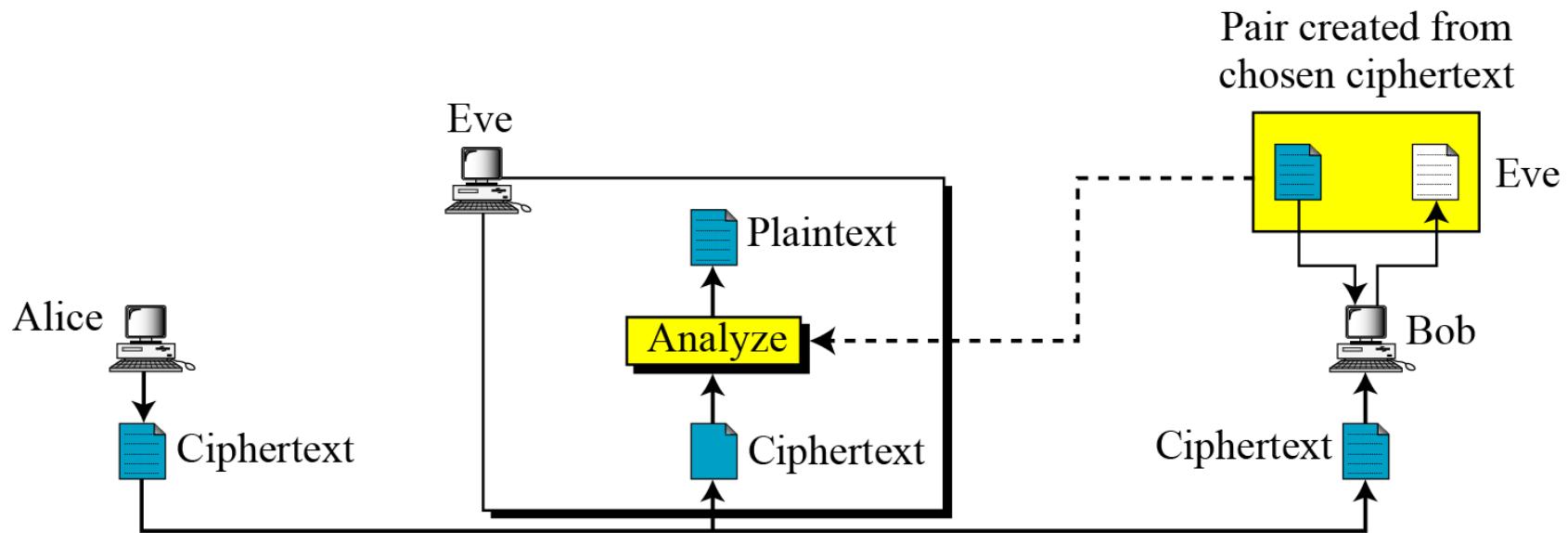
## Chosen-Plaintext Attack



**Figure 6** *Chosen-plaintext attack*

# Continued

## Chosen-Ciphertext Attack



**Figure 7** *Chosen-ciphertext attack*

# **Classical Encryption Techniques**

There are two basic building blocks of all encryption techniques: substitution and transposition.

## **1. Substitution Techniques**

- A substitution technique is one in which the letters of plaintext are replaced by other letters or by numbers or symbols.
- If the plaintext is viewed as a sequence of bits, then substitution involves replacing plaintext bit patterns with cipher text bit patterns.

## **2. Transposition Techniques**

A very different kind of mapping is achieved by performing some sort of permutation on the plaintext letters. This technique is referred to as a transposition cipher.

# 1. SUBSTITUTION CIPHERS

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

**Note**

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

## 1.1. Monoalphabetic Ciphers

**Note**

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

# Continued

## Example 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 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.

**Plaintext:** hello

**Ciphertext:** KHOGR

# Continued

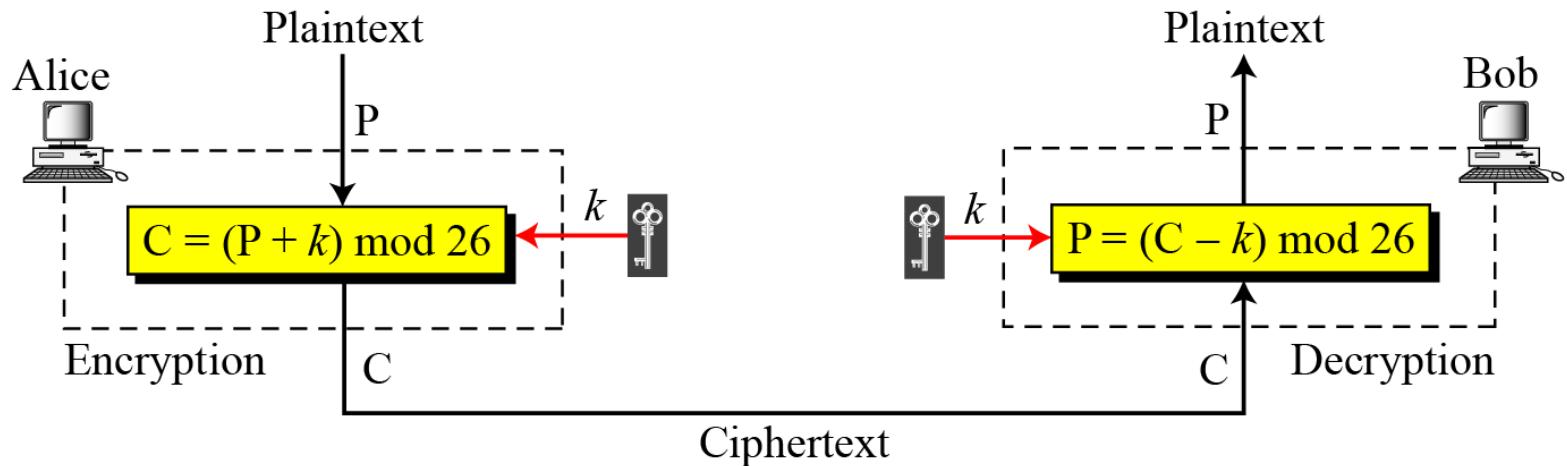
## Additive Cipher

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.

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

**Figure 8** Plaintext and ciphertext in  $Z_{26}$

# Continued



**Figure 9** *Additive cipher*

**Note**

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

# Continued

## Example 3

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

### Solution

We apply the encryption algorithm to the plaintext, character by character:

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

# Continued

## Example 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

# 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.

## 2.1 Continued

### Example 5

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

### Solution

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

Ciphertext: UVACLYFZLJBYL

<b>K = 1</b>	→	<b>Plaintext:</b> tuzbkxeykiaxk
<b>K = 2</b>	→	<b>Plaintext:</b> styajwdxjhzwj
<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> opuwfsztfdfs
<b>K = 7</b>	→	<b>Plaintext:</b> notverysecure

# Continued

**Table 1** *Frequency of characters in English*

<i>Letter</i>	<i>Frequency</i>	<i>Letter</i>	<i>Frequency</i>	<i>Letter</i>	<i>Frequency</i>	<i>Letter</i>	<i>Frequency</i>
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 2** *Frequency of 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

# Continued

## Example 6

Eve has intercepted the following ciphertext. Using a statistical attack, find the plaintext.

XLILSYWIMWRSAJSVWEPIJSVJSYVQMPPMSRHSPPEVWMXMWASVX-LQSVILY-  
VVCFIJSVIXLIWIPPIVIGIMZIWQSVISJIVW

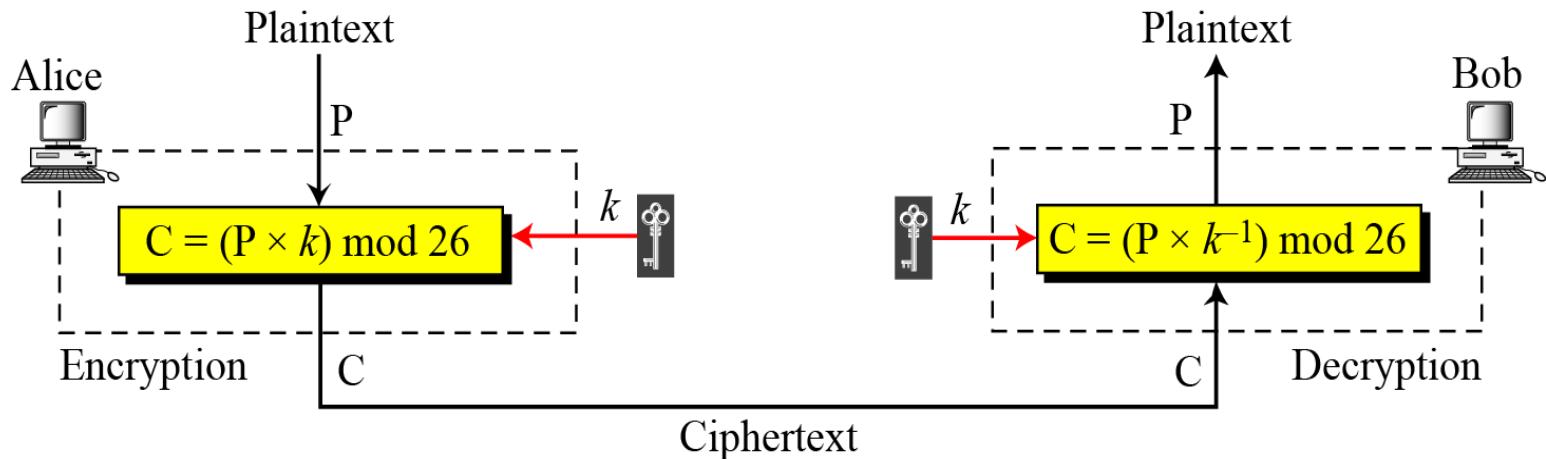
## Solution

When Eve tabulates the frequency of letters in this ciphertext, she gets: I =14, V =13, S =12, and so on. The most common character is I with 14 occurrences. This means key = 4.

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

# Continued

## Multiplicative Ciphers



**Figure 10** Multiplicative cipher

**Note**

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

# Continued

## Example 7

**What is the key domain for any multiplicative cipher?**

## Solution

The key needs to be in  $Z_{26}^*$ . This set has only 12 members: 1, 3, 5, 7, 9, 11, 15, 17, 19, 21, 23, 25.

## Example 8

We use a multiplicative cipher to encrypt the message “hello” with a key of 7. The ciphertext is “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

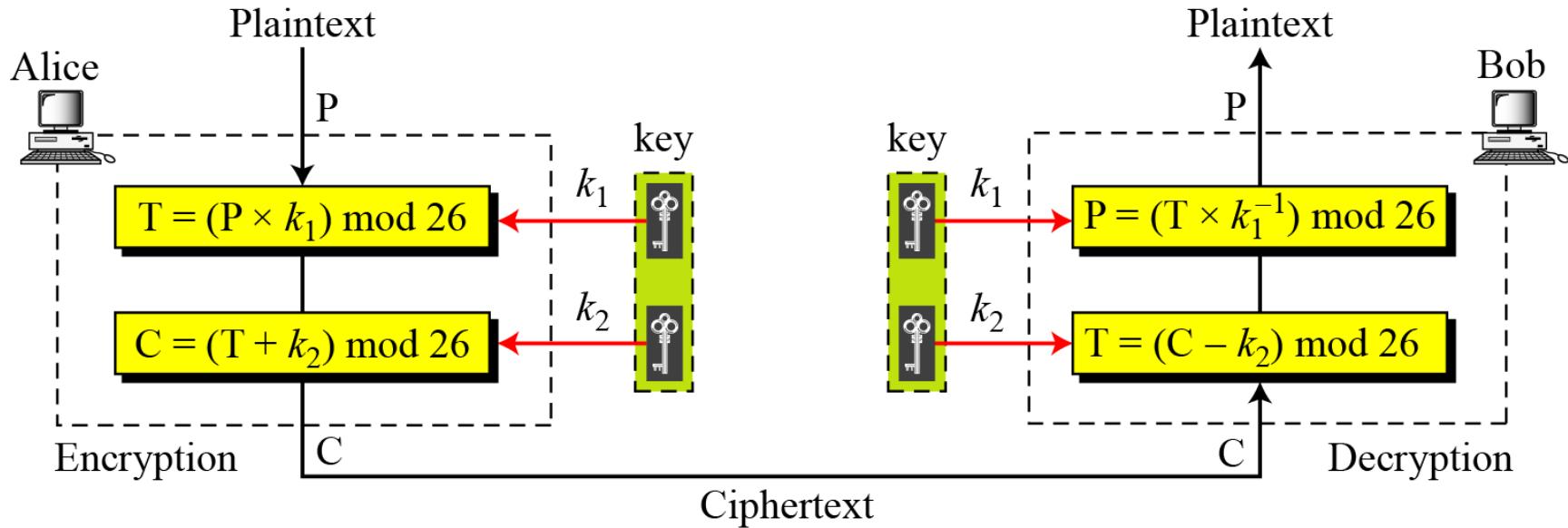
Plaintext: o → 14

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

ciphertext: 20 → U

# Continued

## Affine Ciphers



**Figure 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  $k_2$

## 2.1 Continued

### Example 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  $26 \times 12 = 312$ .

### Example 10

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

P: h → 07	Encryption: $(07 \times 7 + 2) \text{ mod } 26$	C: 25 → Z
P: e → 04	Encryption: $(04 \times 7 + 2) \text{ mod } 26$	C: 04 → E
P: l → 11	Encryption: $(11 \times 7 + 2) \text{ mod } 26$	C: 01 → B
P: l → 11	Encryption: $(11 \times 7 + 2) \text{ mod } 26$	C: 01 → B
P: o → 14	Encryption: $(14 \times 7 + 2) \text{ mod } 26$	C: 22 → W

## 2.1 Continued

### Example 11

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

### Solution

C: Z → 25	Decryption: $((25 - 2) \times 7^{-1}) \bmod 26$	P:07 → h
C: E → 04	Decryption: $((04 - 2) \times 7^{-1}) \bmod 26$	P:04 → e
C: B → 01	Decryption: $((01 - 2) \times 7^{-1}) \bmod 26$	P:11 → l
C: B → 01	Decryption: $((01 - 2) \times 7^{-1}) \bmod 26$	P:11 → l
C: W → 22	Decryption: $((22 - 2) \times 7^{-1}) \bmod 26$	P:14 → o

### Example 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  $k_2 = 0$ .

## 2.1 Continued

### Monoalphabetic Substitution Cipher

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

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.

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

**Figure 12** An example key for monoalphabetic substitution cipher

## 2.1 Continued

### Example 13

We can use the key in Figure 12 to encrypt the message

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

The ciphertext is

ICFVQRVVNEFVRNVSIYRGAHSLIOJICNHTIYBFGTICRXRS

## 2.2 Polyalphabetic Ciphers

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.

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

## 2.2 Continued

### Example 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.

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

## 2.2 Continued

### Playfair Cipher

- A 5X5 matrix of letters based on a keyword
- Fill in letters of keyword (sans duplicates)
- Fill rest of matrix with other letters
- Eg. using the keyword MONARCHY

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

## 2.2 Continued

### Encrypting and Decrypting in Playfair Cipher

- Plain text is encrypted two letters at a time
  1. If a pair is a repeated letter, insert filler like 'X'
  2. If both letters fall in the same row, replace each with letter to right (wrapping back to start from end)
  3. If both letters fall in the same column, replace each with the letter below it (again wrapping to top from bottom)
  4. Otherwise each letter is replaced by the letter in the same row and in the column of the other letter of the pair

## 2.2 Continued

### Example 15-1 Playfair Cipher

- Message = Move forward
- Plaintext = mo ve fo rw ar dx
- Here x is just a filler, message is padded and segmented
- Ciphertext = ON UF PH NZ RM BZ

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

### 3.2.2 Continued

#### Playfair Cipher

**Example 15-2** *An example of a secret key in the Playfair cipher is:*

***PLAYFAIR***

Let us encrypt the plaintext “balloon” using the key given in Fig. 15-2.

## 2.2 Continued

### Security of Playfair Cipher

- security much improved over monoalphabetic
- since have  $26 \times 26 = 676$  digrams
- would need a 676 entry frequency table to analyse (verses 26 for a monoalphabetic)
- and correspondingly more ciphertext
- was widely used for many years
  - eg. by US & British military in WW1
- it can be broken, given a few hundred letters
- since still has much of plaintext structure

## 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 16

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

## 3.2.2 Continued

### Example 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).

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 17

Vigenere cipher can be seen as combinations of  $m$  additive ciphers.

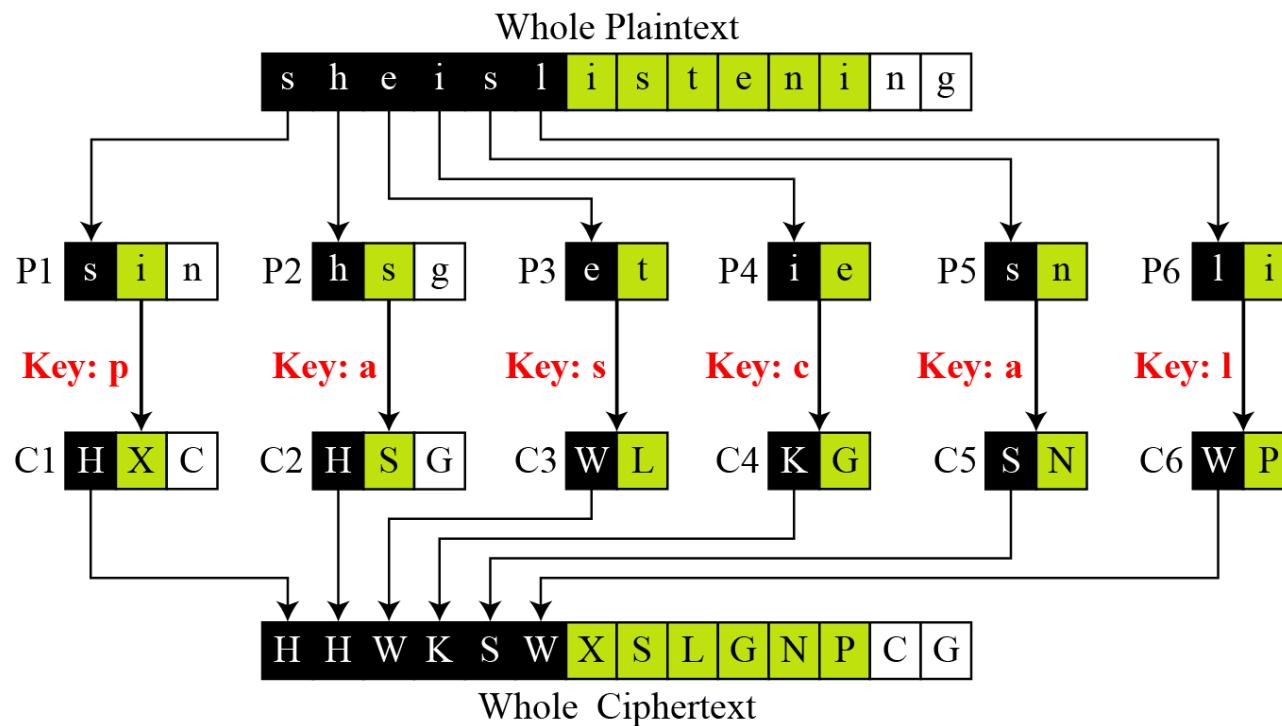


Figure 14 A Vigenere cipher as a combination of  $m$  additive ciphers

## 3.2.2 Continued

### Example 18

Using Example 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**  
*A Vigenere Tableau*

## 3.2.2 Continued

### Vigenere Cipher (Crypanalysis)

#### Example 19

Let us assume we have intercepted the following ciphertext:

LIOMWGFEGGDVWGHHCQUCRHRWAGWIOWQLKGZETKKMEVLWPCZVGTH-  
VTSGXQOVGCSVETQLTJSUMVWVEUVLXEWSLGFMVVWLGYHCUSWXQH-  
KVGSHHEEVFLCFDGVSUMPHKIRZDMPHHBVWWJWIXGFWLTSHGJOUEEHH-  
VUCFVGOWICQLTJSUXGLW

The Kasiski test for repetition of three-character segments yields the results shown in Table 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 19

Let us assume we have intercepted the following ciphertext:

LIOMWGFEGGDVWGHHCQUCRHRWAGWIOWQLKGZETKKMEVLWPCZVGTH-  
VTSGXQOVGCSVETQLTJSUMVWVEUVLXEWSLGFZMVVWLGYHCUSWXQH-  
KVGSHEEVFLCFDGVSUMPHKIRZDMPHBWWVWJWIXGFWLTSHGJOUEEHH-  
VUCFVGOWICQLTJSUXGLW

The Kasiski test for repetition of three-character segments yields the results shown in Table 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 19 (Continued)

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

C1 : LWGWCRAOKTEPGTQCTJVUEGVGUQGECPVPRPVJGTJEUGCJG

P1 : jueuapymircneroarhtsthihytrahcieixsthcarrehe

C2 : IGGGQHGWGKVCTSOSQS WVWFVYSHSVFSHZHWWFSOHCOQSL

P2 : usssctsiswhofeaeciehcetesesoecatn p ntherhctecex

C3 : OFDHURWQZKLZHGVVLUVLSZWHWKHFDUKDHVIWHUHFWLW

P3 : lcaerotnwhiwedssirs iirhkete hretl t i ideat rairt

C4 : MEVHCWILEMWVVXGETMEXMLCXVELGMIMBWXLGEVVITX

P4 : i ardysehaisrrt capiafpwtethecarhaesfterectpt

In this case, the plaintext makes sense.

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

- This cipher is based on linear algebra.
- Each letter is represented by numbers from 0 to 25 and calculations are done modulo 26.
- This encryption algorithm takes  $m$  successive plaintext letters and substitutes them with  $m$  cipher text
- The substitution determined by  $m$  linear equations. For  $m = 3$ , the system can describe as:

$$c_1 = (k_{11}p_1 + k_{21}p_2 + k_{31}p_3) \bmod 26$$

$$c_2 = (k_{12}p_1 + k_{22}p_2 + k_{32}p_3) \bmod 26$$

$$c_3 = (k_{13}p_1 + k_{23}p_2 + k_{33}p_3) \bmod 26$$

- This can also expressed in terms of row vectors and matrices.

$$(c_1 \ c_2 \ c_3) = (p_1 \ p_2 \ p_3) \begin{pmatrix} k_{11} & k_{12} & k_{13} \\ k_{21} & k_{22} & k_{23} \\ k_{31} & k_{32} & k_{33} \end{pmatrix} \bmod 26$$

$$\mathbf{C} = \mathbf{PK} \bmod 26$$

- Where  $\mathbf{C}$  and  $\mathbf{P}$  are row vectors of length 3 representing the plaintext and cipher text, and  $\mathbf{K}$  is a  $3 \times 3$  matrix representing the encryption key

### 3.2.2 Continued

- Key is an invertible matrix  $K$  modulo 26, of size  $m$ . For example:

$$K = \begin{pmatrix} 17 & 17 & 5 \\ 21 & 18 & 21 \\ 2 & 2 & 19 \end{pmatrix} \quad K^{-1} = \begin{pmatrix} 4 & 9 & 15 \\ 15 & 17 & 6 \\ 24 & 0 & 17 \end{pmatrix}$$

This is demonstrated as

$$\begin{pmatrix} 17 & 17 & 5 \\ 21 & 18 & 21 \\ 2 & 2 & 19 \end{pmatrix} \begin{pmatrix} 4 & 9 & 15 \\ 15 & 17 & 6 \\ 24 & 0 & 17 \end{pmatrix} = \begin{pmatrix} 443 & 442 & 442 \\ 858 & 495 & 780 \\ 494 & 52 & 365 \end{pmatrix} \text{mod } 26 = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}$$

- Encryption and decryption can give by the following formulae: Hill Cipher

$$\text{Encryption: } C = E(K, P) = PK \text{ mod } 26$$

$$\text{Decryption: } P = D(K, C) = CK^{-1} \text{ mod } 26 = PKK^{-1} = P$$

- The strength of the Hill cipher is that it completely hides single-letter frequencies.

### 3.2.2 Continued

#### Example 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”.

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

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 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 17.

$$\begin{bmatrix} 05 & 07 & 10 \end{bmatrix} \longleftrightarrow \begin{bmatrix} 03 & 06 & 00 \end{bmatrix}$$
$$\begin{bmatrix} 13 & 17 & 07 \end{bmatrix} \longleftrightarrow \begin{bmatrix} 14 & 16 & 09 \end{bmatrix}$$
$$\begin{bmatrix} 00 & 05 & 04 \end{bmatrix} \longleftrightarrow \begin{bmatrix} 03 & 17 & 11 \end{bmatrix}$$

**P**   **C**

Figure 17

### 3.2.2 Continued

#### Example 21

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 18.

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

$\mathbf{K}$                        $\mathbf{P}^{-1}$                        $\mathbf{C}$

Figure 18

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

## 3.2.2 Continued

### One-Time Pad

**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**.

## 3.2.2 Continued

An example should illustrate our point.

**Suppose that we are using a Vigenère scheme with 27 characters in which the twenty-seventh character is the space character, but with a one-time key that is as long as the message.**

Consider the ciphertext

ANKYODKYUREPFJBYOJDSPLREYIUNOFDOIUFPLUYTS

We now show two different decryptions using two different keys:

ciphertext: ANKYODKYUREPFJBYOJDSPLREYIUNOFDOIUFPLUYTS

key: *pxlmvmsydoфuyrvzwc tnlebnecvgdupahfzzlmnyih*

plaintext: mr mustard with the candlestick in the hall

ciphertext: ANKYODKYUREPFJBYOJDSPLREYIUNOFDOIUFPLUYTS

key: *pftgpmiydgaxgoufhklllhmhsqdqogtewbqfqgyovuhwt*

plaintext: miss scarlet with the knife in the library

### 3.2.2 Continued

The one-time pad offers complete security but, in practice, has two fundamental difficulties:

1. There is the practical problem of making large quantities of random keys. Any heavily used system might require millions of random characters on a regular basis. Supplying truly random characters in this volume is a significant task.
2. Even more daunting is the problem of key distribution and protection. For every message to be sent, a key of equal length is needed by both sender and receiver. Thus, a mammoth key distribution problem exists.

### 3.2.2 Continued

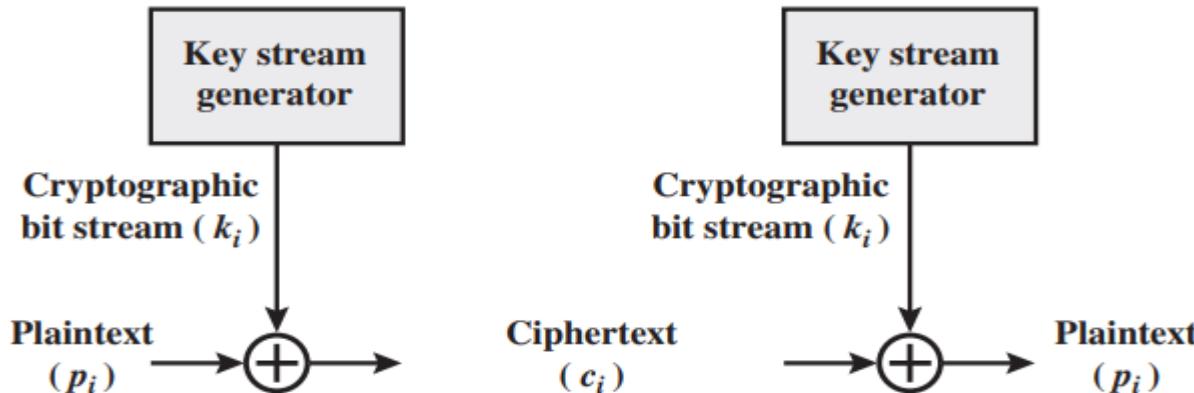
## Vernam Cipher

It works on binary data (bits) rather than letters. The system can be expressed succinctly as follows:

$$c_i = p_i \oplus k_i$$

where  $p_i$  = ith binary digit of plaintext,  $k_i$  = ith binary digit of key,  $c_i$  = ith binary digit of ciphertext ,  $\oplus$  = exclusive-or (XOR) operation

Thus, the ciphertext is generated by performing the bitwise XOR of the plaintext and the key.

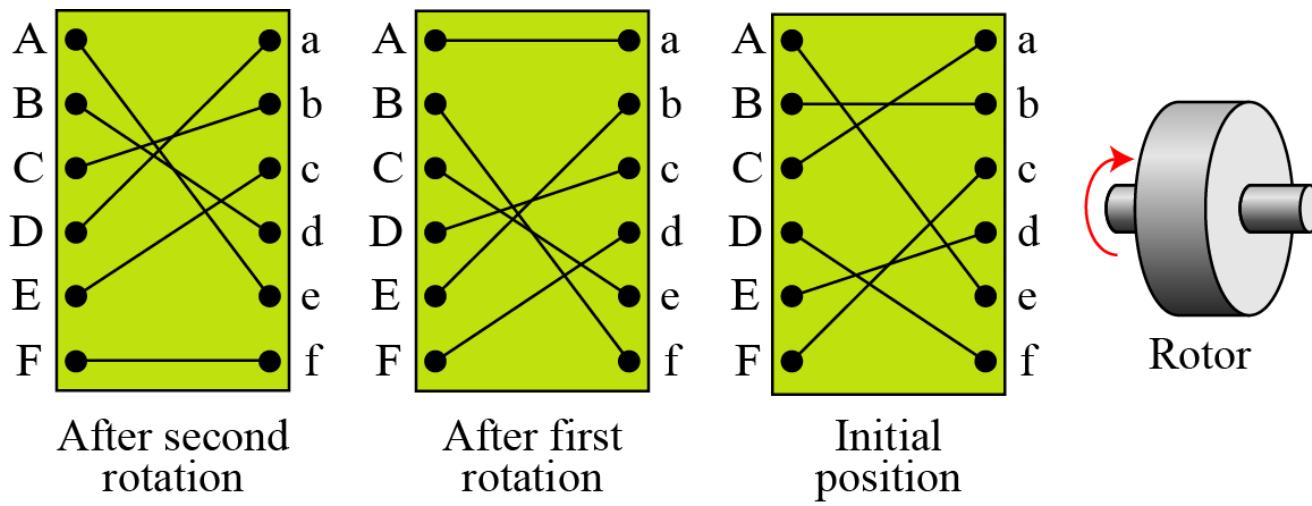


Because of the properties of the XOR, decryption simply involves the same bitwise operation:

$$p_i = c_i \oplus k_i$$

## 3.2.2 Continued

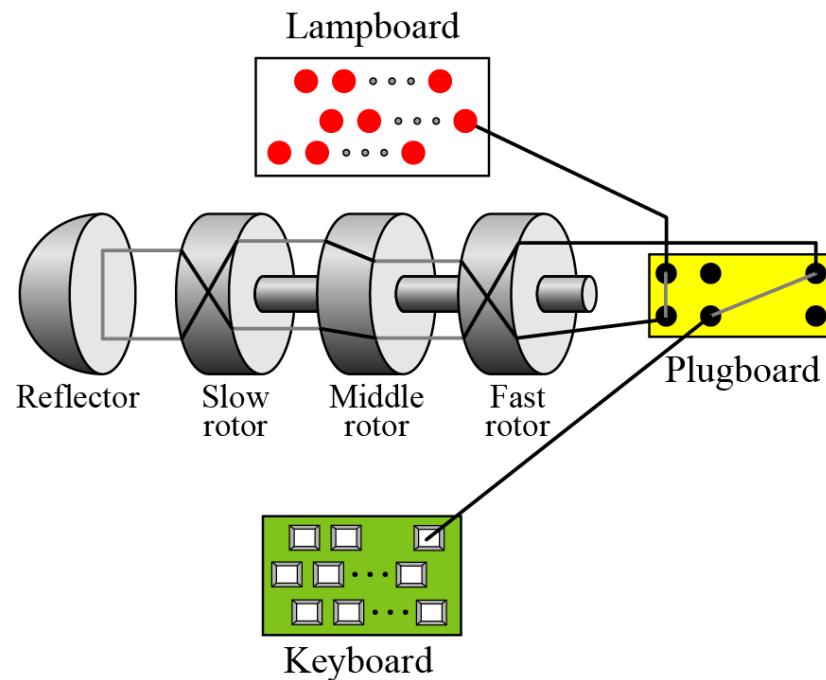
### Rotor Cipher



**Figure 19** *A rotor cipher*

## 3.2.2 Continued

### Enigma Machine



**Figure 20** *A schematic of the Enigma machine*

## 3-3 TRANSPOSITION CIPHERS

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

**Note**

**A transposition cipher reorders symbols.**

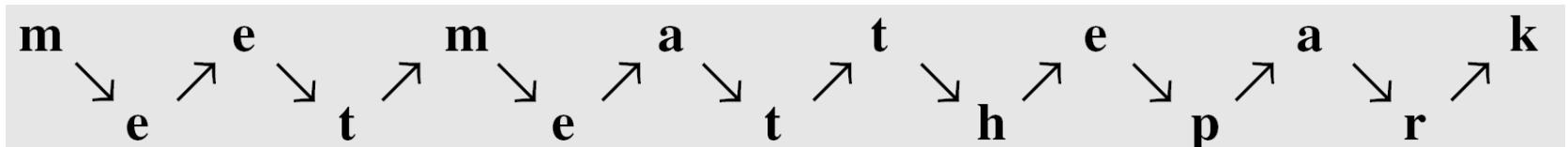
- ✓ Keyless Transposition Ciphers
- ✓ Keyed Transposition Ciphers
- ✓ Combining Two Approaches

### 3.3.1 Keyless Transposition Ciphers

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

#### Example 22

A good example of a keyless cipher using the first method is the **rail fence cipher**. The ciphertext is created reading the pattern row by row. For example, to send the message “Meet me at the park” to Bob, Alice writes



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

### 3.3.1 Continued

#### Example 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 “MMTAEEHREAEKTTP”.

### 3.3.1 Continued

#### Example 24

The cipher in Example 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**

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.

### 3.3.2 Continued

#### Example 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 character are permuted.

Encryption ↓

3	1	4	5	2
1	2	3	4	5

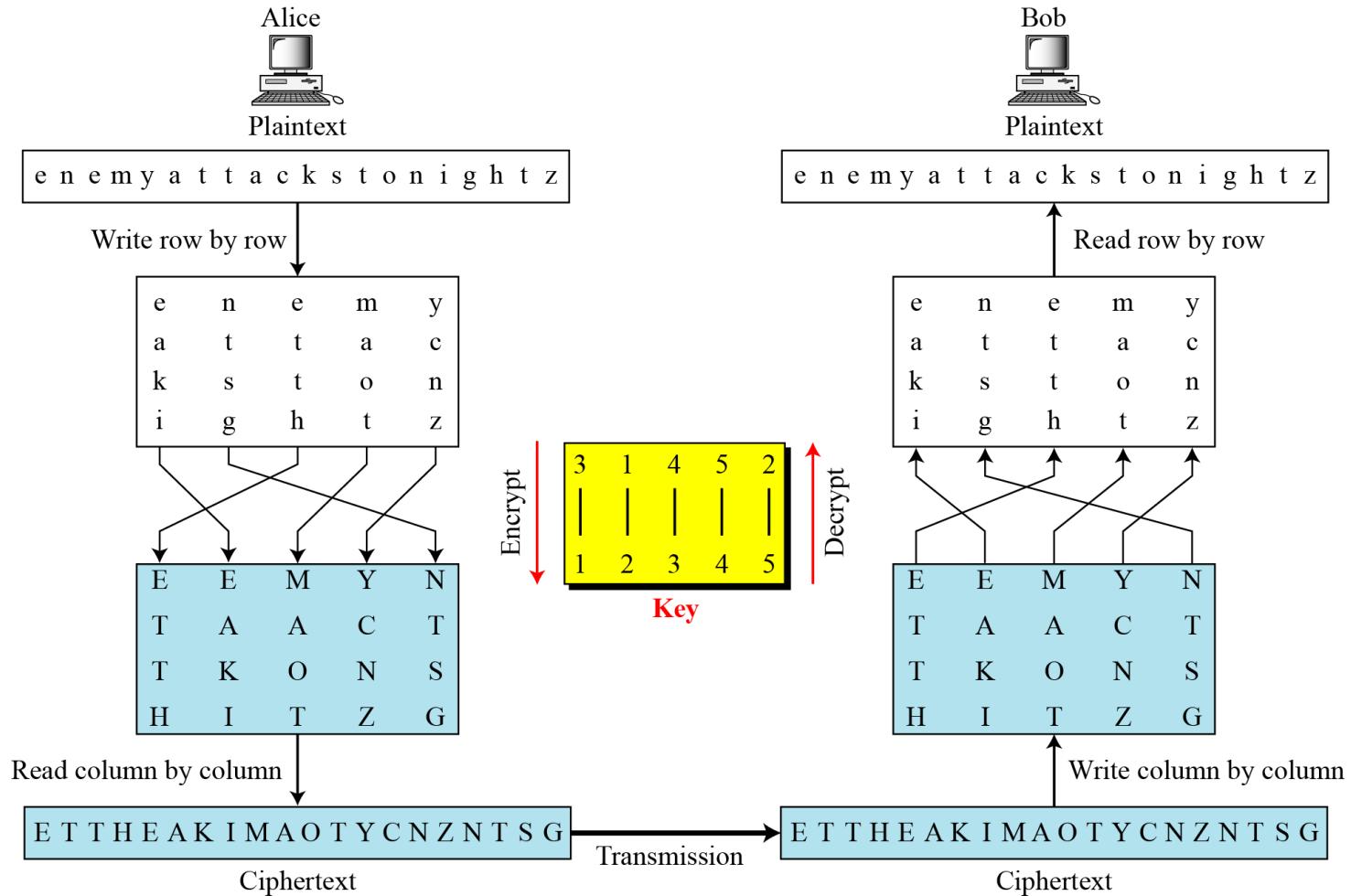
↑ Decryption

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

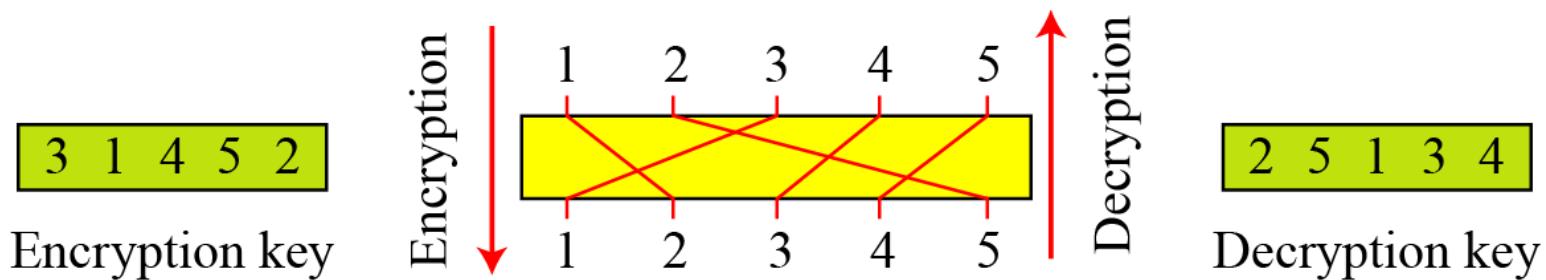
#### Example 26



### 3.3.3 Continued

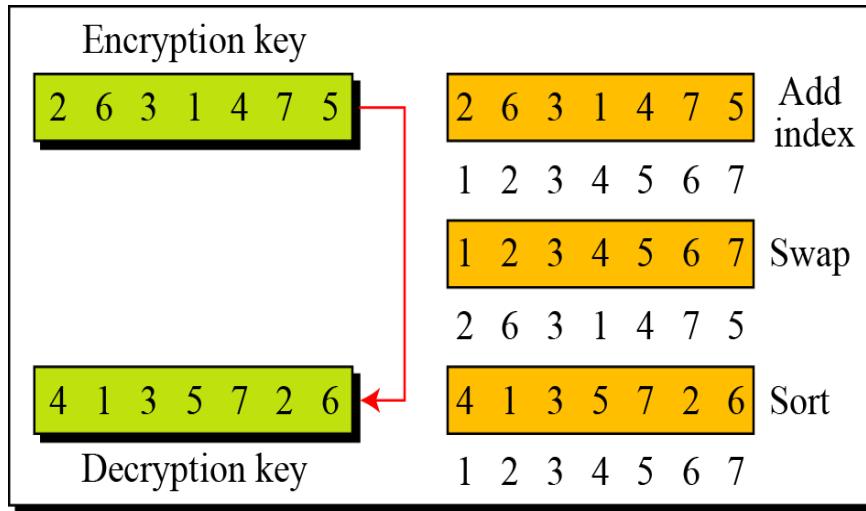
#### Keys

In Example 27, 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.



**Figure 22** *Encryption/decryption keys in transpositional ciphers*

### 3.3.3 Continued



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

**Figure 23** Key inversion in a transposition cipher

### 3.3.3 Continued

#### Using Matrices

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

#### Example 27

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

**Figure 24** Representation of the key as a matrix in the transposition cipher

### 3.3.3 Continued

#### Example 27

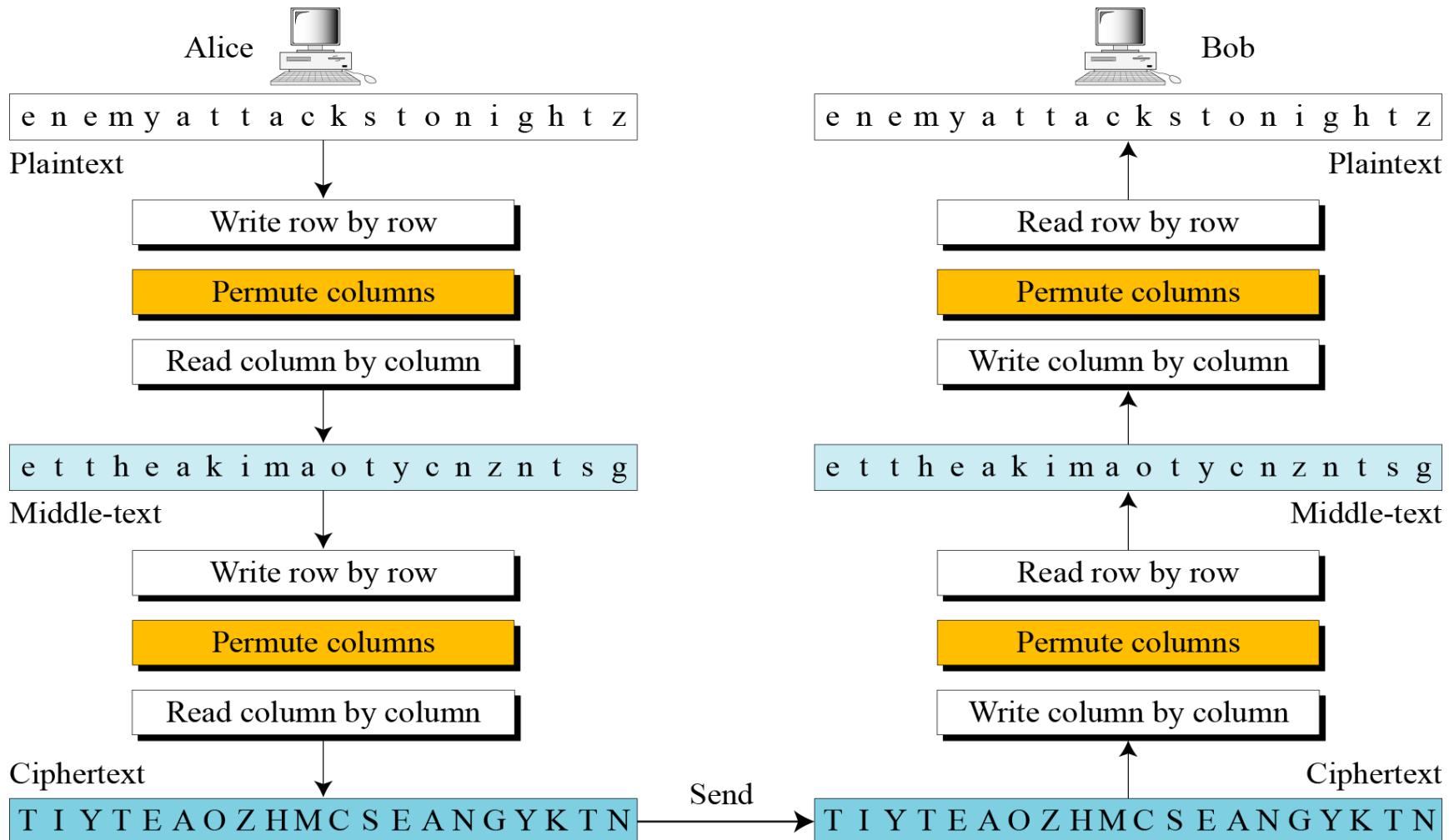
Figure 24 shows the encryption process. Multiplying the  $4 \times 5$  plaintext matrix by the  $5 \times 5$  encryption key gives the  $4 \times 5$  ciphertext matrix.

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

Figure 24 *Representation of the key as a matrix in the transposition cipher*

### 3.3.3 Continued

## Double Transposition Ciphers



**Figure 25** Double transposition cipher

## **3-4 STREAM AND BLOCK CIPHERS**

*The literature divides the symmetric ciphers into two broad categories: stream ciphers and block ciphers. Although the definitions are normally applied to modern ciphers, this categorization also applies to traditional ciphers.*

- ✓ Stream Ciphers
- ✓ Block Ciphers
- ✓ Combination

### 3.4.1 Stream Ciphers

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

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

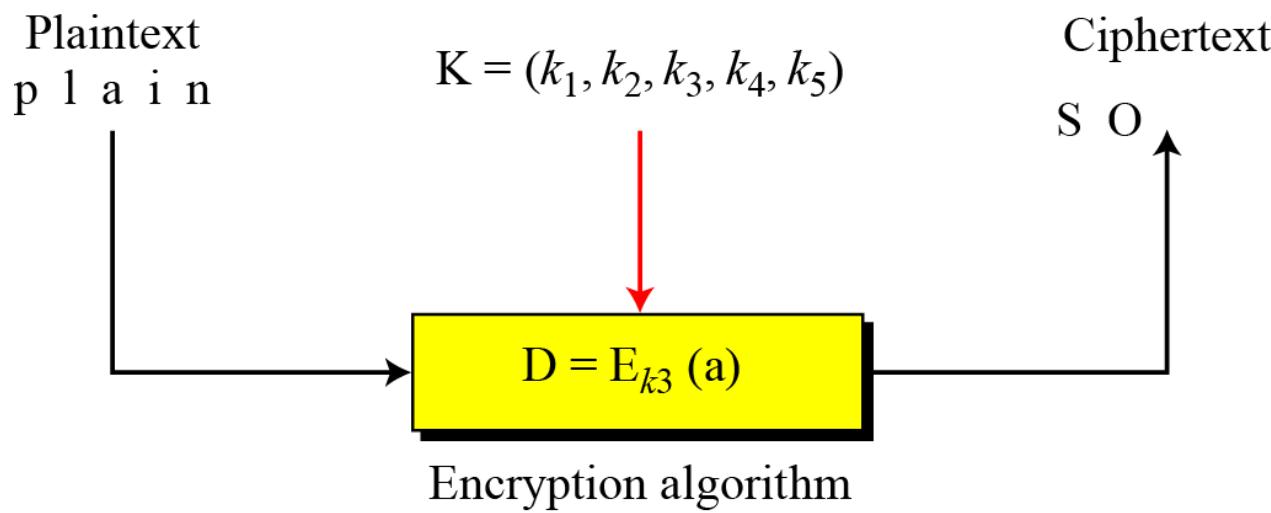
$$C = C_1 C_2 C_3, \dots$$

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

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

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

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



**Figure 26** Stream cipher

### 3.4.1 Continued

#### Example 30

Additive ciphers can be categorized as stream ciphers in which the key stream is the repeated value of the key. In other words, the key stream is considered as a predetermined stream of keys or  $K = (k, k, \dots, k)$ . In this cipher, however, each character in the ciphertext depends only on the corresponding character in the plaintext, because the key stream is generated independently.

#### Example 31

The monoalphabetic substitution ciphers discussed in this chapter are also stream ciphers. However, each value of the key stream in this case is the mapping of the current plaintext character to the corresponding ciphertext character in the mapping table.

### 3.4.1 Continued

#### Example 32

Vigenere ciphers are also stream ciphers according to the definition. In this case, the key stream is a repetition of  $m$  values, where  $m$  is the size of the keyword. In other words,

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

#### Example 33

We can establish a criterion to divide stream ciphers based on their key streams. We can say that a stream cipher is a monoalphabetic cipher if the value of  $k_i$  does not depend on the position of the plaintext character in the plaintext stream; otherwise, the cipher is polyalphabetic.

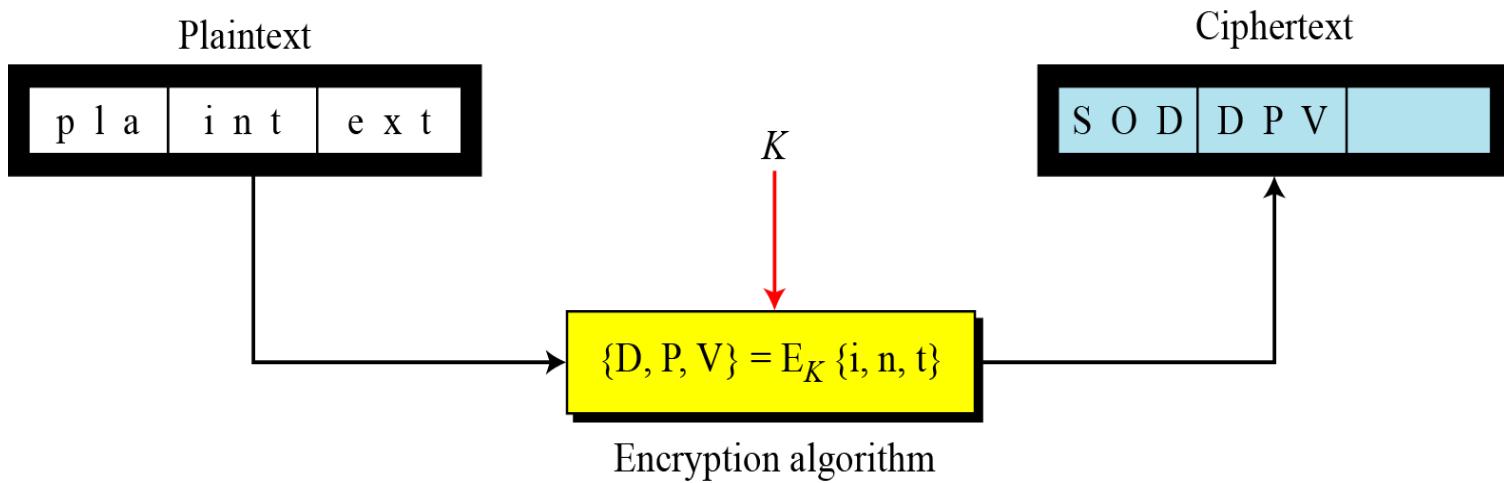
### 3.4.1 Continued

#### Example 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 Stream Ciphers

In a block cipher, a group of plaintext symbols of size  $m$  ( $m > 1$ ) are encrypted together creating a group of ciphertext of the same size. A single key is used to encrypt the whole block even if the key is made of multiple values. Figure 27 shows the concept of a block cipher.



**Figure 27** *Block cipher*

### 3.4.2 Continued

#### Example 34

Playfair ciphers are block ciphers. The size of the block is  $m = 2$ . Two characters are encrypted together.

#### Example 35

Hill ciphers are block ciphers. A block of plaintext, of size 2 or more is encrypted together using a single key (a matrix). In these ciphers, the value of each character in the ciphertext depends on all the values of the characters in the plaintext. Although the key is made of  $m \times m$  values, it is considered as a single key.

#### Example 36

From the definition of the block cipher, it is clear that every block cipher is a polyalphabetic cipher because each character in a ciphertext block depends on all characters in the plaintext block.

### 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.