The Islamic University
College of Technical Engineering
Department of Computer Technical Engineering

Fourth Stage

Security

Lecture 1

Asst. Lec. Yousif Samer Mudhafar

Email: yousif.samir19@gmail.com

Lecture objectives

The student will recognize the following objectives:

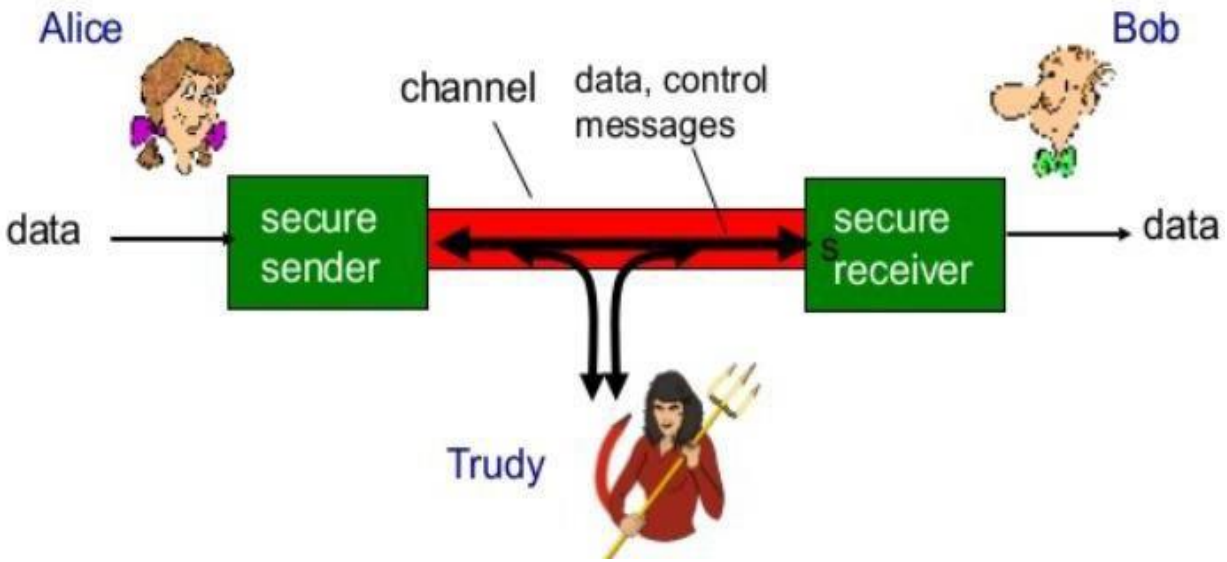
1. **Types of network security methods**
   - Symmetric key encryption
   - A Symmetric key encryption
2. **Types of encryption and decryption algorithms**
3. **Encryption and Decryption using Caesar Cipher**

Content

- Network Security
- Types of Network Security Methods
- Simplified Model of Encryption and Decryption
- Classification of Encryption Algorithms
- Caesar Cipher (Encryption and Decryption)

Network Security

Network security consists of the policies, processes and practices adopted to prevent, detect and monitor unauthorized access, misuse, modification, or denial of a computer network and network-accessible resources.



There are two types of network security :

1. **Symmetric key encryption :-** it's a system when the sender encrypt the message with a specific key and the receiver use the same key to decrypt the encrypted message.
2. **Asymmetric key encryption :-** it's a system when the sender encrypt the message with a specific key and the receiver use different key to decrypt the encrypted message.

There are five special ingredients in each encryption and decryption methods which are:

1.Plaintext (P):- This is the original intelligible message or data that is fed into the algorithm as input.

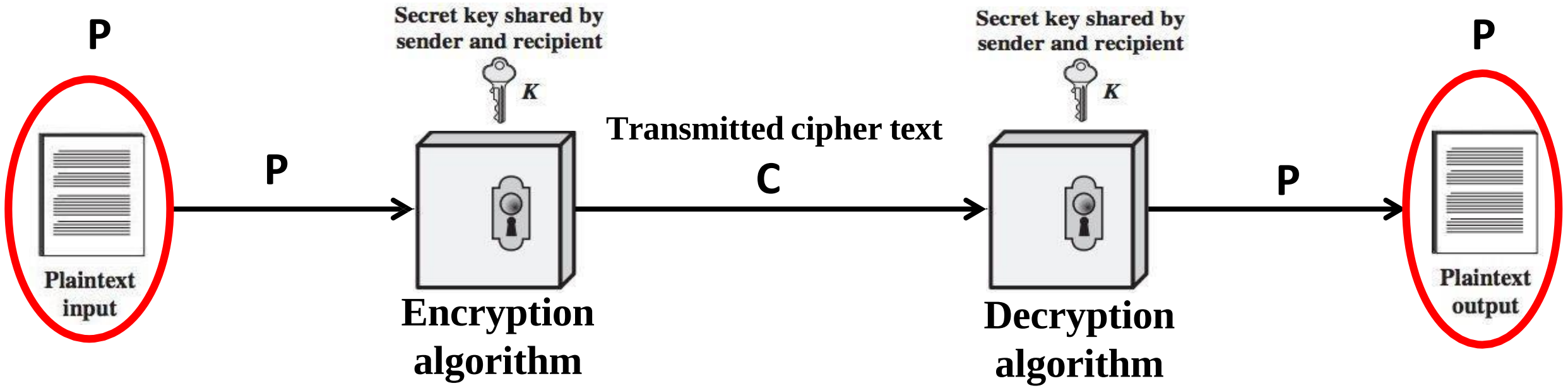
2.Encryption algorithm (E):- The encryption algorithm performs various substitutions and transformations on the plaintext.

3.Secret key (K) :- The secret key is also input to the encryption algorithm. The key is a value independent of the plaintext and of the algorithm.

4.Cipher text (C) :- This is the scrambled message produced as output. It depends on the plaintext and the secret key.

5.Decryption algorithm (D) :- This is essentially the encryption algorithm run in reverse. It takes the cipher text and the secret key and produces the original plaintext.

Simplified Model of Encryption and Decryption



Classification of Encryption Algorithm

Classical Techniques

1. Caesar Cipher
2. Affine Cipher
3. Play fair Cipher
4. Vigenere Cipher
5. Autokey Cipher

Modern Techniques

1. Data Encryption Standard (DES)
2. Advanced Encryption Standard (AES)
3. Secure Hash Algorithm
4. Rivest Shamir Adleman (RSA)

Alphabet (character)

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

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

Caesar Cipher (Shift Cipher or Additive Cipher)

The earliest known, and the simplest, use of a substitution cipher was by Julius Caesar. The Caesar cipher involves replacing each letter of the alphabet with the letter standing three places further down the alphabet.

1. The Encryption algorithm can be written as

$$C_i = (P_i + K)\ mod\ 26$$

2. The Decryption algorithm can be written as

$$P_i = (C_i - K)\ mod\ 26$$

Note:

- **Encryption**

P → Plaintext → small letter

C → Cipher text → capital letter

K → Key

- **Decryption**

C → Cipher text → capital letter

P → Plaintext → small letter

Mod

Note:

3 **mod** 26 = 3

15 **mod** 26 = 15

40 **mod** 26 = 14

80 **mod** 26 = 2

-3 **mod** 26 =-3+26=23

-40 **mod** 26 =-14+26=12

$$\frac{80}{26} = 3.076923$$

3 * 26 = 78

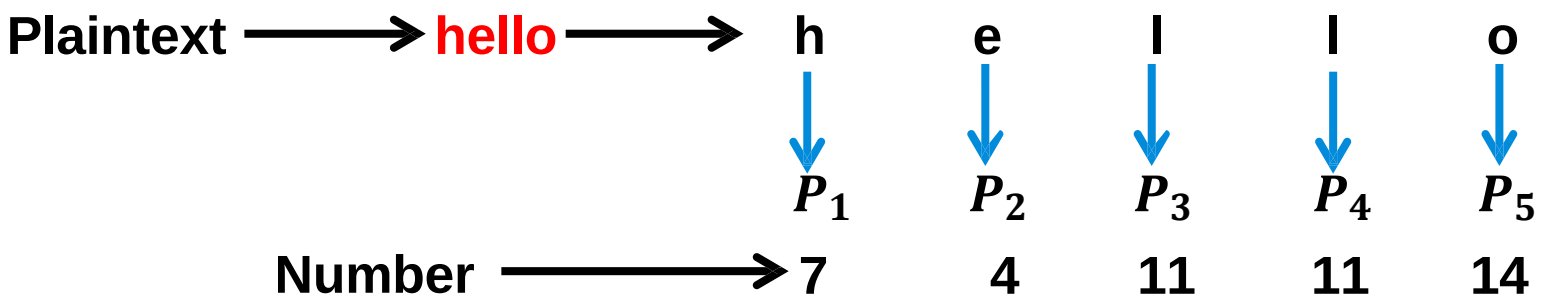
80 – 26 = 2

Example 1

Encrypt and decrypt for the Plaintext "**hello**" by using **Caesar Cipher**.

Ans: Encryption

$$C_i = (P_i + K)\ mod\ 26$$



$C_1 = (P_1 + K)\ mod\ 26$

$C_1 = (7 + 3)\ mod\ 26$

$C_1 = (10)\ mod\ 26$

$C_1 = (10) = K$

$C_2 = (P_2 + K)\ mod\ 26$

$C_2 = (4 + 3)\ mod\ 26$

$C_2 = (7)\ mod\ 26$

$C_2 = (7) = H$

$C_3 = (P_3 + K)\ mod\ 26$

$C_3 = (11 + 3)\ mod\ 26$

$C_3 = (14)\ mod\ 26$

$C_3 = (14) = O$

$C_4 = (P_4 + K)\ mod\ 26$

$C_4 = (11 + 3)\ mod\ 26$

$C_4 = (14)\ mod\ 26$

$C_4 = (14) = O$

$$C_5 = (P_5 + K)\ mod\ 26$$

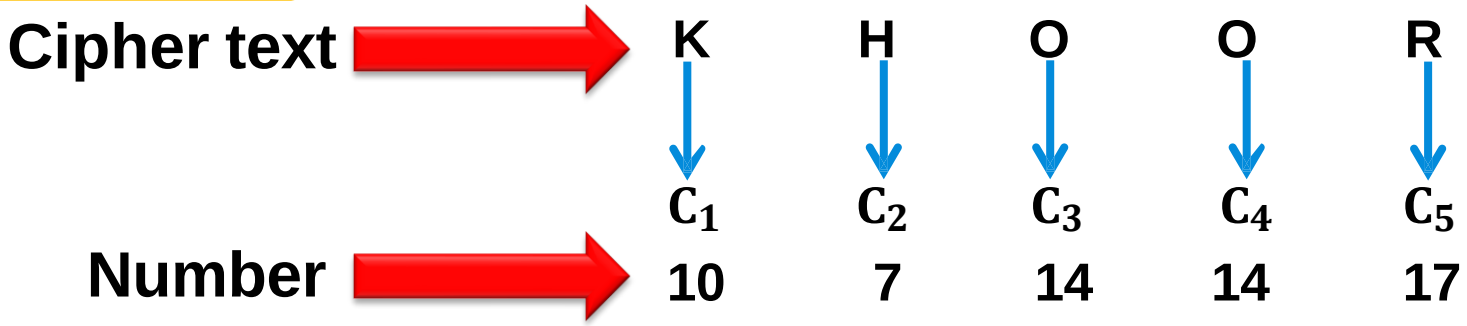
$$C_5 = (14 + 3)\ mod\ 26$$

$$C_5 = (17)\ mod\ 26$$

$$C_5 = (17) = R$$

Cipher text : $C_1C_2C_3C_4C_5$ → **KHOOR**

2. Decryption Algorithm



$$P_i = (C_i - K)\ mod\ 26$$

$P_1 = (C_1 - K)\ mod\ 26$

$P_1 = (10 - 3)\ mod\ 26$

$P_1 = (7)\ mod\ 26$

$P_1 = (7) = h$

$P_2 = (C_2 - K)\ mod\ 26$

$P_2 = (7 - 3)\ mod\ 26$

$P_2 = (4)\ mod\ 26$

$P_2 = (4) = e$

$P_3 = (C_3 - K)\ mod\ 26$

$P_3 = (14 - 3)\ mod\ 26$

$P_3 = (11)\ mod\ 26$

$P_3 = (11) = l$

$P_4 = (C_4 - K)\ mod\ 26$

$P_4 = (14 - 3)\ mod\ 26$

$P_4 = (11)\ mod\ 26$

$P_4 = (11) = l$

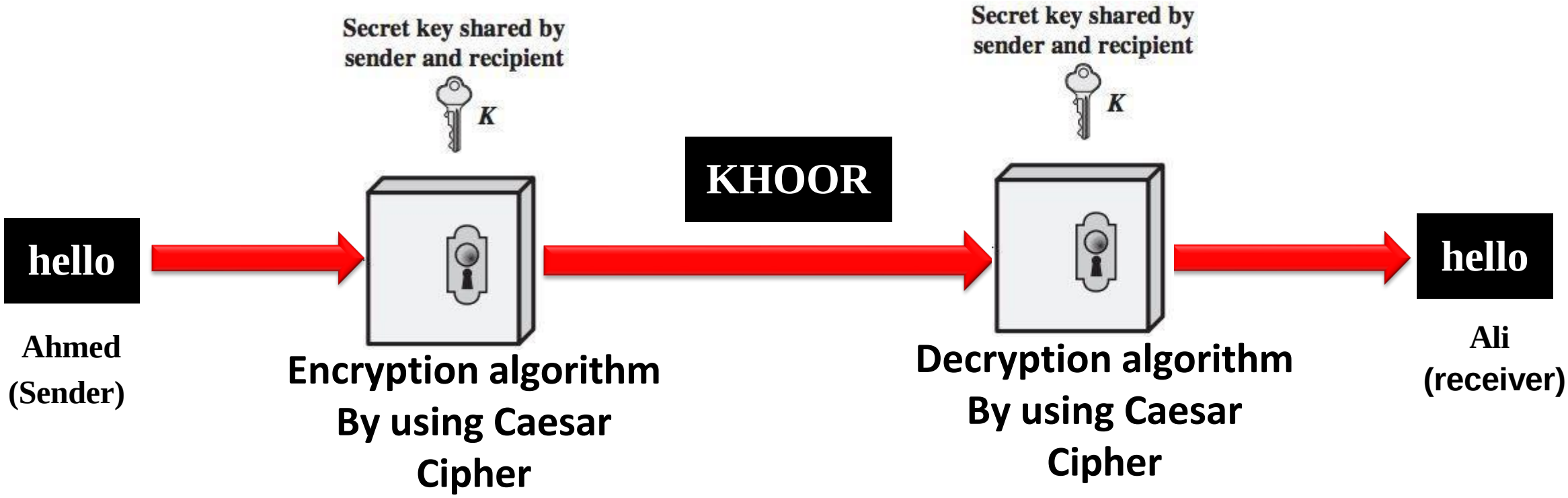
$P_5 = (C_5 - K)\ mod\ 26$

$P_5 = (17 - 3)\ mod\ 26$

$P_5 = (14)\ mod\ 26$

$P_5 = (14) = o$

Plaintext : $P_1P_2P_3P_4P_5$ → hello


Secret key shared by sender and recipient
K
Secret key shared by sender and recipient
K
KHOOR
hello
hello
Ahmed (Sender)
Encryption algorithm By using Caesar Cipher
Decryption algorithm By using Caesar Cipher
Ali (receiver)

Homework

1. By using **Additive Cipher** find the encrypt and decrypt for the message "**meet me after the conference**" with **K=u**.
2. By using **Shift Cipher** find the Plaintext for the Cipher text "**FVBKPKPANYLHAQVI**" with the Key **K=7**.