جامعة الحمدانية /كلية التربية

قسم علوم الحاسوب

Fourth Class

# Data Security


استاذ المادة:

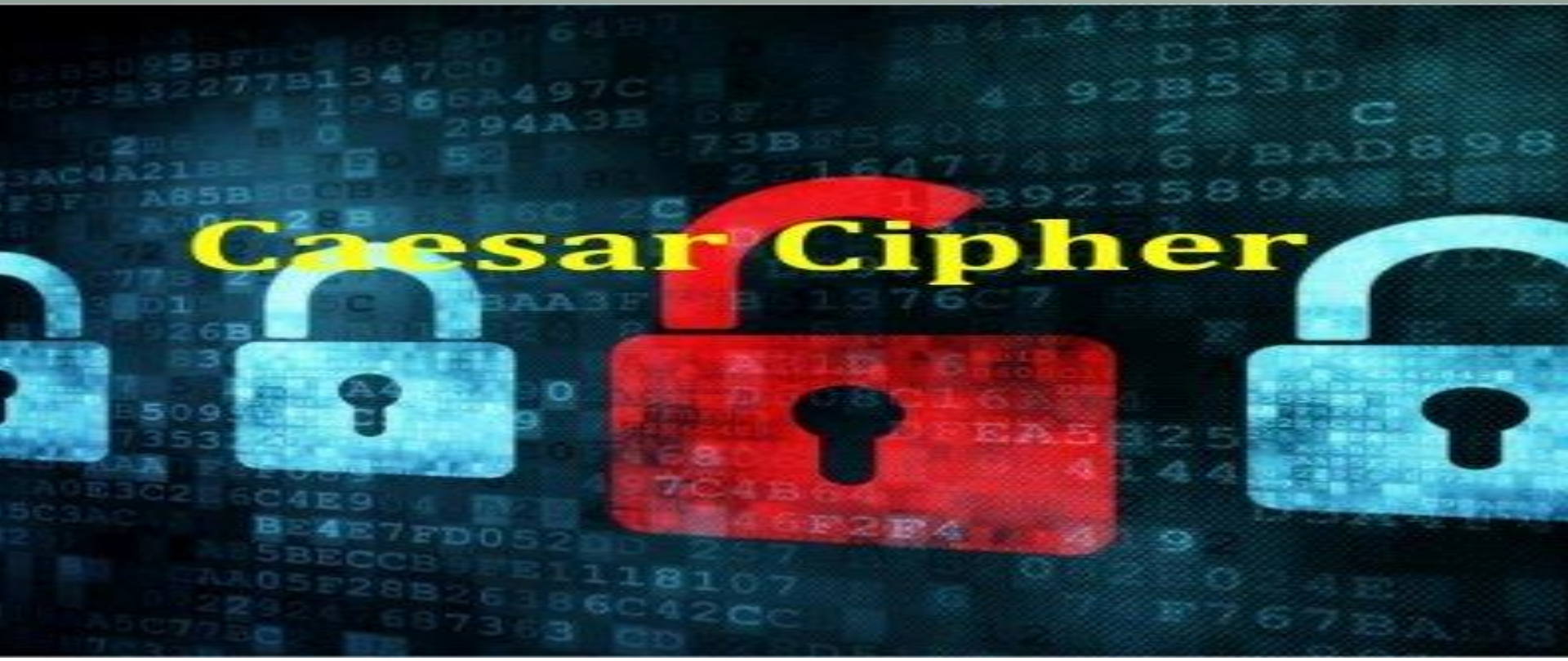
م. سماح فخري عزيز

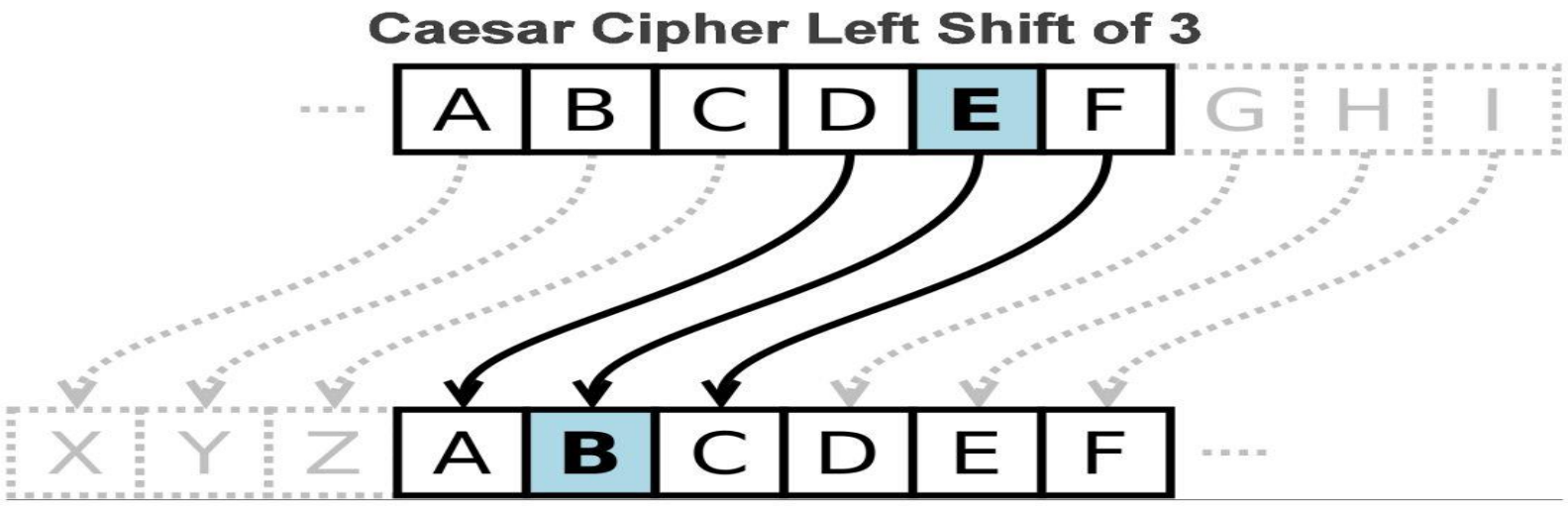
# Lecture

## Caesar Cipher

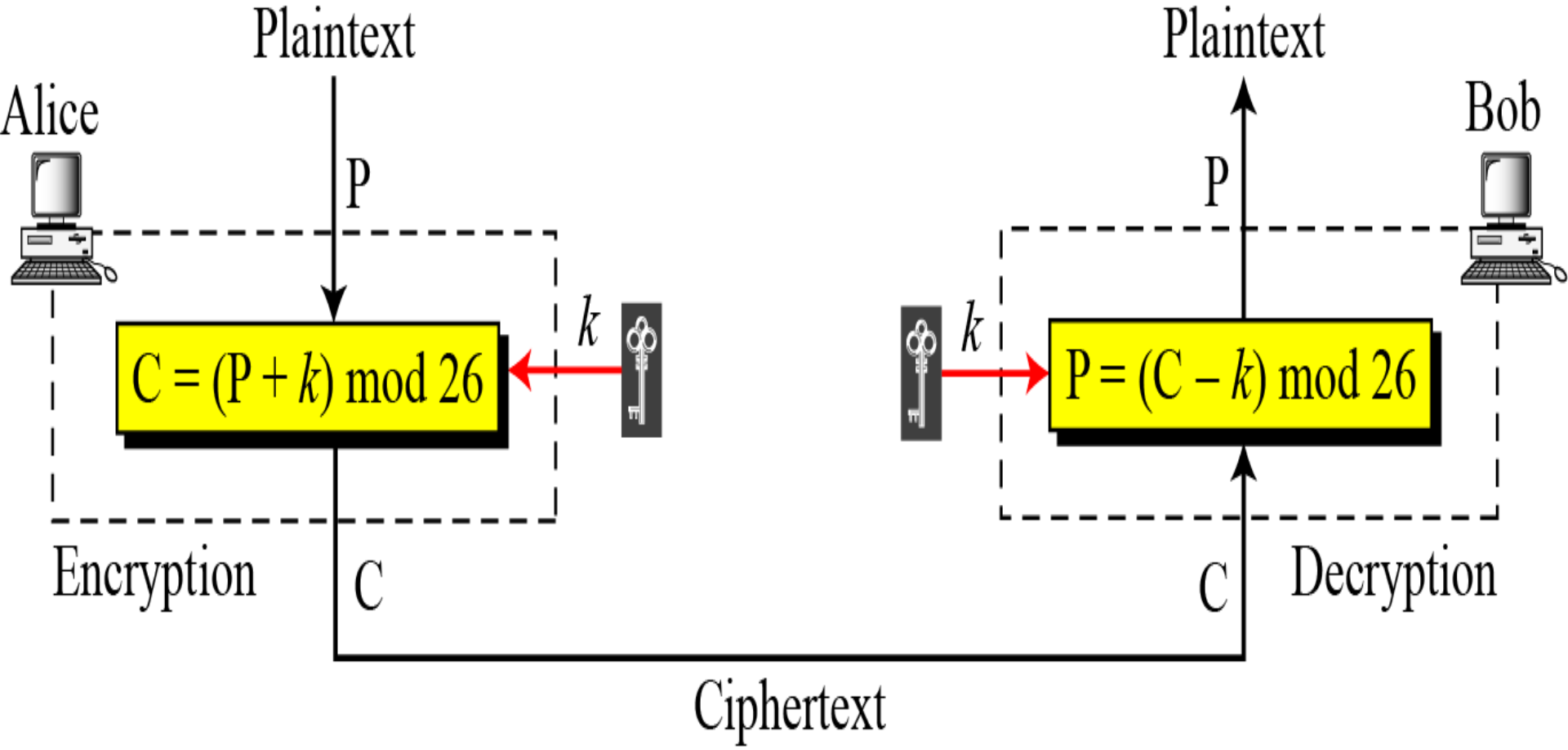
- is the simplest monoalphabetic cipher. It is sometimes called a shift cipher and sometimes **a Caesar cipher**, but the term additive cipher better reveals its mathematical nature. When the cipher is additive, the plaintext, ciphertext, and key are integers.

- **Additive Cipher**


Caesar Cipher


Caesar Cipher Left Shift of 3
A B C D E F G H I
X Y Z A B C D E F

# Caesar cipher



- **Caesar Cipher: -** Named for Julious Caesar.
- Caesar used a key of 3 for his communications.

- **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

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

- **Ciphertext**

- Plaintext : computer

  ciphertext : FRPSXWHU

# Caesar cipher

- **K= number of shift**

$$C=Ek(m)= (m+k) \text{ mode } 26$$

*The nubmer of accept keys is 26*

# *Example*

- Use the additive cipher with key = 15 to encrypt the plain text (hello).

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

- Plaintext : h e l l o

7 4 11 11 14

# Encryption

- (7+15) mod 26=22→ W
- (4+15) mod 26=19 →T
- (11 +15) mod 26=0 →A
- (11+15) mod 26=0 →A
- (14+15) mod 26=3 →D
- Ciphertext WTAAD

# Decryption

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

- Ciphertext: W T A A D
  22 19 0 0 3

(22-15) mod 26=7→ h
(19-15) mod 26=4 →e
(0-15) mod 26=11 →l
(0-15) mod 26=11 →l
(3-15) mod 26=14 →0

plaintext: h e l l o

شكرا

لكم