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

Fourth Stage

Security

Lecture 10

Asst. Lec. Yousif Samer Mudhafar

Email: yousif.samir19@gmail.com

Lecture objective

The student will recognize the following objective :

- **Encryption and Decryption using One Time Pad Cipher.**

One Time Pad

- One Time Pad (OTP) is a crypto algorithm where plaintext is combined with a random key.
- The key is at least as long as the message or data that must be encrypted.
- Each key is used only once, and both sender and receiver must destroy their key after use.
- This technique suggests using a random key that is as the message, so that the key need not be repeated. In addition, the key is to be used to encrypt and decrypt a single message, and then is discarded. Each new message requires a new key of the same length as the new message. Such a scheme, known as a One Time Pad, is unbreakable. It produces random output that bears no statistical relationship to the plaintext. Because the Ciphertext contains no information whatsoever about the plaintext, there is simply no way to break the code.

One Time Pad Cipher

Alice

Sender

Bob

Receiver

$C_i=(P_i+K_i) \bmod 26$ ← K

Encryption

K → $P_i=(C_i-K_i) \bmod 26$

Decryption

Cipher text

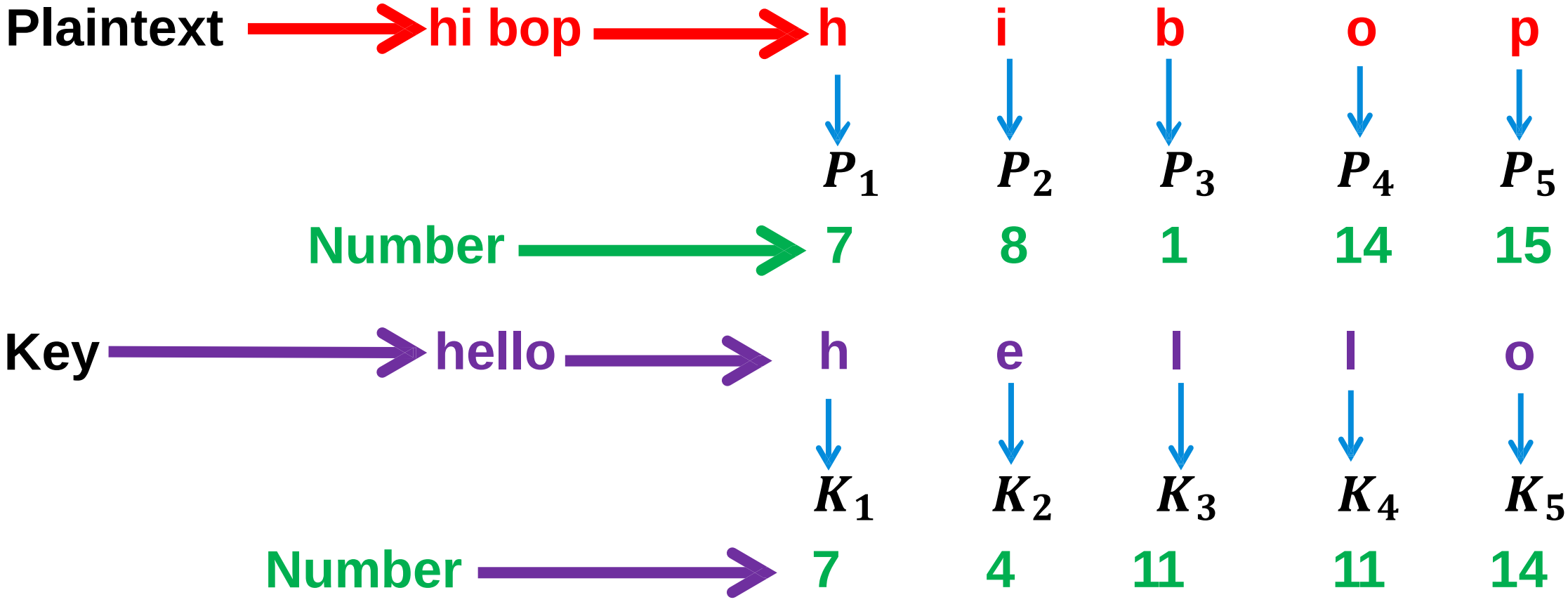
Example

Encrypt and decrypt the **Plaintext "hi bop"** by using **One Time Pad Cipher** with the **Keyword "hello"**

Ans:-

1. Encryption Algorithm

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



$$C_1 = (P_1 + K_1) \bmod 26$$
$$C_1 = (7 + 7) \bmod 26$$
$$C_1 = (14) \bmod 26$$
$$C_1 = (14) = O$$

$$C_2 = (P_2 + K_2) \bmod 26$$
$$C_2 = (8 + 4) \bmod 26$$
$$C_2 = (12) \bmod 26$$
$$C_2 = (12) = M$$

$$C_3 = (P_3 + K_3) \bmod 26$$
$$C_3 = (1 + 11) \bmod 26$$
$$C_3 = (12) \bmod 26$$
$$C_3 = (12) = M$$

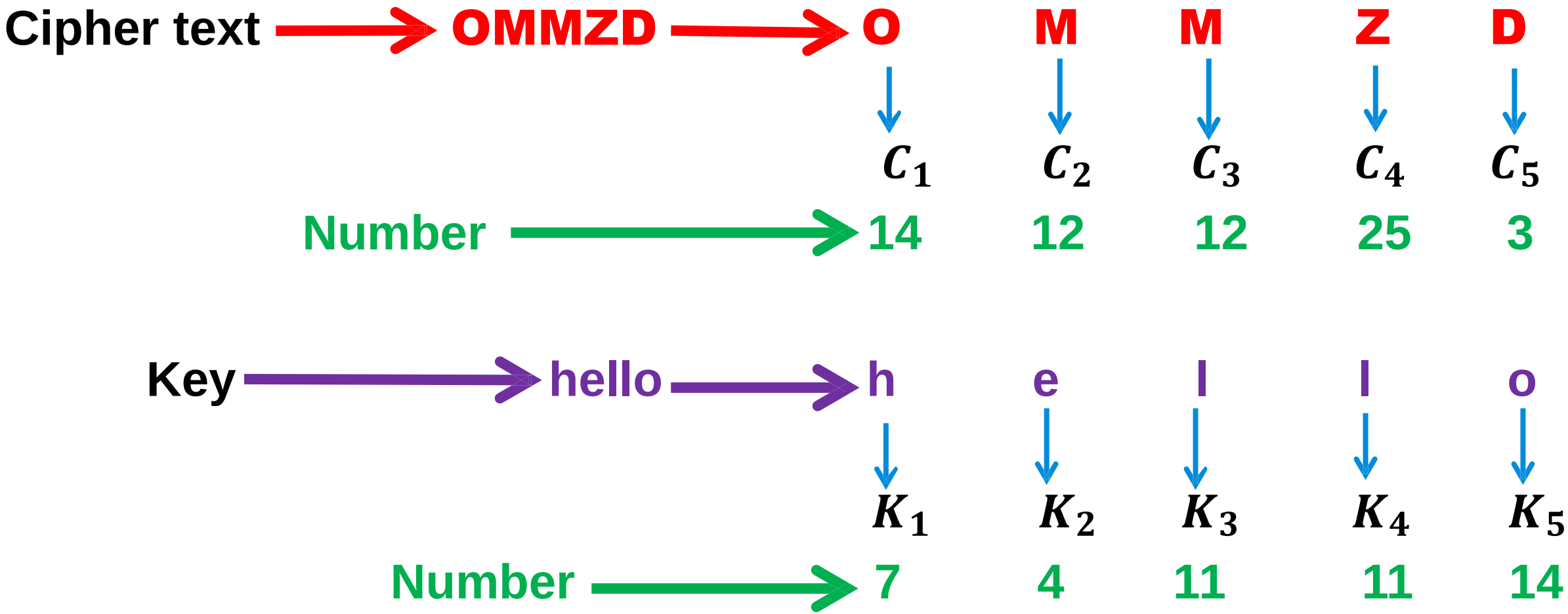
$$C_4 = (P_4 + K_4) \bmod 26$$
$$C_4 = (14 + 11) \bmod 26$$
$$C_4 = (25) \bmod 26$$
$$C_4 = (25) = Z$$

$$C_5 = (P_5 + K_5) \bmod 26$$
$$C_5 = (15 + 14) \bmod 26$$
$$C_5 = (29) \bmod 26$$
$$C_5 = (3) = D$$

The **Cipher text** is "**OMMZD**"

2. Decryption Algorithm

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



$$P_1 = (C_1 - K_1) \bmod 26$$
$$P_1 = (14 - 7) \bmod 26$$
$$P_1 = (7) \bmod 26$$
$$P_1 = (7) = h$$

$$P_2 = (C_2 - K_2) \bmod 26$$
$$P_2 = (12 - 4) \bmod 26$$
$$P_2 = (8) \bmod 26$$
$$P_2 = (8) = i$$

$$P_3 = (C_3 - K_3) \bmod 26$$
$$P_3 = (12 - 11) \bmod 26$$
$$P_3 = (1) \bmod 26$$
$$P_3 = (1) = b$$

$$P_4 = (C_4 - K_4) \bmod 26$$
$$P_4 = (25 - 11) \bmod 26$$
$$P_4 = (14) \bmod 26$$
$$P_4 = (14) = o$$

$$P_5 = (C_5 - K_5) \bmod 26$$
$$P_5 = (3 - 14) \bmod 26$$
$$P_5 = (-11) \bmod 26$$
$$P_5 = (-11 + 26) = 15 = p$$

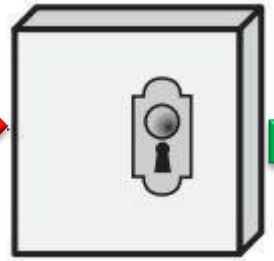
The Plaintext is "hi bop"

Keyword is “hello”

Keyword is “hello”

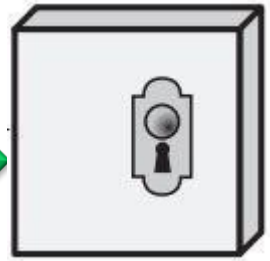
hi bop

(Sender)



Encryption algorithm
By using One Time
Pad Cipher

OMMZD



Decryption algorithm
By using One Time Pad
Cipher

hi bop

(receiver)