جامعة الحمدانية /كلية التربية

قسم علوم الحاسوب

Fourth Class

Data Security

استاذ المادة:

م. سماح فخري عزيز

- **Multiplicative Cipher**

- While using Caesar cipher technique, encrypting and decrypting symbols involves converting the values into numbers with a simple basic procedure of addition or subtraction.

- Let us think up a different method of enciphering a message. Instead of adding a key number to the equivalents of the plain text letters, we shall multiply by the key number.

- **Multiplicative Cipher**

Multiplicative Cipher

- is the simplest monoalphabetic cipher. It is sometimes called a **Multiplicative Cipher**.

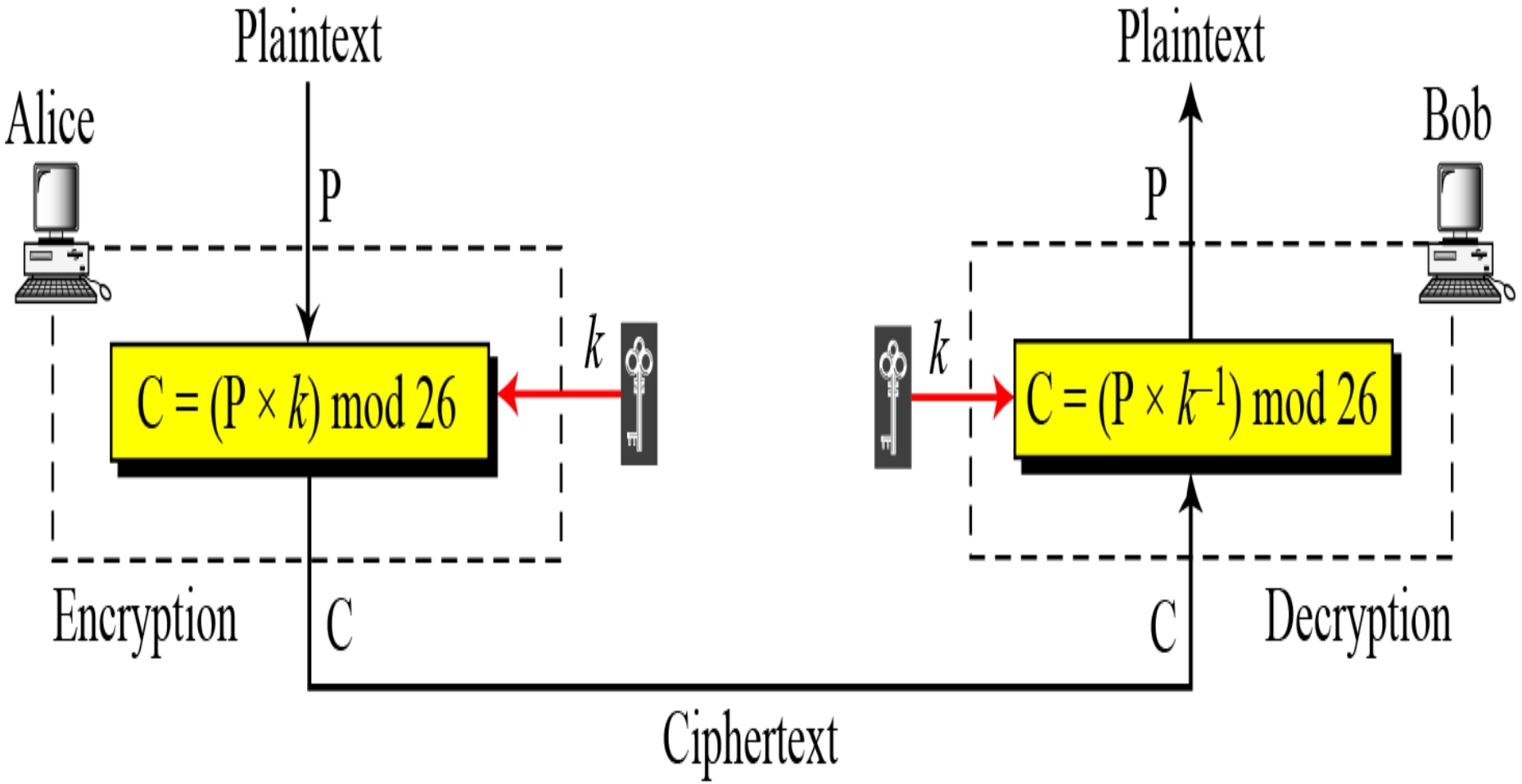
- If multiplication is used to convert to cipher text, it is called a wrap-around situation.

Accepted keys

- Number of accepted keys for any multiplicative cipher which must be is the set that has only 12 key:

[1, 3, 5, 7, 9, 11, 15, 17, 19, 21, 23, 25]

Multiplicative Cipher



Encryption using the Multiplication Cipher

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

The nubmer of accept keys is 12

Alphabetic

0	1	2	3	4	5	6	7	8	9	10	11	12
A	B	C	D	E	F	G	H	I	J	K	L	M

13	14	15	16	17	18	19	20	21	22	23	24	25
N	O	P	Q	R	S	T	U	V	W	X	Y	Z

Example

- We use a multiplicative cipher to encrypt the message “**hello**”
- with a key of 7.

Encryption

Plaintext: h → 07	Encryption: (07 x 07) mod 26	ciphertext: 23 → X
Plaintext: e → 04	Encryption: (04 x 07) mod 26	ciphertext: 02 → C
Plaintext: l → 11	Encryption: (11 x 07) mod 26	ciphertext: 25 → Z
Plaintext: l → 11	Encryption: (11 x 07) mod 26	ciphertext: 25 → Z
Plaintext: o → 14	Encryption: (14 x 07) mod 26	ciphertext: 20 → U

The ciphertext is “XCZZU

Example 2

- **plaintext [Computer] by using Multiplicative cipher by equations with key [5]**

- **Computer**
- **C1= 2*5 mod 26**= 10= K

- Homework:
- Write the decryption equation?

شكرا

لكم