جامعة الحمدانية /كلية التربية

قسم علوم الحاسوب

Fourth Class

Data Security

استاذ المادة:

م. سماح فخري عزيز

Lecture

- **Affine Cipher**

- The additive cipher is a special case of an affine cipher. The multiplicative cipher is a special case of affine cipher.

- The affine cipher uses a pair of keys in which the first key is from Z26* and the second is from Z26+. The size of the key domain is 26 × 12 = 312.

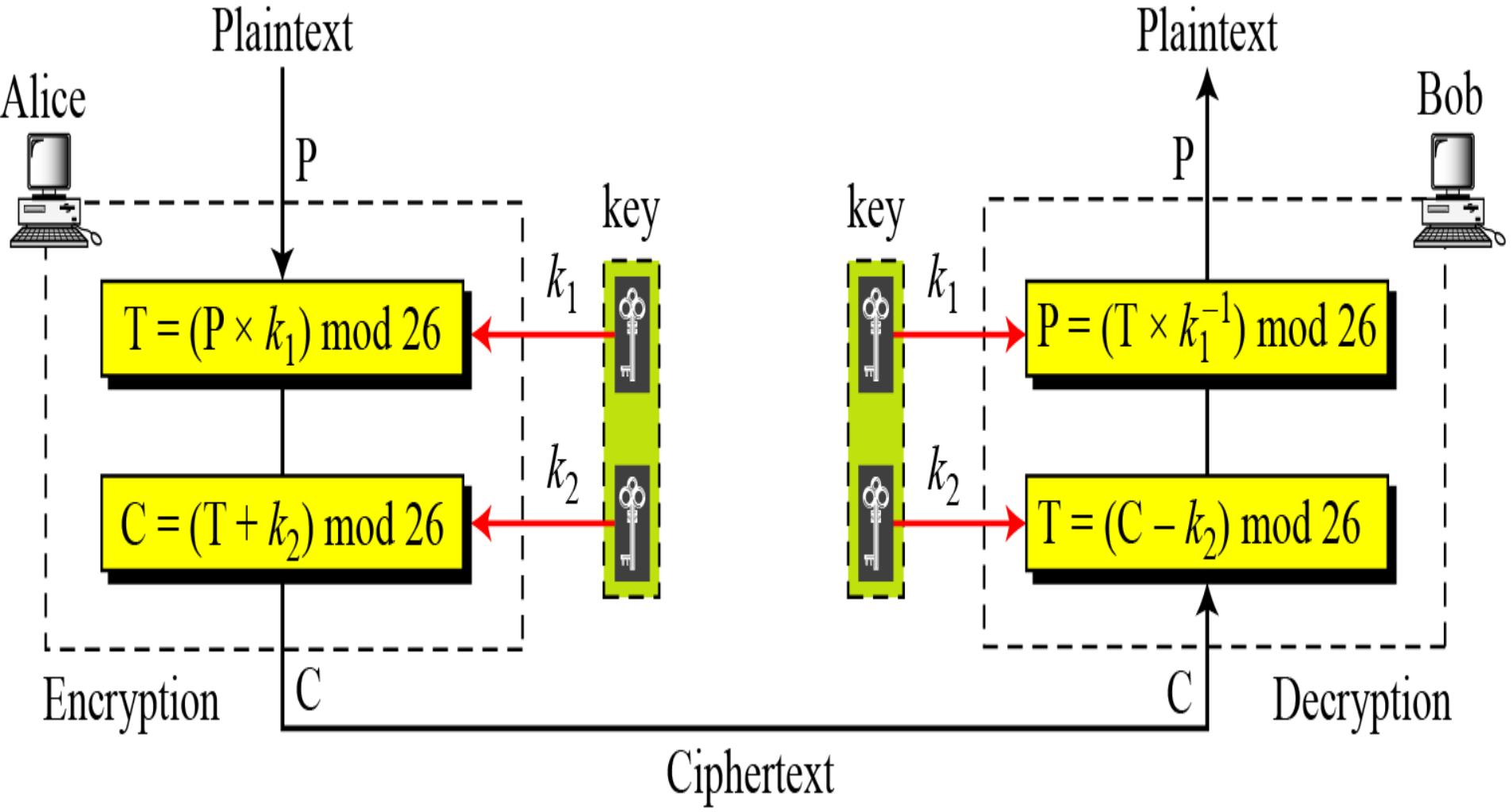
- Affine cipher

Accepted keys

- Number of accepted keys for any affine cipher which must be is the set that has only 312 key:

➢ $26 \times 12 = 312$.

Affine Cipher



Encryption using the Affine Cipher

$$C = (P \times k_1 + k_2) \bmod 26$$

The number of accept keys is 312

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

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

  with a key of 7,2.

Encryption

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

To decrypt the message “ZEBBW” with the key pair (7, 2) in modulus 26.

Example 2

- **plaintext [Computer] by using affine cipher by equations with key [7,2]**

Computer

- Homework:

- Write the affine decryption equation?

شكرا لكم