Network and Information Security
Lecture 6

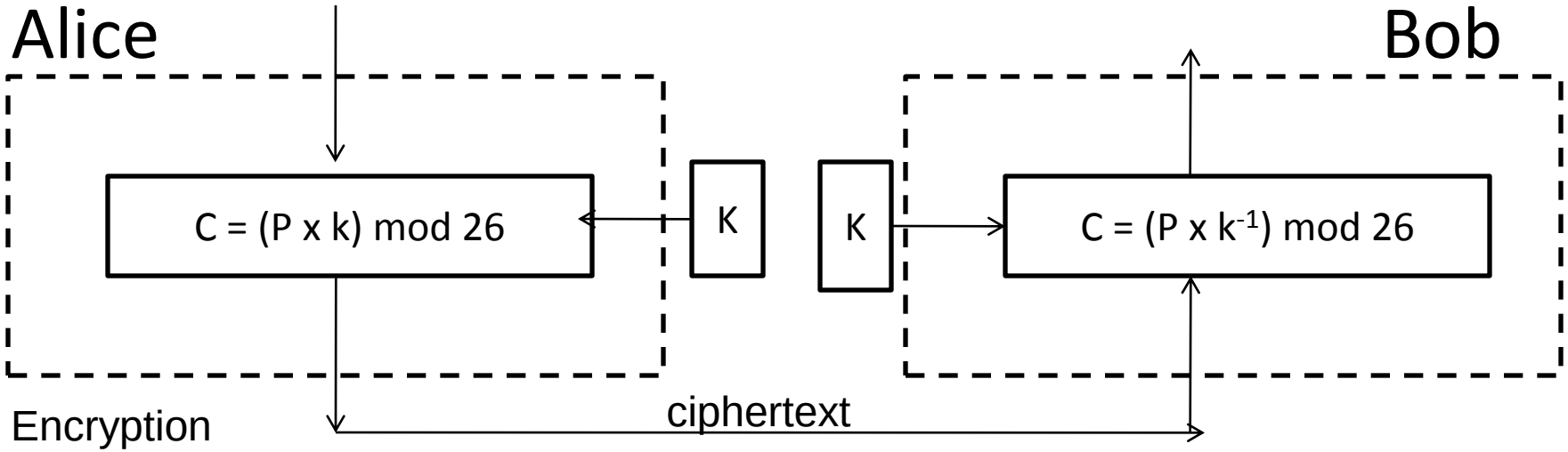
B.Tech. Computer Engineering
Sem. VI.

Prof. Mrudang T. Mehta
Associate Professor
Computer Engineering Department
Faculty of Technology,
Dharmsinh Desai University, Nadiad

Multiplicative Cipher

- Encryption
- $C = (p \times k) \bmod 26$
- Decryption
- $C = (p \times k^{-1}) \bmod 26$
- In multiplicative cipher, the plaintext and the cipher text are integers in Z_{26}, the key is an integer in Z_{26*}.
- What is the key domain of the multiplicative cipher?

- The encryption algorithm specifies multiplication of the plaintext by the key and the decryption algorithm specifies division of the ciphertext by the key.



The key needs to belong to the set Z_{26^*} to guarantee that the encryption and decryption are inverses of each other.

Decryption
Multiplying by the multiplicative inverse of the key

- Example

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

Plain text : h e l l o (07 04 11 11 14)

Encryption:

(07 x 07) mod 26 = 23 (X)

(04 x 07) mod 26 = 02 (C)

(11 x 07) mod 26 = 25 (Z)

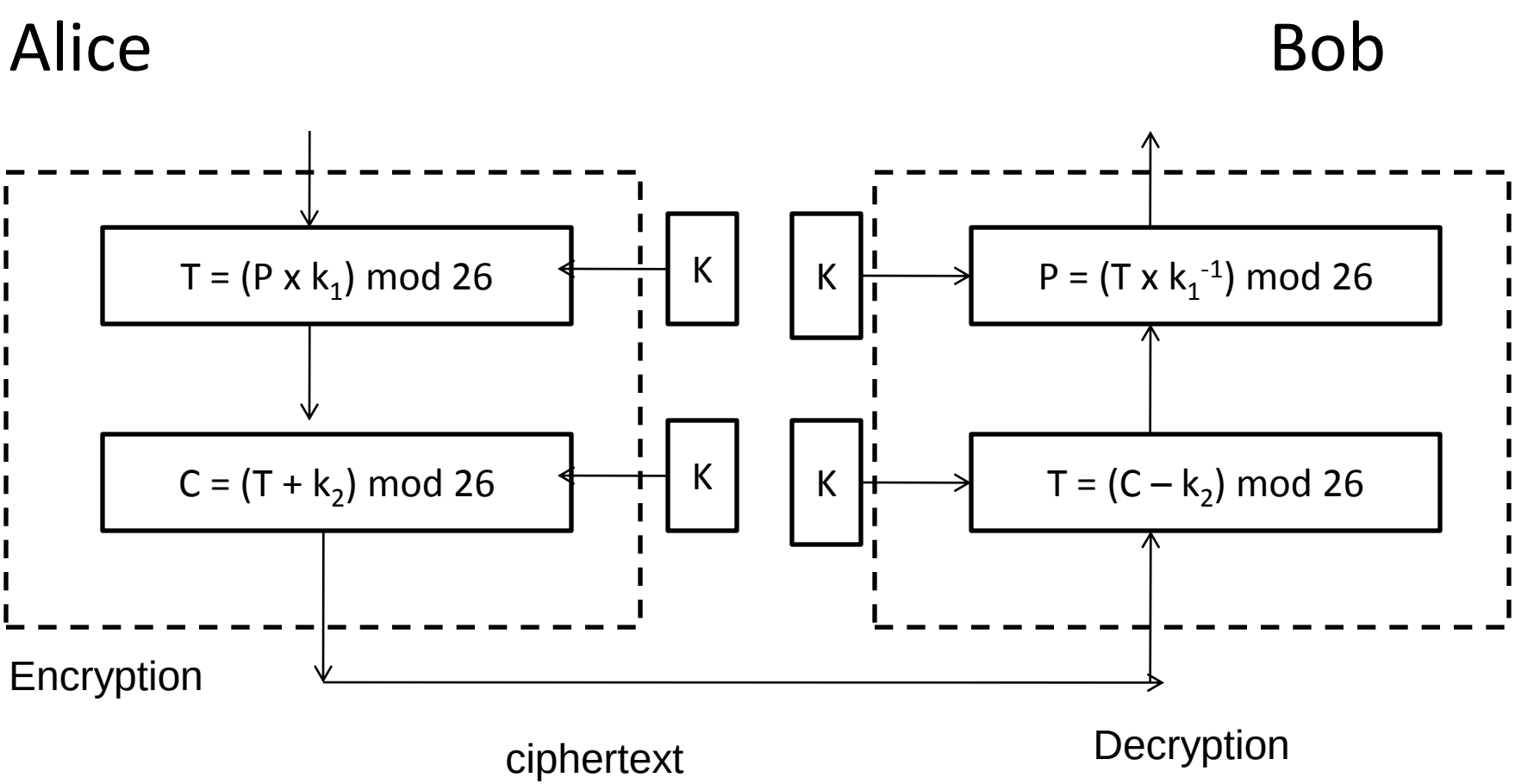
(11 x 07) mod 26 = 25 (Z)

(14 x 07) mod 26 = 20 (U)

Use Key value 9 and encrypt the plain text.

Affine Cipher

- Affine cipher is a combination of additive and multiplicative ciphers with a pair of keys.
- First key: Multiplicative cipher [From Z_{26^*}]
- Second key: Additive Cipher [From Z_{26}]


Alice
Bob
T = (P x k1) mod 26
K
K
P = (T x k1-1) mod 26
C = (T + k2) mod 26
K
K
T = (C – k2) mod 26
Encryption
ciphertext
Decryption

- Example
- Use the affine cipher to decrypt the message “ZEBBW” with the key pair (7,2) in modulus 26.

Cryptanalysis of Affine Cipher

- Chosen plain text attack
- Assume that Eve intercepts the following cipher text: PWUFFOGWCHFDWTWEJOUUNJORSMDWRHVCMWJUPVCCG
- Eve also very briefly obtains access to Alice's computer and has only enough time to type a two-letter plain text “et”
- She then tries to encrypt short plain text using two different algorithms because she is not sure which one is the affine cipher.

- Algorithm 1: Plaintext of et -> ciphertext ->WC
- Algorithm 2: Plaintext of et -> ciphertext ->WF
- To, find the key Eve uses the following strategy,

a. Eve knows that if the first algorithm is affine,

PT	CT	PT	CT
e	W	t	C
04	22	19	02

$$04 \times k_1 + k_2 \equiv 22 \pmod{26}$$

$$-\ 19 \times k_1 + k_2 \equiv 02 \pmod{26}$$

$$(-15) \times k_1 \equiv 20 \pmod{26}$$

$$k_1 \equiv (-15)^{-1} \times 20 \pmod{26}$$

$$\equiv (11)^{-1} \times 20 \pmod{26}$$

Multiplicative inverse of 11 is 19.

$(19 \times 11) \bmod 26 = (209) \bmod 26 = 1$

$k_1 = (19 \times 20) \bmod 26 = 380 \bmod 26 = 16$

16 is not having multiplicative inverse in Z_{26^*}

b. Eve now tries the result of the second set of data.

PT	CT	PT	CT
e	W	t	F
04	22	19	05

$$04 \times k_1 + k_2 \equiv 22 \pmod{26}$$

$$-\ 19 \times k_1 + k_2 \equiv 05 \pmod{26}$$

$$(-15) \times k_1 \equiv 17 \pmod{26}$$

$$k_1 \equiv (-15)^{-1} \times 17 \pmod{26}$$

$$\equiv (11)^{-1} \times 17 \pmod{26}$$

Multiplicative inverse of 11 is 19.

$(19 \times 11) \bmod 26 = (209) \bmod 26 = 1$

$k_1 = (19 \times 17) \bmod 26 = 323 \bmod 26 = 11$

$k_1 = 11$

$4 \times 11 + k_2 \equiv 22 \pmod{26}$

$44 + k_2 \equiv 22 \pmod{26}$

$k_2 = 22 - 44 \pmod{26}$

$= -22 \bmod 26$

$= 04 \bmod 26$

$= 4$