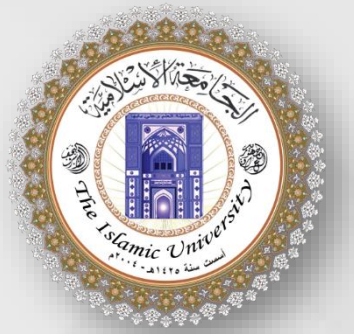


The Islamic University
College of Technical Engineering
Department of Computer Technical Engineering

Fourth Stage

Security

Lecture 2

Asst. Lec. Yousif Samer Mudhafar

Email: yousif.samir19@gmail.com

Lecture objectives

The student will recognize the following objectives :

1. **Encryption and Decryption using Multiplicative Cipher.**
2. **Encryption and Decryption using Affine Cipher.**

Multiplicative Cipher

Alice

Sender

Bob

Receiver

C_i=(P_i*K) mod 26

K

Encryption

K^{-1}

P_i=(C_i*K^{-1}) mod 26

Decryption

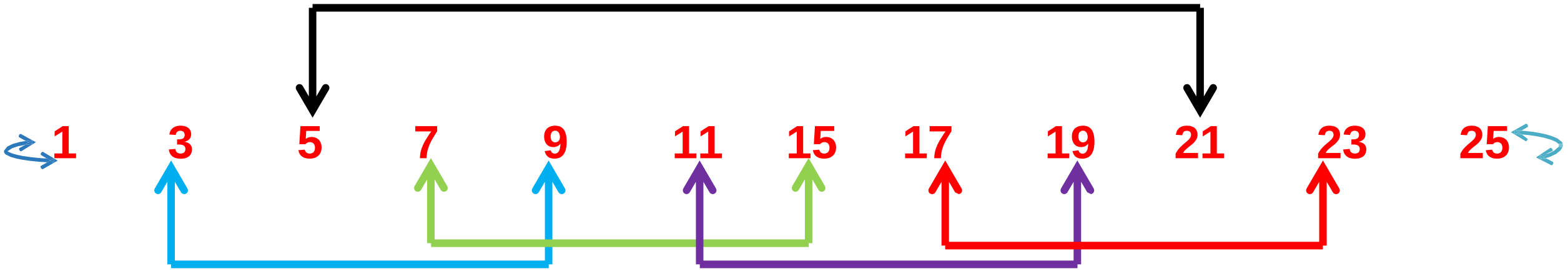
Cipher text

Key

The set which is used as a Keys in the Multiplicative Cipher are 12 Numbers.

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

$$[(K * K^{-1}) \bmod 26] = 1$$



Example 1

Encrypt and decrypt for the Plaintext "**hello**" by using Multiplicative Cipher by using the **Key** = **9**.

Ans:-

1. Encryption

$$C_i = (P_i * K) \ mod \ 26$$

Plaintext	hello	h	e	l	l	o
		P_1	P_2	P_3	P_4	P_5
Number		7	4	11	11	14

$C_1 = (P_1 * K) \ mod \ 26$

$C_1 = (7 * 9) \ mod \ 26$

$C_1 = (63) \ mod \ 26$

$C_1 = (11) = L$

$C_2 = (P_2 * K) \ mod \ 26$

$C_2 = (4 * 9) \ mod \ 26$

$C_2 = (36) \ mod \ 26$

$C_2 = (10) = K$

$C_3 = (P_3 * K) \ mod \ 26$

$C_3 = (11 * 9) \ mod \ 26$

$C_3 = (99) \ mod \ 26$

$C_3 = (21) = V$

$C_4 = (P_4 * K) \ mod \ 26$

$C_4 = (11 * 9) \ mod \ 26$

$C_4 = (99) \ mod \ 26$

$C_4 = (21) = V$

$$C_5 = (P_5 * K)\ mod\ 26$$

$$C_5 = (14 * 9)\ mod\ 26$$

$$C_5 = (126)\ mod\ 26$$

$$C_5 = (22) = W$$

Cipher text : $C_1C_2C_3C_4C_5$ → **LKVVW**

The Cipher text for the Plaintext (hello) will be (LKVVW)

$\mathbf{Key^{-1}}$

K=9

$\mathbf{K^{-1}}$ **= 3**

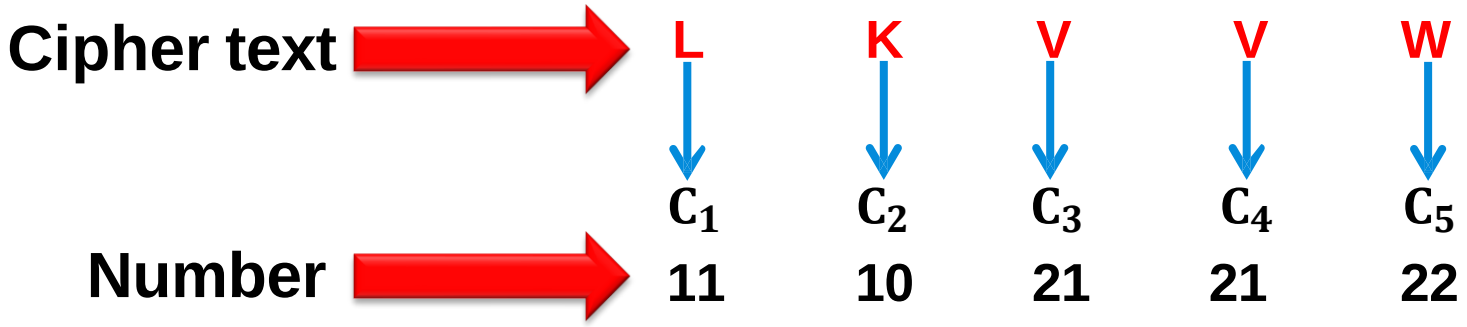
$$[(K * K^{-1}) \bmod 26] = 1$$

$$[(9 * 3) \bmod 26]$$

$$[(27) \bmod 26] = 1$$

2. Decryption

$$P_i = (C_i * K^{-1}) \bmod 26$$



$P_1 = (C_1 * K^{-1}) \ mod \ 26$

$P_1 = (11 * 3) \ mod \ 26$

$P_1 = (33) \ mod \ 26$

$P_1 = (7) = h$

$P_2 = (C_2 * K^{-1}) \ mod \ 26$

$P_2 = (10 * 3) \ mod \ 26$

$P_2 = (30) \ mod \ 26$

$P_2 = (4) = e$

$P_3 = (C_3 * K^{-1}) \ mod \ 26$

$P_3 = (21 * 3) \ mod \ 26$

$P_3 = (63) \ mod \ 26$

$P_3 = (11) = l$

$P_4 = (C_4 * K^{-1}) \ mod \ 26$

$P_4 = (21 * 3) \ mod \ 26$

$P_4 = (63) \ mod \ 26$

$P_4 = (11) = l$

$P_5 = (C_5 * K^{-1}) \ mod \ 26$

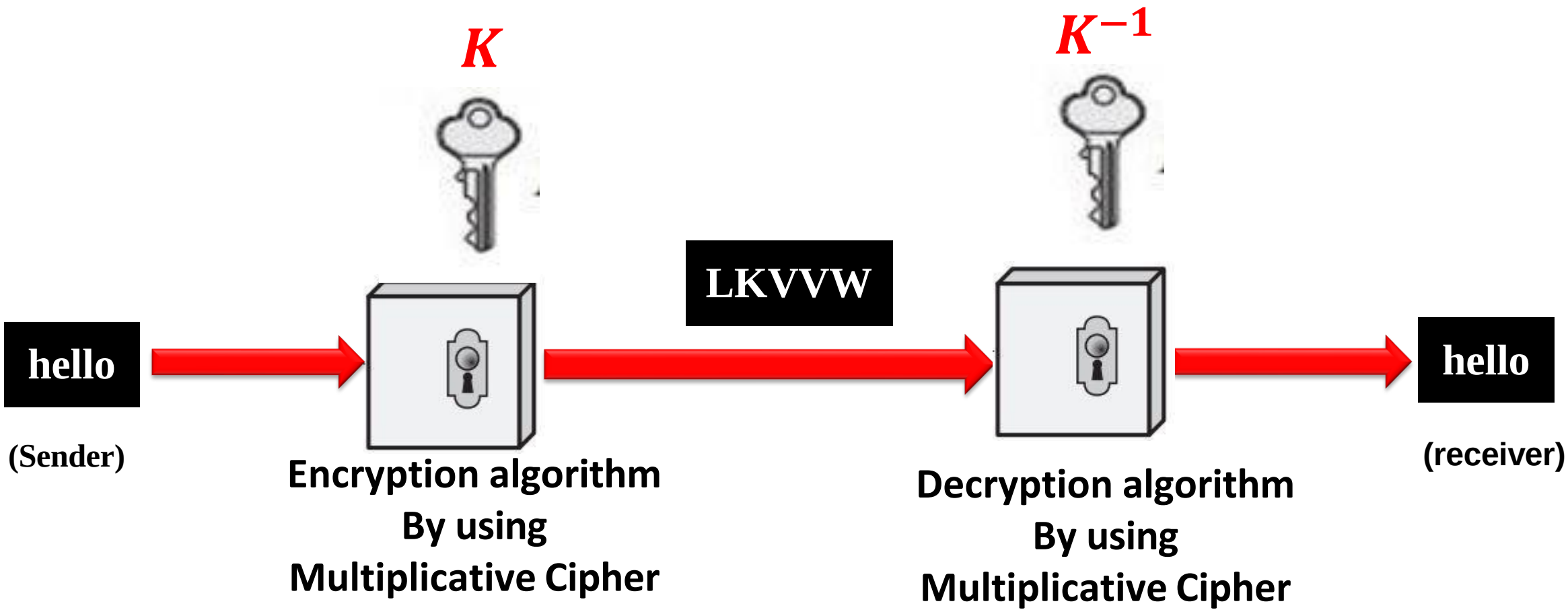
$P_5 = (22 * 3) \ mod \ 26$

$P_5 = (66) \ mod \ 26$

$P_5 = (14) = o$

Plaintext : $P_1P_2P_3P_4P_5$ → hello

The Plain text for the Cipher text (**LKVVW**) will be (**hello**)


K
K^{-1}
hello
LKVVW
hello
(Sender)
Encryption algorithm
By using
Multiplicative Cipher
Decryption algorithm
By using
Multiplicative Cipher
(receiver)

Affine Cipher

It is a technique where performed two encryption algorithms at once the first on is multiplication and the second one is addition cipher (Caesar cipher) in this order as Encryption operation and reversible in the decryption, in this technique it will require two Keys (K_1, K_2), The first Key (K_1) is for the multiplication operation while the second Key (K_2) its for the second operation.

Where K_1 is the first Key

K_2 is the second Key

Affine Cipher

Alice

Sender

Bob

Receiver

$$C_i = [(P_i * K_1) + K_2] \bmod 26$$

Encryption

$$P_i = [(C_i - K_2) * K_1^{-1}] \bmod 26$$

Decryption

Cipher text

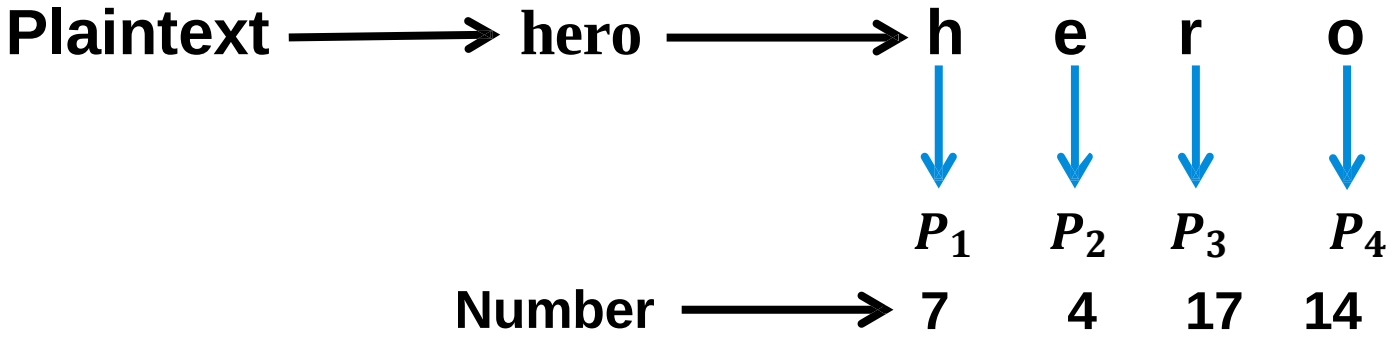
Example 2

Encrypt and decrypt for the word "**Hero**" by using **Affine Cipher** with the **Pair Key** (7, 2).

Ans:-

1. Encryption

$$C_i = [(P_i * K_1) + K_2] \bmod 26$$



$C_1 = *(P_1 * K_1) + K_2] \bmod 26$

$C_1 = *(7 * 7) + 2] \bmod 26$

$C_1 = (51)\ mod\ 26$

$C_1 = (25) = Z$

$C_2 = *(P_2 * K_1) + K_2] \bmod 26$

$C_2 = *(4 * 7) + 2] \bmod 26$

$C_2 = (30)\ mod\ 26$

$C_2 = (4) = E$

$C_3 = *(P_3 * K_1) + K_2] \bmod 26$

$C_3 = *(17 * 7) + 2] \bmod 26$

$C_3 = (121)\ mod\ 26$

$C_3 = (17) = R$

C_4=*(P_4*K_1)+K_2] mod 26

C_4=*(14*7)+2] mod 26

$C_4 = (100)\ mod\ 26$

$C_4 = (22) = W$

Cipher text : $C_1C_2C_3C_4$  ZERW

The Cipher text for the Plaintext (hero) will be (ZERW)

$\mathbf{Key^{-1}}$

$K_1 = 7$

$K_1^{-1} = 15$

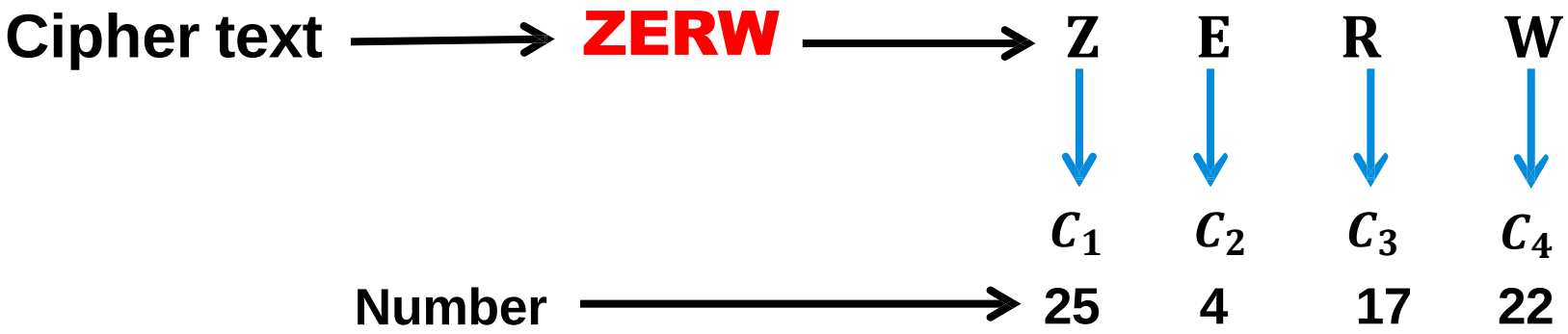
$$[(K_1 * K_1^{-1}) \bmod 26] = 1$$

$$[(7 * 15) \bmod 26]$$

$$[(105) \bmod 26] = 1$$

2. Decryption

$$P_i = [(C_i - K_2) * K_1^{-1}] \bmod 26$$



$$P_1 = [(C_1 - K_2) * K_1^{-1}] \, mod \, 26$$

$$P_1 = [(25 - 2) * 15] \, mod \, 26$$

$$P_1 = (345) \, mod \, 26$$

$$P_1 = (7) = \mathrm{h}$$

$$P_2 = [(C_2 - K_2) * K_1^{-1}] \, mod \, 26$$

$$P_2 = [(4 - 2) * 15] \, mod \, 26$$

$$P_1 = (30) \, mod \, 26$$

$$P_1 = (4) = e$$

$$P_3 = [(C_3 - K_2) * K_1^{-1}] \; mod \; 26$$

$$P_3 = [(17 - 2) * 15] \; mod \; 26$$

$$P_3 = (225) \; mod \; 26$$

$$P_3 = (17) = r$$

$$P_4 = [(C_4 - K_2) * K_1^{-1}] \; mod \; 26$$

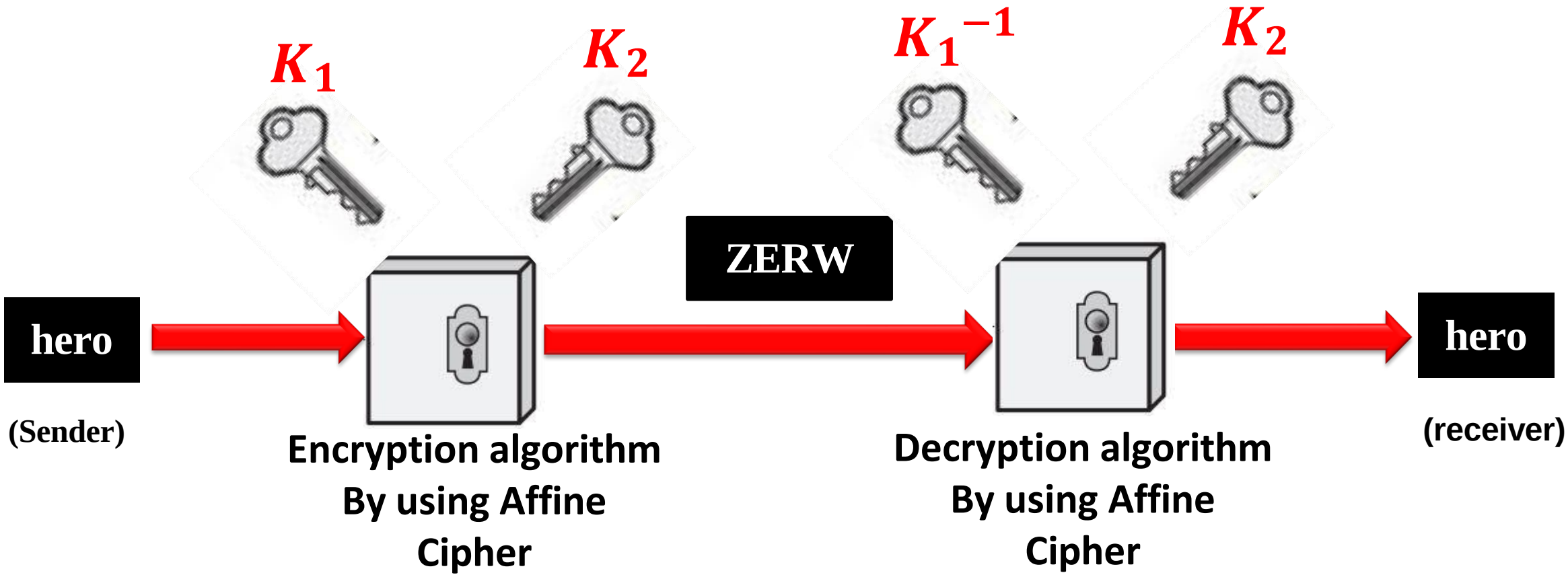
$$P_4 = [(22 - 2) * 15] \; mod \; 26$$

$$P_4 = (300) \; mod \; 26$$

$$P_4 = (14) = o$$

Plain text : $P_1 \, P_2 P_3 P_4$ → *hero*

The Plain text for the Cipher text (ZERW) will be (hero)


K_1
K_2
K_1^{-1}
K_2
hero
ZERW
hero
(Sender)
Encryption algorithm
By using Affine
Cipher
Decryption algorithm
By using Affine
Cipher
(receiver)

Homework

1. By using **Affine Cipher** decrypt the following message "**KYGREZ**" with the Pair **Key** (**9**,**4**).

2. Encrypt the message "**this is an exercise**" using the following ciphers.

- **Additive Cipher with key (20).**
- **Multiplicative Cipher with key (15).**
- **Affine Cipher with key (19, 20).**