جامعة الحمدانية /كلية التربية

قسم علوم الحاسوب

Fourth Class

Data Security

استاذ المادة:

م. سماح فخري عزيز

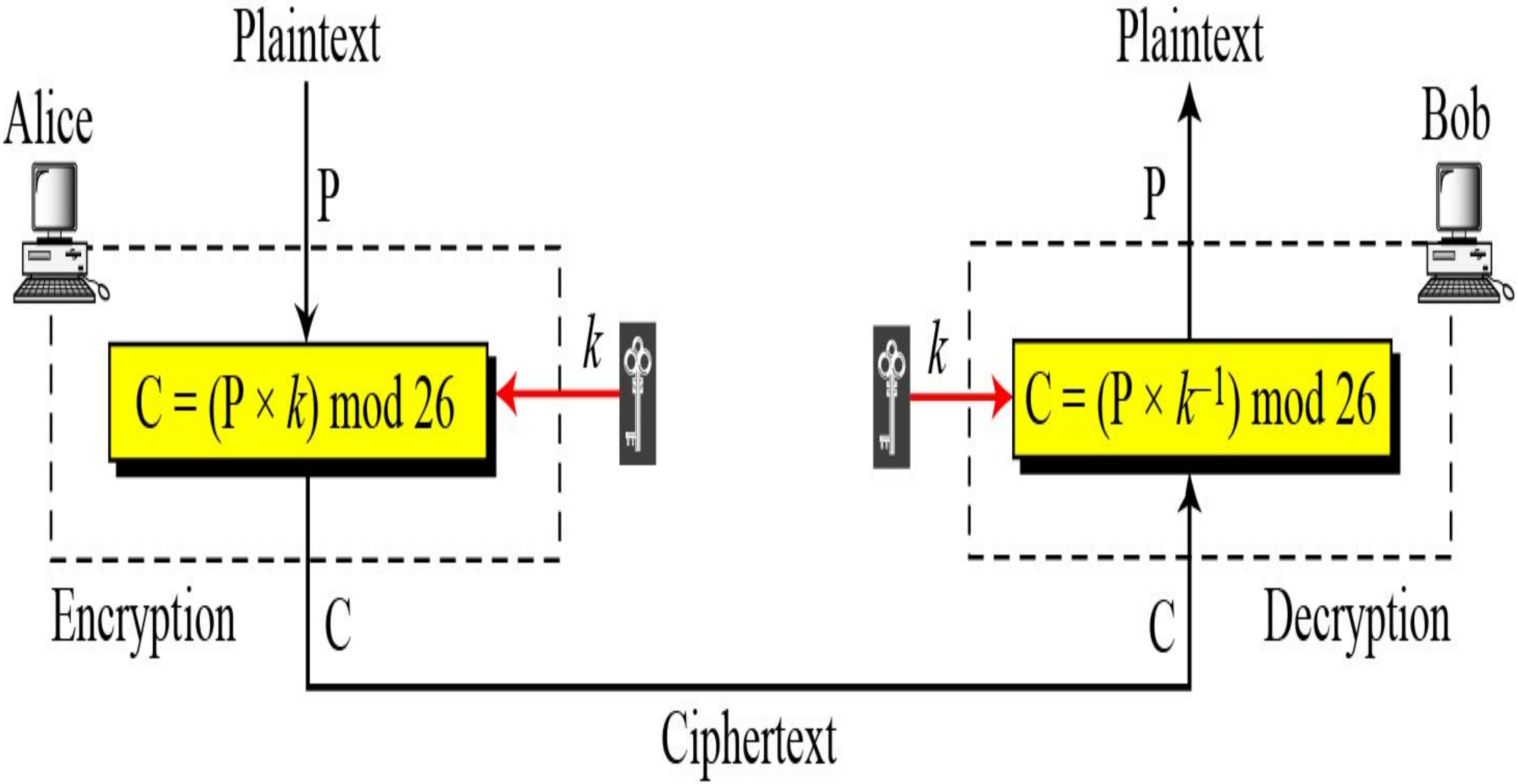
- Multiplicative Inverse

Accepted keys

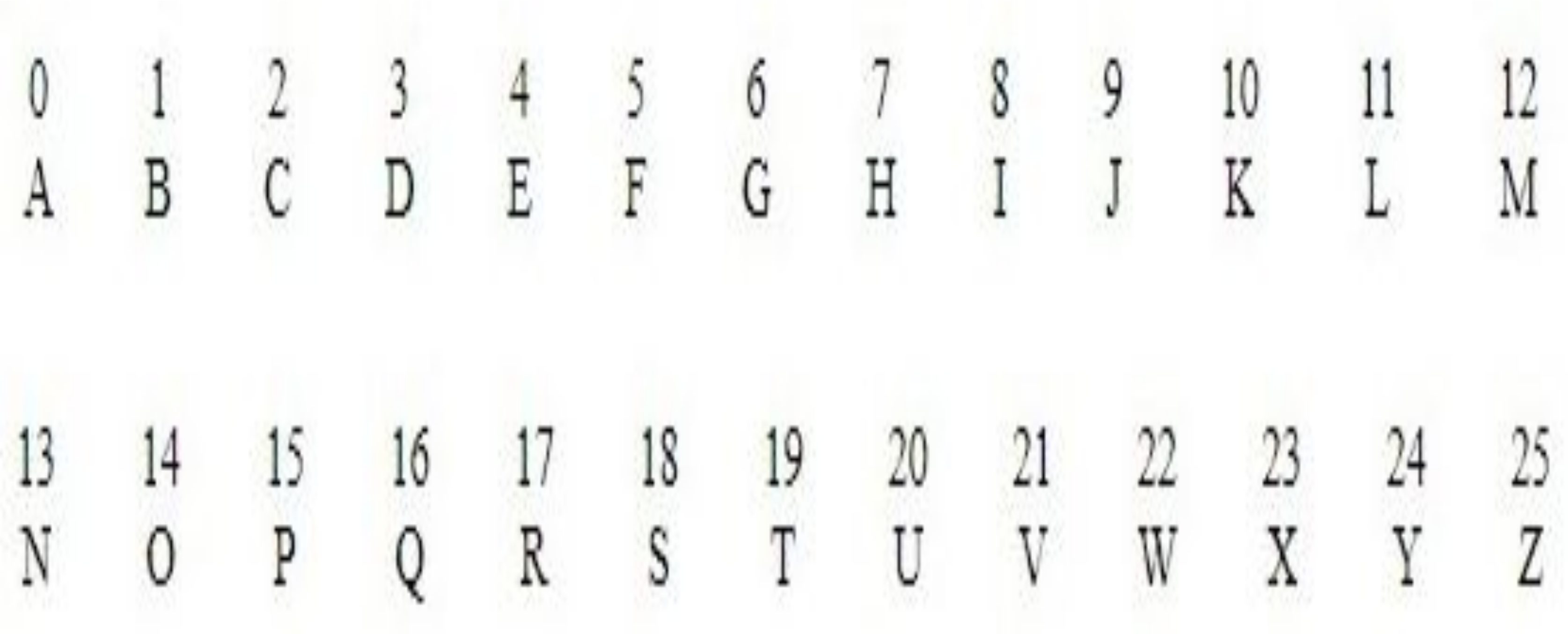
- Number of accepted keys for any multiplicative cipher which must be is the set that has only 12 key:

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

Multiplicative Cipher



Alphabetic

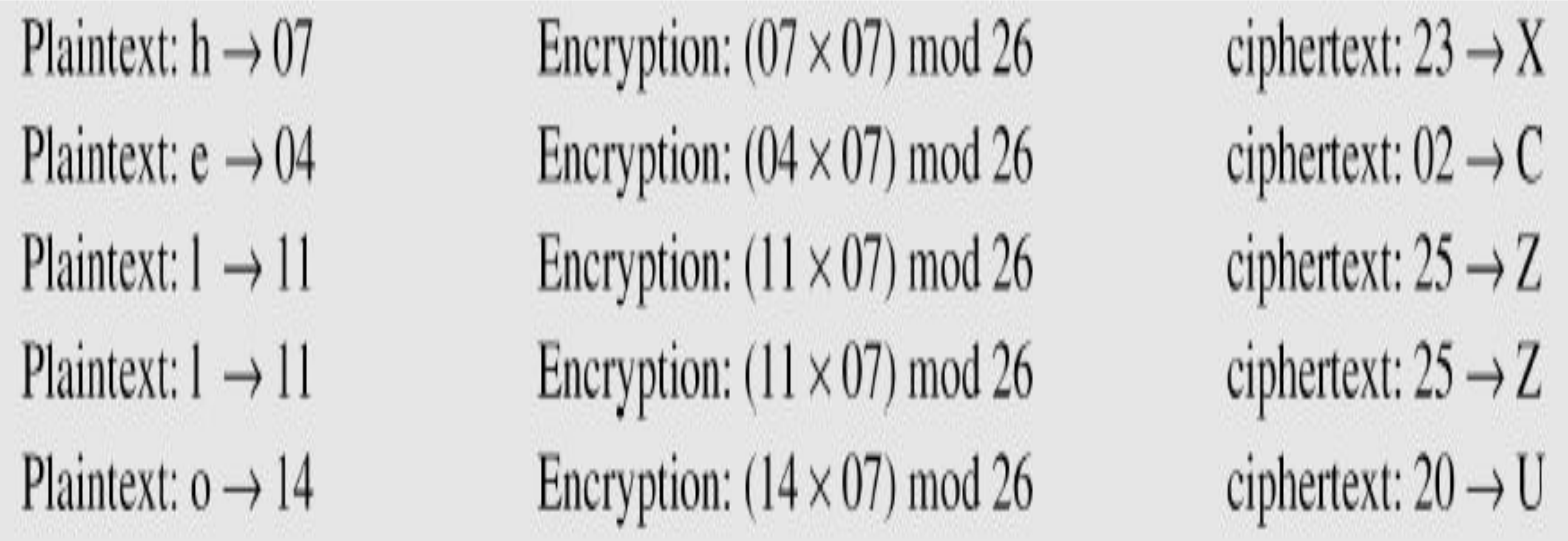


0	1	2	3	4	5	6	7	8	9	10	11	12
A	B	C	D	E	F	G	H	I	J	K	L	M
13	14	15	16	17	18	19	20	21	22	23	24	25
N	O	P	Q	R	S	T	U	V	W	X	Y	Z

Example

- Example: - We use a multiplicative cipher to encrypt the message “hello” with a key of 7. The ciphertext is “XCZZU”.

Encryption



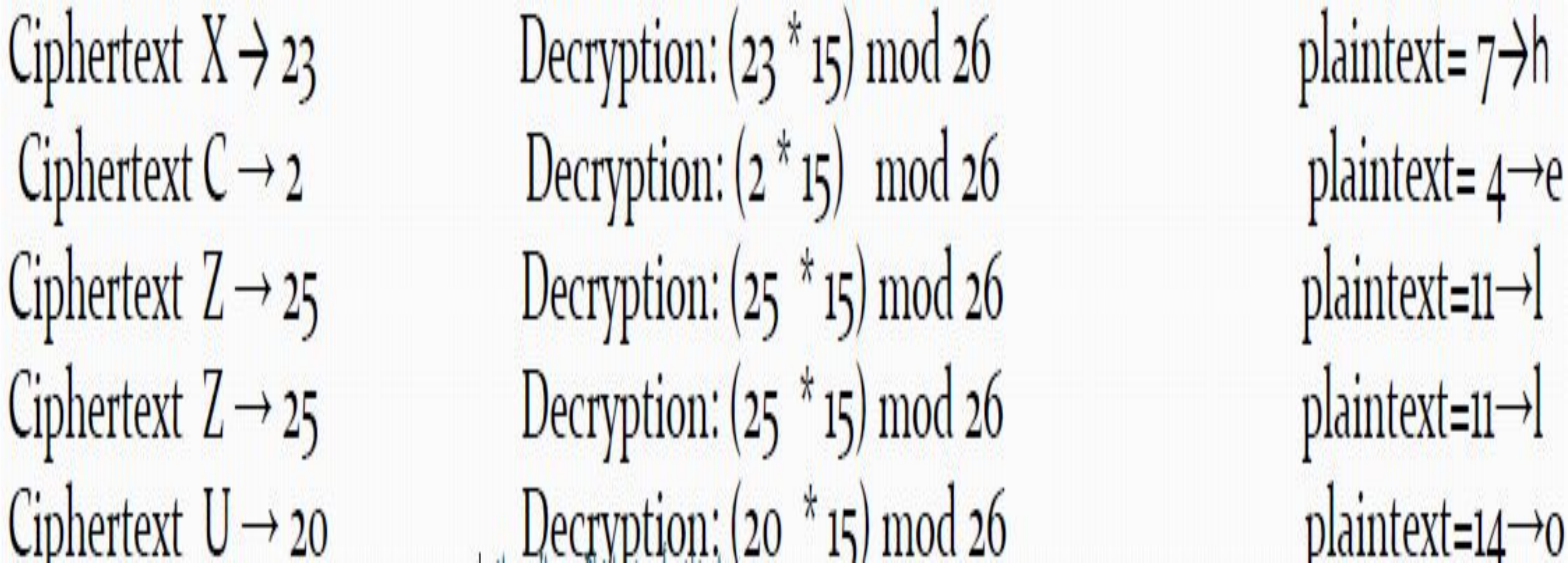
Plaintext: h → 07	Encryption: $(07 \times 07) \bmod 26$	ciphertext: 23 → X
Plaintext: e → 04	Encryption: $(04 \times 07) \bmod 26$	ciphertext: 02 → C
Plaintext: l → 11	Encryption: $(11 \times 07) \bmod 26$	ciphertext: 25 → Z
Plaintext: l → 11	Encryption: $(11 \times 07) \bmod 26$	ciphertext: 25 → Z
Plaintext: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

The ciphertext is “XCZZU

Decryption

- Cryptanalyses of the multiplicative cipher based on finding the multiplication
- inverse of the key (where the multiplication inverse of **7 is 15**) as shown

Decryption



Ciphertext X → 23	Decryption: (23 * 15) mod 26	plaintext= 7→h
Ciphertext C → 2	Decryption: (2 * 15) mod 26	plaintext= 4→e
Ciphertext Z → 25	Decryption: (25 * 15) mod 26	plaintext=11→l
Ciphertext Z → 25	Decryption: (25 * 15) mod 26	plaintext=11→l
Ciphertext U → 20	Decryption: (20 * 15) mod 26	plaintext=14→o

GCD

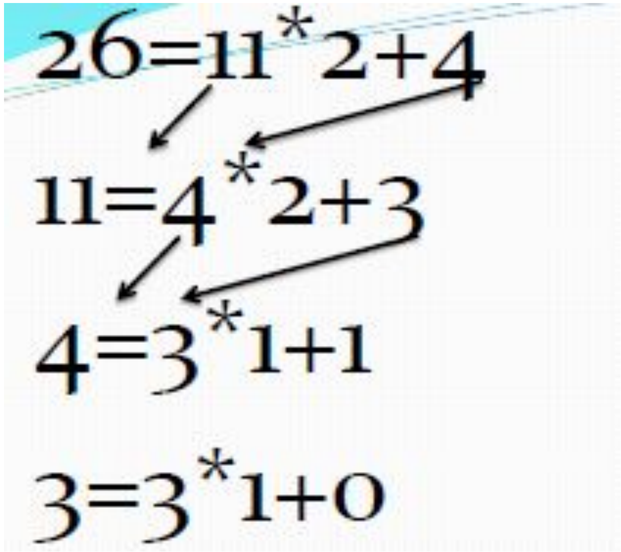
- we can find the inverse based on using the equation
- The GCD(26,11)must be 1 in order to find the inverse
- a=q b+r
- q=a/b
- r= a- q b

Example:

- Example: - Find the multiplicative inverse of 11 in N=26

$r = a - q^* b$

- **GCD**



26=11*2+4

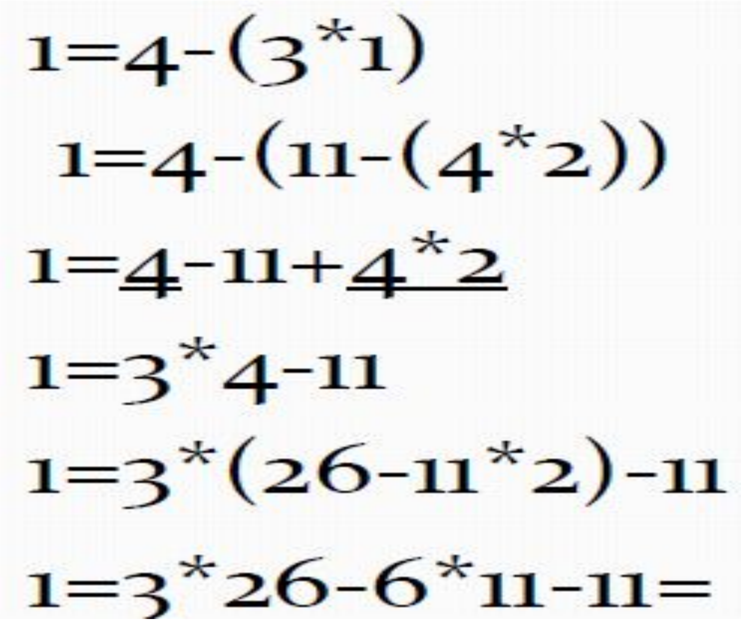
11=4*2+3

4=3*1+1

3=3*1+0

inverse

- We are now in reverse compensation starting from one as shown



$$1=4-(3*1)$$

$$1=4-(11-(4*2))$$

$$1=\underline{4}-11+\underline{4*2}$$

$$1=3*4-11$$

$$1=3*(26-11*2)-11$$

$$1=3*26-6*11-11=$$

- so the multiplicative inverse of 11 is -7

شكرا لكم