



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



Fourth Stage

***Security
Lab.***

Lecture 10

Asst. Lec. Yousif Samer Mudhafar

Email: yousif.samir19@gmail.com

Lecture objective

The student will recognize the following objective :

- **Multiplicative modulo inverse for any number.**

Example

Write a program in MATLAB to find the **inverse** of the **key** for **any number**.

Inverse key equation



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

Inverse key Code

```
clc, clear
```

```
k=input('Enter the Key: ');
```

```
m=input('Enter the modulo number: ');
```

```
if gcd(k,m)~=1
```

```
    disp(['Multiplicative inverse is not found'])
```

```
else
```

```
    for i=1:m
```

```
        if mod(k*i,m)==1
```

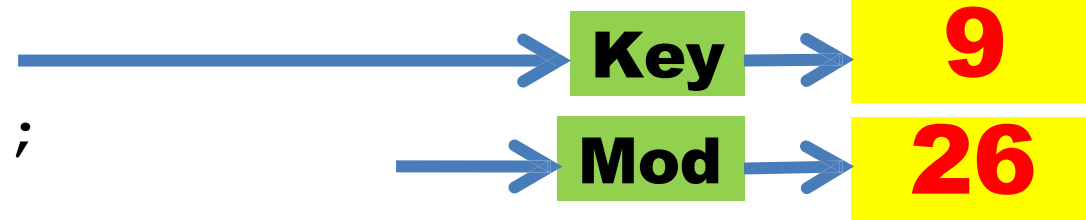
```
            kk=i;
```

```
        end
```

```
    end
```

```
    disp(['Multiplicative inverse is ' num2str(kk)])
```

```
end
```



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

Result

The Result of the **key inverse** for **9** is

3

Homework

By using **Multiplicative Cipher**, Decrypt the message **“GQKKINYGAFYQNC”** with the **Key 3** and the **inverse** of the key must be programmed **automatically**.