جامـــعـة المـــسـتـقـبـل
AL MUSTAQBAL UNIVERSITY

قســـــــم الأمـــــــــــن
الـــــــــــــــســيبرانــــــــــــــي

Department of Cyber Security

Subject:

Principles of Cyber Security

Class:

First

Lecturer:

MSC .Najwan thaeer ali

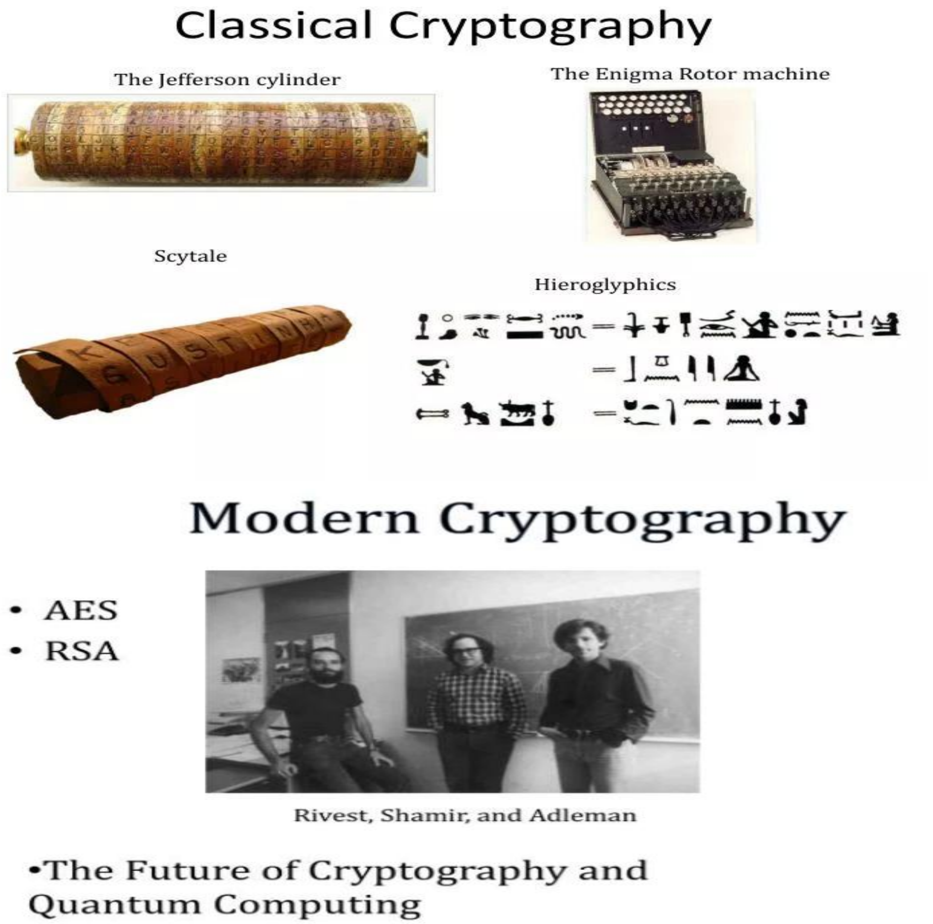
Lecture: final

Classical Encryption Methods in Cryptography

1-Traditional encryption methods

Introduction

- Encryption is the science of securing information and protecting it from unauthorized access. Before the advent of computers, ancient civilizations used various methods to encrypt messages, such as the Caesar cipher used by the Romans and the Scytale cipher used by the Greeks.



Classical Cryptography

The Jefferson cylinder

The Enigma Rotor machine

Scytale

Hieroglyphics

Modern Cryptography

- AES
- RSA

Rivest, Shamir, and Adleman

•The Future of Cryptography and Quantum Computing

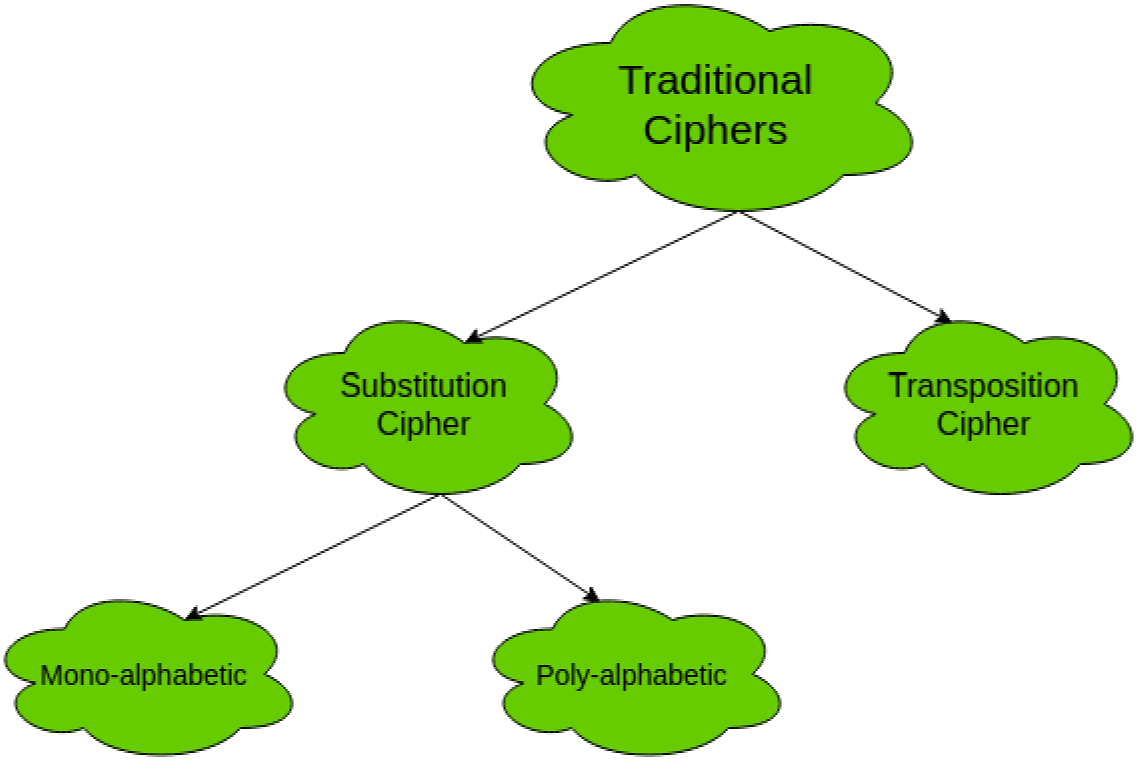
- Traditional encryption is primarily based on substitution (replacing letters with others) or transposition (rearranging letters), making the text unreadable without the correct key.

- Although these methods were effective in the past, the rise of computers made them vulnerable to frequency analysis and computational attacks. This led to the development of modern encryption techniques, such as symmetric-key encryption and public-key encryption, to secure digital data.

Some of the most well-known traditional encryption techniques include:

Traditional Symmetric Ciphers The two types of traditional symmetric ciphers are **Substitution Cipher** and **Transposition Cipher**. The following

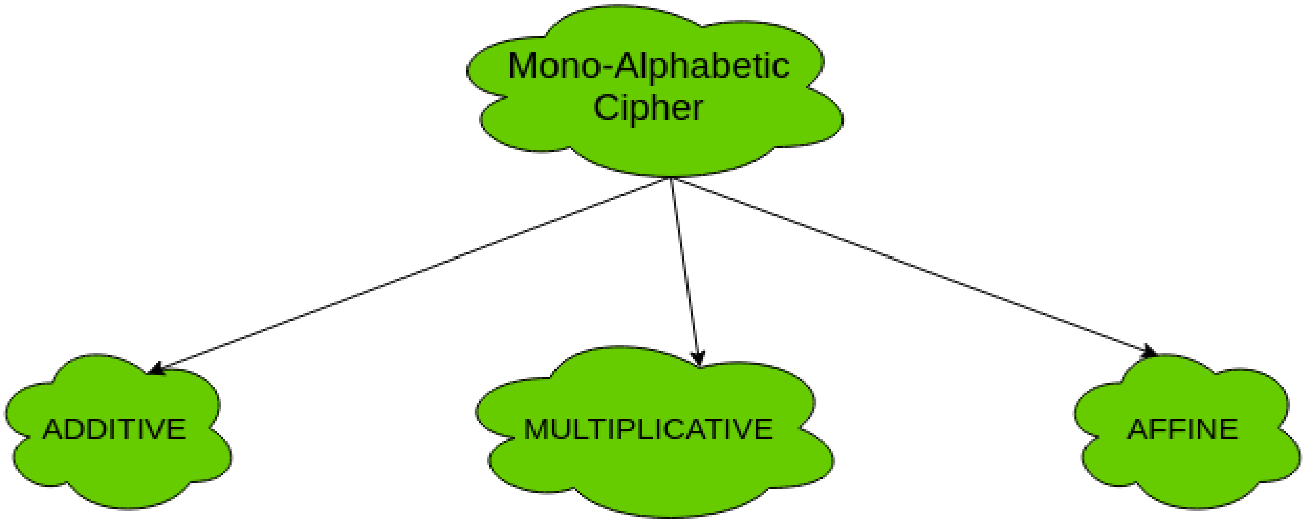
flowchart categories **TRADITIONAL CIPHERS:**



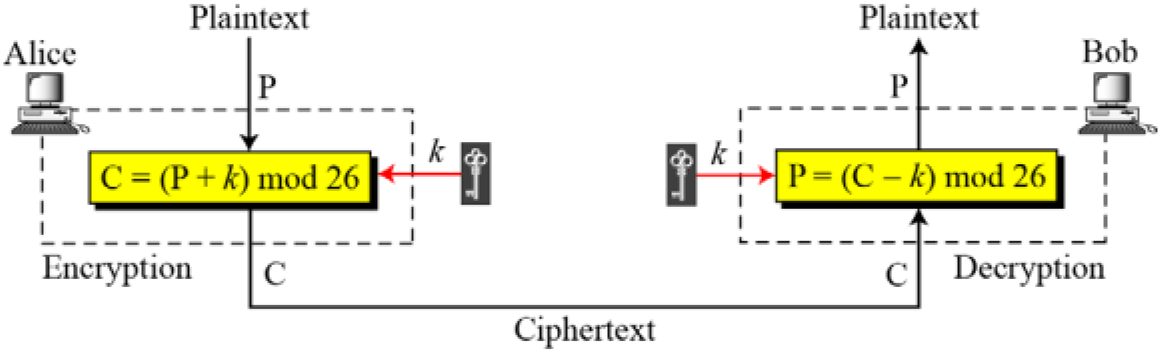
1. Substitution Cipher: Substitution Ciphers are further divided into **Mono-alphabetic Cipher** and **Poly-alphabetic Cipher**. First, let's study about mono-alphabetic cipher.

1. **Mono-alphabetic Cipher -** In mono-alphabetic ciphers, each symbol in plain-text (eg; 'o' in 'follow') is mapped to one cipher-text symbol. No matter how many times a symbol occurs in the plain-text, it will correspond to the same cipher-text symbol. For example, if the plain-text is 'follow' and the mapping is :
   - f -> g
   - o -> p
   - l -> m
   - w -> x

The cipher-text is 'gpmmpx'. Types of mono-alphabetic ciphers are:



1. **Additive Cipher (Shift Cipher / Caesar Cipher) -** The simplest mono-alphabetic cipher is additive cipher. It is also referred to as 'Shift Cipher' or 'Caesar Cipher'. As the name suggests, 'addition modulus 2' operation is performed on the plain-text to obtain a cipher-text. C = (M + k) mod n M = (C - k) mod n where, C -> cipher-text M -> message/plain-text k -> key The key space is 26. Thus, it is not very secure. It can be broken by brute-force attack



2. **Multiplicative Cipher -** The multiplicative cipher is similar to additive cipher except the fact that the key bit is multiplied to the plain-text symbol during encryption. Likewise, the cipher-text is multiplied by the multiplicative inverse of key for decryption to obtain back the plain-text. C = (M * k) mod n . Thus, it is also not very secure.

3. **Affine Cipher -** The affine cipher is a combination of additive cipher and multiplicative cipher.

- **$k_1 = 5$**
- **$k_2 = 8$**
- الترميز الأبجدي:

```
A = 0, B = 1, ..., H = 7, ..., Z = 25
```

H=7

$$\text{mod } 26 \quad ({}_2k + {}_1k \times M) = C$$

$$\text{mod } 26 \quad (8 + 5 \times 7) = C$$

$$\text{mod } 26 \quad (8 + 35) = C$$

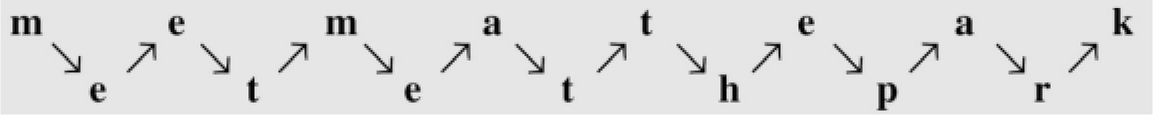
$$\text{mod } 26 \quad 43 = C$$

$$17 = C$$

4. **Poly-alphabetic Cipher -** In poly-alphabetic ciphers, every symbol in plain-text is mapped to a different cipher-text symbol regardless of its occurrence. Every different occurrence of a symbol has different mapping to a cipher-text. For example, in the plain-text 'follow', the mapping is : f -> q, o -> w ,l -> e, l -> r, o -> t, w -> y Thus, the ciphtexis 'qwerty'. Types of poly-alphabetic ciphers are:

Transposition Ciphers A transposition cipher does not substitute one symbol for another, instead it changes the location of the symbols. A transposition cipher reorders symbols.

Example A good example of a keyless cipher using the first method is the rail fence cipher. The cipher text is created reading the pattern row by row. For example, to send the message —**Meet me at the park** to Bob, Alice writes



She then creates the cipher text —**MEMATEAKETETHPR**.

Column Transposition Cipher is a type of encryption that relies on changing only the positions of the letters, without changing the letters themselves. That is, all the letters of the original text remain, but their order is changed according to a specific rule.
In this type of encryption, we use a key. The length of the key determines the number of columns in which we will write the original text. We begin by writing the original text letter by letter in rows, from left to right, under the key letters .After finishing writing the text, we arrange the columns of the table according to the alphabetical order of the key letters. That is, we look at the key letters and determine which letter comes first in the alphabet, then the next, and so on.After rearranging the columns, we read the

letters column by column from top to bottom, in the new column order. The resulting letters form the ciphertext.

key : Z E B R A

5 3 2 4 1

Plaintext: WEAREDISCOVERED

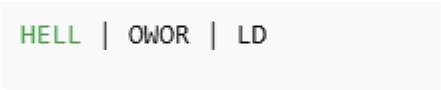
A B E R Z	Z E B R A
1 2 3 4 5	53241
E A E R W	WEARE
O S I C D	DISCO
D R E E V	VERED
EOD ASR EIE RCE WDV دمجها بدون فراغات EODASREIERCEWDV	ترتيب الحروف حسب الارقام

Fixed Period Transposition Cipher (PPT) is a type of encryption that relies on rearranging letters without altering their order. Each letter of the original text remains present in the ciphertext, but in a different position. The term "Fixed Period" refers to the fact that the text is divided into small groups of a fixed number of letters, called the .ciphertext

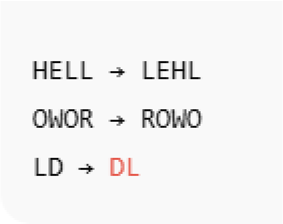
The process works as follows: First, we choose the length of the period, which is the number of letters in each group. Then, we divide the original text into groups of equal length. Next, we apply a specific order to the letters within each group, such as reversing the order of the letters or swapping certain positions within the group. Finally, we read the .letters after arranging all the groups together to form the final ciphertext

One advantage of this type of encryption is that it preserves the same letters and does not increase the length of the text, but it hides the original order, making the text more difficult to understand when viewed .directly

HELLOWORLD
4=PERIOD



```
HELL | OWOR | LD
```



```
HELL → LEHL
OWOR → ROWO
LD → DL
```

LEHLROWODL