Al-Mustaqbal University
College of Sciences
Intelligent Medical System Department

جامـــــعة المـــــستـقبـل
AL MUSTAQBAL UNIVERSITY

كلية العلوم

قســـم الانظمة الطبية الذكية

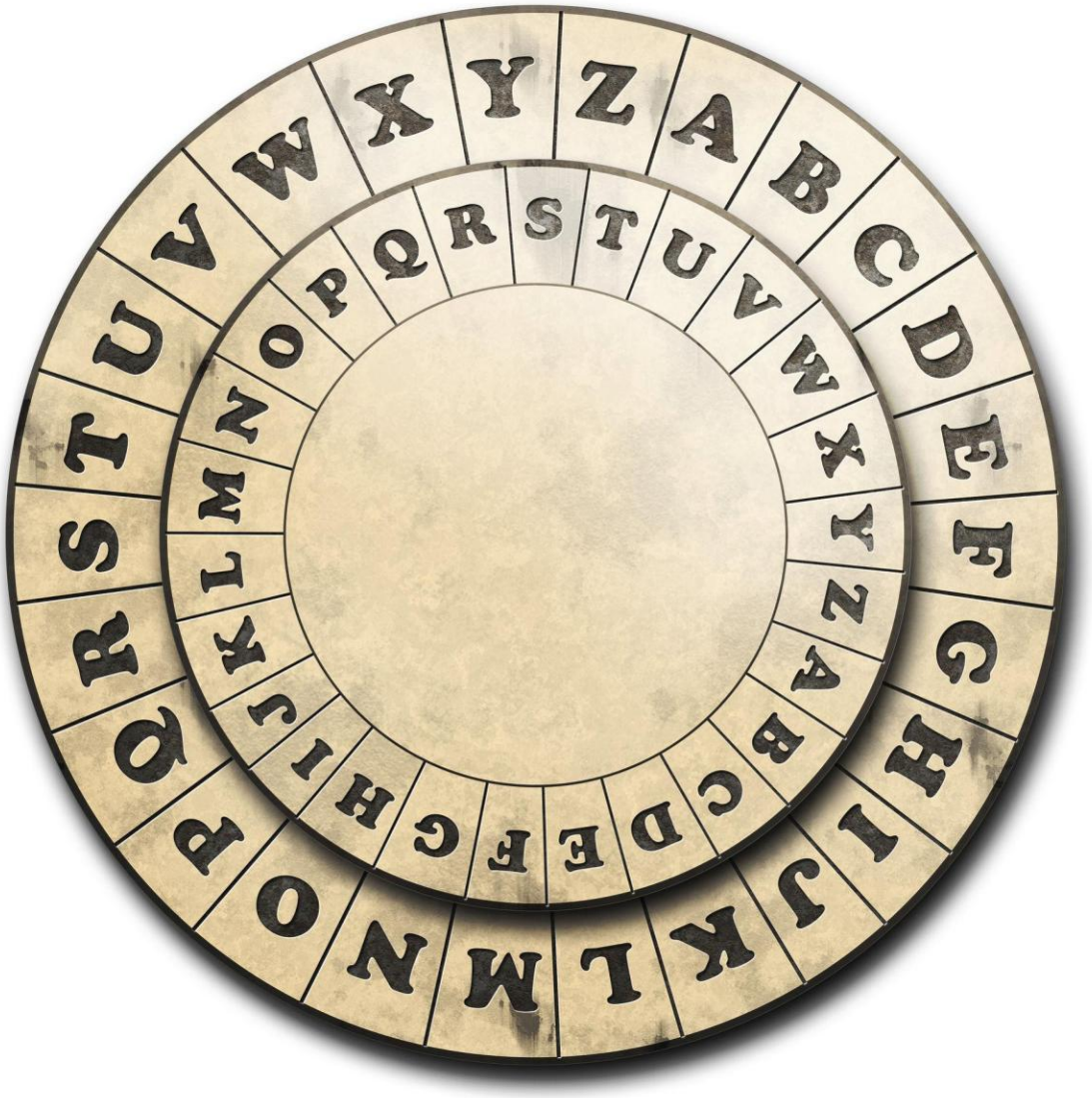
Lecture for Ceaser Encryption Lab

Information Security in Healthcare

Subject: Caesar Encryption
Level: Fourth
Lecturer: Prof. Dr. Mehdi Ebady Manaa

المحاضرة رقم 1

برنامج شفرة قيصر(Caesar Cipher)



أولاً: التعريف

شفرة قيصر (Caesar Cipher) هي واحدة من أقدم تقنيات التشفير في علم التشفير الكلاسيكي (Classical Cryptography). تعتمد على مبدأ بسيط يسمى **الإزاحة(Shift)** ، حيث يتم استبدال كل حرف بحرف آخر يقع بعده بعدد ثابت من المواضع في الأبجدية.

سميت بهذا الاسم نسبة إلى **يوليوس قيصر (Julius Caesar)** الذي استخدمها لإرسال رسائل عسكرية سرية.

ثانياً: المبدأ الرياضي

إذا رمزنا إلى:

- الحرف الأصلي(Plaintext) (P) :
- الحرف المشفر(Ciphertext) (C) :
- مقدار الإزاحة(k) :
- عدد أحرف الأبجدية الإنجليزية(26) :

فإن معادلة التشفير هي:

$$C = (P + k) \bmod 26$$

ومعادلة فك التشفير:

$$P = (C - k) \bmod 26$$

ثالثاً: مثال عملي

نفترض:

- النص الأصلي:

```
HELLO
```

- مقدار الإزاحة:

```
k = 3
```

النتيجة:

الحرف الأصلي	الحرف المشفر
H	K
E	H
L	O
L	O
O	R

النص المشفر:

KHOOR

رابعاً: برنامج بسيط بلغةPython

```
def caesar_encrypt(text, shift):
    result = ""
    ABCa@##
    DEFd@##
3
    for char in text:
        if char.isalpha(): هذه الدالة تختبر فقط الحروف
            if char.isupper():
                result += chr((ord(char) - 65 + shift) % 26 + 65)
            else:
                result += chr((ord(char) - 97 + shift) % 26 + 97)
        else:
            result += char

    return result

def caesar_decrypt(text, shift):
    return caesar_encrypt(text, -shift)


# مثال
plain = "HELLO"
shift = 3

encrypted = caesar_encrypt(plain, shift)
decrypted = caesar_decrypt(encrypted, shift)

print("Original:", plain)
print("Encrypted:", encrypted)
print("Decrypted:", decrypted)
```

الناتج:

```
Original: HELLO
Encrypted: KHOOR
```

```
Decrypted: HELLO
```

خامساً: الخصائص الأمنية

المميزات

- بسيط جداً وسهل التنفيذ
- مناسب للتعليم وفهم أساسيات التشفير

العيوب

- ضعيف جداً أمنياً
- يمكن كسره باستخدام **Brute Force Attack**
- عدد المفاتيح الممكنة فقط 25

سادساً: استخداماته التعليمية الحديثة

يستخدم في تدريس:

- أساسيات علم التشفير Cryptography
- أمن المعلومات Cybersecurity
- مفاهيم:
  - Encryption
  - Decryption
  - Keys
  - Attack Models

سابعاً: مثال عربي توضيحي

إذا استخدمنا إزاحة 1:

```
ABC → BCD
XYZ → YZA
```

ثامناً: تطبيق عملي في الأمن السيبراني

شفرة قيصر تمثل نموذجاً لما يسمى:

Substitution Cipher

وهي الأساس الذي تطورت منه خوارزميات حديثة مثل:

- AES

- RSA
- DES

Khoor; Krz duh brx !!!!!!!

توزيع شفرة قيصير على صفوف وافرض عدد الصفوف هي 3

K r

h o

o

Cipher = row= 3

Cipher = Krhoo