الجامعة المستنصرية-كلية العلوم- قسم علوم الحاسوب- فرع الأمن السيبراني- الامتحان الأول- الأحد الموافق 2023-03-26

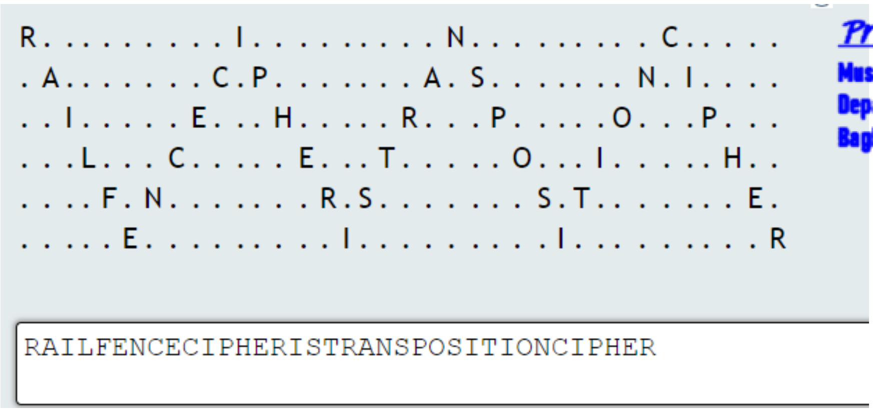
الاسم الثلاثي:

**Q1) ANSWER THE FOLLOWING QUESTION:**

**a) Use Rail Fence with KEY=6 to decrypts the cipher-text="RINCACPASNIIEHRPOPLCETOIHFNRSSTEEIIR".**

**b) Which type of cryptography is Rail-Fence?**

**ANSWER:**



```
R . . . . . . . . . I . . . . . . . . . N . . . . . . . . . C . . . . .
. A . . . . . . . C . P . . . . . . . A . S . . . . . . . N . I . . . .
. . I . . . . . E . . . H . . . . . R . . . P . . . . . O . . . P . . .
. . . L . . . C . . . . . E . . . T . . . . . O . . . I . . . . . H . .
. . . . F . N . . . . . . . R . S . . . . . . . S . T . . . . . . . E .
. . . . . E . . . . . . . . . I . . . . . . . . . I . . . . . . . . . R
```

RAILFENCECIPHERISTRANSPOSITIONCIPHER

*Professor Dr. Bashar M. Nema*

**Mustansiriyah University-College of Science,**
**Department of CS,**
**Baghdad, IRAQ.**

✓

**The plain-text= "RAIL FENCE CIPHER IS TRANSPOSITION CIPHER"**

**Q2) Define the Public key cryptography? Describe the Advantages and Disadvantages of It? What are Practical application of It?**

Answer:

Public key cryptography is a cryptographic system that enables secure communication between two parties without the need for a shared secret key. Instead, the system uses two mathematically related keys: a public key and a private key. These keys are used to encrypt and decrypt messages in such a way that only the intended recipient can read the message.

**Advantages:**

- Provides a secure means of communication without the need for a shared secret key.
- Enables digital signatures, which can be used to ensure the authenticity and integrity of a message.

**Disadvantages:**

- Computationally intensive, which means that it can be ***slower than*** symmetric key cryptography.
- Vulnerable to attacks such as brute force attacks and man-in-the-middle attacks.

**Practical Applications:**

1) **Secure communication** over the internet: HTTPS, the protocol used to secure web traffic, uses public key cryptography to ensure the confidentiality and integrity of data sent between a web server and a client.
2) **Digital signatures**: used to ensure the authenticity and integrity of electronic documents.

**Q3) Use RSA to generate Public and Private keys where P= 11 and Q=13?**
**ANSWER:**

## TO GENERATE THE PUBLIC AND PRIVATE KEYS USING THE RSA ALGORITHM, WE NEED TO FOLLOW THESE STEPS:

1) Choose two distinct **prime** numbers, let's say P=11 and Q=13.
2) Compute N = P * Q. In this case, N=11*13=143.
3) Compute φ(N) = (P-1) * (Q-1). In this case, φ(143) = (11-1) * (13-1) = 120.
4) Choose an integer **e** as public key, such that:
   a. **1 < e < φ(N)** and,
   b. **gcd(e, φ(N)) = 1**. In this case, we can choose e=7.
5) Compute the private key **d** such that:
   a. (d * e) mod φ(N) = 1.
   b. In this case, we need to find d such that (d * 7) mod 120 = 1.
   **One possible solution is d=103**.
6) The **public key** is (N, e), which in this case is (143, 7).
7) The **private key** is (N, d), which in this case is (143, 103).
8) Therefore, the public key is (143, 7) and the private key is (143, 103).

**Q4) Answer the following questions:**

A. **What is Authentication?**
B. **What are types of Authentications?**
C. **What is 2FA?**
D. **Benefits of Digital Signatures:**

**ANSWER:**
**AUTHENTICATION:**

Authentication is the process of verifying the identity of a user, device, or application. It is the first line of defense against unauthorized access to a system, network, or data.

**There are three types of authentication:**

- **Something you know:** This type of authentication requires the user to enter a password, PIN, or some other secret information that only they know.
- **Something you have:** This type of authentication involves a physical object such as a smart card, token, or a mobile device that contains a unique identifier.
- **Something you are:** This type of authentication involves biometric identification such as fingerprints, facial recognition, or iris scans.

## TWO-FACTOR AUTHENTICATION:

**Two-factor authentication (2FA)** is a security measure that requires two different forms of authentication in order to grant access to a system or service. Typically, this involves something the user knows, such as a password, and something the user possesses, such as a smartphone or hardware token.

**BENEFITS OF DIGITAL SIGNATURES:**

Digital signatures offer several benefits over traditional signatures:

1) Security: Digital signatures use cryptography to ensure that the signature is secure and cannot be tampered with.
2) Efficiency: Digital signatures can be created and verified quickly and easily.
3) Non-repudiation: Digital signatures provide non-repudiation, which means that the sender cannot deny having signed the document.
4) Cost Savings: Digital signatures eliminate the need for paper-based signatures and reduce the cost of printing, scanning, and shipping documents.