 a. Discuss how cryptography achieves different security services [4 Marks]

* **Confidentiality**: Ensured through encryption, where data is transformed into an unreadable format for unauthorized users.
* **Integrity**: Achieved by using hash functions and message authentication codes (MACs). These ensure that the data has not been altered in transit or storage by generating a unique value that changes if any alteration occurs.
* **Authentication**: Verifies the identity of the sender or recipient using digital signatures or certificates.
* **Non-repudiation**: Prevents an entity from denying the authenticity of their signature or the transmission of a message.

b. Discuss the Strengths and weaknesses of  Single Sign On (SSO) [authentication](https://elearning.kisiiuniversity.ac.ke/mod/resource/view.php?id=35370) technique [4 Marks]

**Strengths of Single Sign-On (SSO) Authentication:**

* **Convenience**: SSO allows users to access multiple applications or services with a single set of credentials, reducing the need to remember numerous usernames and passwords.
* **Improved User Experience**: Users can seamlessly transition between applications without needing to log in repeatedly, enhancing productivity and satisfaction.

**Weaknesses of Single Sign-On (SSO) Authentication:**

* **Increased Target for Attackers**: Since all applications rely on a single authentication system, compromising the SSO credentials can give attackers access to multiple services, increasing the risk.
* **Complexity in Implementation**: Implementing and maintaining an SSO solution can be complex, especially in environments with legacy systems or multiple applications requiring integration.

c.  Describe four possible attacks that can be perpetuated on a system and its resources in the context of communication across a network [4 Marks]

**Denial of Service (DoS) Attack**: In a DoS attack, the attacker overwhelms a network or server with excessive traffic or requests, making it unavailable to legitimate users.

**Phishing Attack**: Phishing involves tricking users into revealing sensitive information (e.g., usernames, passwords, credit card numbers) by posting as a trusted entity via email, websites, or other forms of communication.  
**Man-in-the-Middle Attack**: in Man-in-the-Middle attack, the attacker intercepts and potentially alters communication between two parties (e.g., a user and a server) without their knowledge.

**Session Hijacking**: In a session hijacking attack, the attacker steals a valid session token (usually after successfully intercepting network traffic) and impersonates the legitimate user.

d. Discuss the different tasks performed by an [access control](https://elearning.kisiiuniversity.ac.ke/mod/resource/view.php?id=35371) system in preventing a system from unauthorized access and unauthorized modification of data [6 Marks]

1. **Authentication**:

* **Purpose**: Verifies the identity of a user or entity trying to access the system.
* **How it Works**: The ACS ensures that only legitimate users can access the system by checking credentials (e.g., usernames, passwords, biometric data, or tokens) against stored information. This step ensures that only authorized individuals can gain access to the system, preventing unauthorized entry.

2. **Authorization**:

* **Purpose**: Determines what resources and actions an authenticated user is allowed to access or perform.
* **How it Works**: Once a user’s identity is verified, the ACS checks the user’s permissions (often stored in an access control list or role-based access control system) to determine what resources they are allowed to interact with (e.g., files, applications, or databases). This ensures that users cannot access or modify data or systems they are not permitted to.

3. **Access Control Policies**:

* **Purpose**: Defines the rules and policies that determine who can access what, under which conditions, and what actions they are allowed to perform.
* **How it Works**: The Access Control Policies enforces predefined policies based on factors like role-based access, least privilege, and need-to-know principles. For example, a policy might allow only administrators to modify system configurations while restricting regular users to read-only access.

e. Use rail fence method of depth 3 to encrypt the following message [2 marks]

         THE MEETING HAS BEEN POSTPONED TO A LATER DATE WHICH WILL BE COMMUNICATED

-Remove spaces and prepare the message.

**THEMEETINGHASBEENPOSTPONEDTOALATERDATEWHICHWILLBECOMMUNICATED**

-Write the message in zig-zag pattern

**Rail 1**: T       E       T       H       S       E       O       N       D       T       A       T       E       H       W       H       W       L       E       C       M       N       C       A

**Rail 2**:

 H   M   I   G   H   A   B   E   N   P   O   E   T   L   A   E   D   T   A   W   I   I   B   O   I   T   E   D

**Rail 3**:

   E       I       N       G       A       S       P       T       O       N       O       L       R       A       D       W       C       L       M       U       E       T

-Combine the rails

**Rail 1**: TETHSEONDTATEHWHWLECMNC  
**Rail 2**: HMIGHABENPOETLADTAWIIBOITED  
**Rail 3**: EINGASPTONOLRADWCLEMUET

-The final encryption message

The final encrypted message after combining the three rails is:

**TETHSEONDTATEHWHWLECMNC HMIGHABENPOETLADTAWIIBOITED EINGASPTONOLRADWCLEMUET**

f.  Using the key word “EXPATRIATE”, convert the following plain text messages to cipher text using plain fair cipher encryption technique [4 Marks]

                                     COME BACK YOU ARE URGENTLY NEEDED IN THE OFFICE

**Step 1**: Construct the Playfair Matrix

The matrix is formed by using the keyword **EXPATRIATE** (removing duplicate letters) and filling in the remaining letters of the alphabet (excluding 'J'):

E X P A T

R I B C D

F G H K L

M N O Q S

U V W Y Z

**Step 2**: Prepare the Plaintext

Remove spaces and split the message into digraphs (pairs of letters): **"COMEBACKYOUAREURGENTLYNEEDEDINTHEOFFICE"** →CO ME BA CK YO UA RE UR GE NT LY NE ED IN TH EO FF IC EX

**Step 3**: Encrypt the Digraphs

Use the Playfair rules to encrypt each digraph:

* **CO** → **RO**
* **ME** → **ME**
* **BA** → **RA**
* **CK** → **DK**
* **YO** → **VS**
* **UA** → **PA**
* **RE** → **TI**
* **UR** → **VR**
* **GE** → **FE**
* **NT** → **NT**
* **LY** → **YL**
* **NE** → **NE**
* **ED** → **CD**
* **IN** → **IN**
* **TH** → **TH**
* **EO** → **EO**
* **FF** → **FF**
* **IC** → **CI**
* **EX** → **PX**

**Step 4**: Final Ciphertext

The final ciphertext is:

**RO ME RA DK VS PA TI VR FE NT YL NE CD IN TH EO FF CI PX**

g. Describe different techniques to put in place to guarantee that systems and system resources are protected from intruder attacks [6 Marks]

* **Firewalls**: They block unauthorized access by filtering incoming and outgoing network traffic.
* **Intrusion Detection and Prevention Systems (IDPS)**: They monitor for suspicious activities and can prevent attacks in real-time.
* **Encryption**: Encrypts data to protect it from being read if intercepted by unauthorized users.
* **Access Control**: Restricts access to resources based on user roles and permissions, minimizing exposure.
* **Software Updates and Patching**: Ensures vulnerabilities are fixed regularly to prevent exploitation by attackers.
* **Multi-Factor Authentication (MFA)**: Adds an extra layer of security, requiring multiple forms of identification to access systems.