In HIS name

Instructor : Vahid Amin-Ghafari
Ali Sheikh Attar

Cryptography - HW2

➔ **Q1. Define Threats, Vulnerabilities, and Controls**

- **Threats**: A threat is any potential negative action or event that can cause damage or harm to information assets. This could include unauthorized access, destruction, modification, or disclosure of data.
- **Vulnerabilities**: Vulnerabilities are weaknesses in a system, network, or organization that can be exploited by threats. For example, a software bug, lack of security measures, or unprotected communication lines can be considered vulnerabilities.
- **Controls**: Controls are measures taken to reduce or eliminate vulnerabilities. They include actions, devices, procedures, or techniques used to protect a system from threats.

➔ **Q2. What are the types of Threats?**

- **Interception**: Unauthorized parties gaining access to an asset, such as wiretapping or copying data files.
- **Interruption**: Loss or unavailability of assets, like malicious destruction of hardware or denial-of-service (DoS) attacks.
- **Modification**: Unauthorized changes to assets, such as altering values in a database.
- **Fabrication**: Creation of fake objects or data, such as inserting false transactions into a network.

➔ **Q3. What are the methods of defense from Threats?**

Methods to defend against threats are often classified as:

- **System Access Controls**: Ensuring that unauthorized users cannot access the system.
- **Data Access Controls**: Monitoring and controlling who can access which data and for what purpose.

- **System and Security Administration**: Managing system security through proper user training, administrator responsibilities, and offline procedures.
- **System Design**: Using security features inherent to hardware and software.
- **Encryption**: Providing confidentiality and integrity to data and communication.

➔ **Q4. What questions should you ask when determining threats?**

When assessing potential threats to a system, you should consider the following:

- **Who are the potential attackers?** (Who might want to harm the system, such as hackers, insiders, or competitors?)
- **What methods or tools could they use?** (Could they use malware, social engineering, or physical access to attack the system?)
- **What are the motivations of the attackers?** (Are they seeking financial gain, political motives, or causing harm for personal reasons?)
- **What are the possible points of entry or vulnerabilities in the system?** (Are there software bugs, unprotected networks, or weak passwords that attackers could exploit?)
- **What is the potential impact of the attack?** (How much damage could the attack cause to data, services, or system operations?)
- **What countermeasures or controls are already in place?** (Are there sufficient protections to mitigate the identified threats?).

➔ **Q5. What is vulnerability, threat, and control?**

- **Vulnerability**: A weakness or flaw in a system, network, or process that can be exploited by a threat. Examples include software bugs, inadequate physical security, or poor password policies.
- **Threat**: A potential event or action that could cause harm or damage to an organization's information assets. Threats may include hackers, natural disasters, or system failures.
- **Control**: A measure taken to reduce or eliminate vulnerabilities and protect against threats. Controls can be physical (e.g., locks, alarms), technical (e.g., firewalls, encryption), or administrative (e.g., security policies, training).