In HIS name

Instructor : Vahid Amin-Ghafari
Ali Sheikh Attar

Cryptography - HW1

→ **Q1. What are the three basic principles of information security? Define each one**

- **Confidentiality**: Ensures that information is accessible only by authorized individuals or systems. It is sometimes referred to as privacy or secrecy.
- **Integrity**: Ensures that information is accurate and unaltered. Only authorized users can make changes in authorized ways.
- **Availability**: Ensures that information and systems are accessible to authorized users when required, without unnecessary delays.

→ **Q2. Give examples for confidentiality without integrity, integrity without confidentiality, and when availability is the primary concern**

- **Confidentiality without Integrity**: A hospital patient's health record needs to remain confidential, even if the exact accuracy of certain details is not vital in some cases.
- **Integrity without Confidentiality**: In voting systems, the integrity of vote counting is critical, but the vote counts may be public once aggregated.
- **Availability as the Overriding Concern**: Emergency response systems, such as 911 services, must be available at all times regardless of confidentiality or integrity concerns.

→ **Q3. From a bank's perspective, which is usually more important, the integrity or confidentiality of its customer's data?**

- For a **bank**, the **integrity** of customer data is typically more important because errors or unauthorized changes could lead to financial loss.
- From the **customer's perspective**, **confidentiality** might be more important as they expect their personal financial details to be kept private.

➔ **Q4. Explain the difference between secrecy, privacy, and confidentiality, and provide examples**

● **Secrecy**: The concept of keeping information hidden. It is akin to confidentiality in general.
    ○ Example: A military operation's details being kept secret.
● **Privacy**: Secrecy applied to personal information.
    ○ Example: An individual's medical history needs to remain private.
● **Confidentiality**: An obligation not to disclose certain information.
    ○ Example: A lawyer keeping client conversations confidential.

➔ **Q5. What is the difference between confidentiality and privacy?**

● **Confidentiality** is the act of protecting information from unauthorized access, while **privacy** is more about protecting personal information from being shared without consent.