INFORMATION SECURITY

NAME: HAMZA MANSOOR RAJPUT
ROLL NO: B-25859

ASSIGNMENT NO. 1

Q: Discuss the Key concepts of information security, including design principles, cryptography..?

ANS: Key concepts of information security:

1) Design Principles:
These are foundational guidelines that help create secure information systems. They ensure that security is built into the architecture of systems rather than added later.

2) Cryptography:
This is the practice of securing information by transforming it into an unreadable format for unauthorized users. It plays a vital role in protecting data confidentiality, integrity and authenticity.

3) Risk Management:
This involves identifying, assessing and prioritizing risks followed by coordinated

effoets to minimize, monitor and control the probability or impact of unfortunate events. Effective risk management helps protect assets and ensure compilance with regulations.

Fundamental Design Principles:

1) Least Privilege:
This principle states that users should have only the access necessary to perform their tasks, By minimizing access rights, the potential for unauthorized actions is reduced.

2) Defense in Depth:
This approach layers multiple security measures to protect information. If one layer fails, others are still in place to prevent unauthorized access.

3) Fail-Safe Defaults:
Systems should default to a secure state unless explicitly configured otherwise. This means that if a system fails, it should deny access rather than allowing it.

Role of Cryptography:

Cryptography protects information through techniques such as encryption, which converts readable data into a coded format. For example:

→ Secure Socket layer / Transport layer security: These protocols use cryptography to secure communication over a computer network, such as securing a website's connection

→ Public key Infrastructure PKI: PKI uses pairs of keys (public and private) for encrypting and singing data. Its widely used in email encryption (e.g PGP) and secure online transactions.

Importance of Risk management:

Risk management is critical in identifying and mitigating potential threat to information security. A basic risk assesessment process involves:

1) Asset identification
2) Threat Assessment
3) Vulunerability Analysis
4) Impact Analysis
5) Risk Mitigation.

legal, Professional and ethical issues:

legal regulations professional standards and ethical consideration shape practices in information security, key points include.

1) Compiliance
2) Professional Integrity
3) Responsibility.

In summary, these concepts and principles are essential in establishing a robust information security framework that protects data and systems while considering legal, ethical and professional responsibilities.