Bh.IMPs - CCS | Computers Sem 6 | Final Sem Exams 2023

1. Enlist security goals. Discuss their significance.

2. Explain with an example keyed and keyless transposition cipher.

3. Compare AES and DES. Which one is bit-oriented? Which one is byte-oriented?

4. Explain to the man in the middle attack on Diffie Hellman. Explain how to overcome the same.

5. What are the requirements of the cryptographic hash functions? Compare MD5 and SHA Hash functions. State real-world applications of hash functions.

6. What are the properties of a hash function? Explain the role of the hash function in security.

7. Explain Kerberos in detail. OR Short note on Kerberos

8. Why are digital signatures and digital certificates required?

9. List various Software Vulnerabilities. How vulnerabilities are exploited to launch an attack.

10. Explain the different types of Denial of Service attacks.

11. What are the different types of firewalls? How is a firewall different from IDS?

12. Short note on (1) Buffer Overflow. (2) Worms and Viruses (3) SQL injection

1 **Introduction & Number Theory** :

Services, Mechanisms, and attacks-the OSI security architecture-Network security model-Classical Encryption techniques (Symmetric cipher model, mono-alphabetic and poly-alphabetic substitution techniques: Vignere cipher, Playfair cipher, Hill cipher, transposition techniques: keyed and keyless transposition ciphers, steganography).

2 **Block Ciphers & Public Key Cryptography** :

2.1 Data Encryption Standard-Block cipher principles-block cipher modes of operationAdvanced Encryption Standard (AES)-Triple DES-Blowfish-RC5 algorithm. Public key cryptography: Principles of public key cryptosystemsThe RSA algorithm, The knapsack algorithm, El-Gamal Algorithm. Key management – Diffie Hellman Key exchange Internal Assessment: Assessment:

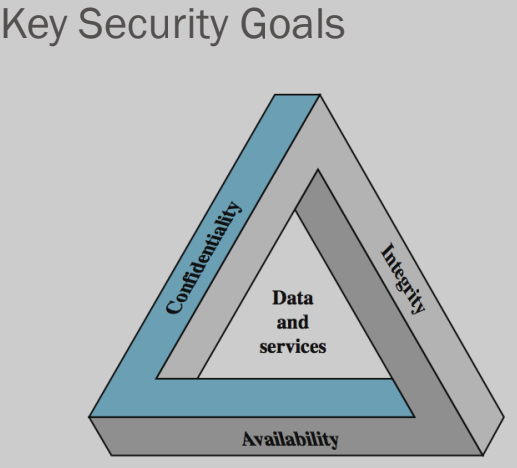
**3 Cryptographic Hashes**, Message Digests and Digital Certificates :

3.1 Authentication requirement – Authentication function , Types of Authentication, MAC – Hash function

Computer Security - generic name for the collection of tools designed to protect data and prevent hackers

Network Security - measures to protect data during their transmission

Internet Security - measures to protect data during their transmission over a collection of interconnected networks



To be secured, information needs to be :

Hidden from unauthorized access i.e. Confidentiality

Protected from unauthorized change i.e. Integrity

Available to an authorized entity when it is needed i.e.

Availability

