Duration: 3 Hrs. **Marks: 80**

Note:

1. **Question 1 is compulsory.**
2. **Attempt any 3 questions out of the remaining questions.**

Q1. Attempt any Four.

a.	Explain the different modes of block ciphers.	**05**
b.	List with examples the different mechanisms to achieve security.	**05**
c.	Differentiate MD5 and SHA-1 algorithms.	**05**
d.	List and explain security requirements of database.	**05**
e.	Explain phishing and list different types of phishing techniques.	**05**

Q2.

a.	User A and B want to use RSA to communicate securely. A chooses public key as (7, 119) and B chooses public key as (13, 221). Calculate their private keys. A wishes to send message m = 10 to B. Produce the ciphertext. Formulate the key using which A encrypt the message "m" if A need to authenticate itself to B.	**10**
b.	Explain memory and address protection in detail. Write a note on file protection.	**10**

Q3.

a.	List the functions of the different protocols of SSL. Explain the handshake protocol.	**10**
b.	List different poly-alphabetic substitution ciphers. Encrypt "The key is hidden under the door" using playfair cipher with keyword "domestic".	**10**

Q4.

a.	Define digital signature. Explain any digital signature algorithm in detail.	**10**
b.	Give the format of X.509 digital certificate and explain the use of a digital signature in it.	**10**

Q5.

a.	Explain session hijacking and management.	**10**
b.	What is need of Diffie-Hellman algorithm. User A and B decide to use Diffie-Hellman algorithm to share a key. They choose p = 23 and g = 5 as the public parameters. Their secret keys are 6 and 15 respectively. Compute the secret key that they share.	**10**

Q6. Attempt any Four.

a.	Explain the different types of firewalls and mention the layer in which they operate.	**05**
b.	List and explain vulnerabilities in windows operating system.	**05**
c.	List and explain characteristics needed in secure hash function.	**05**
d.	Explain Triple DES in short.	**05**
e.	Explain with examples, keyed and keyless transposition ciphers.	**05**

****