

- N. B.: (1) **All** questions are **compulsory**.
(2) Make **suitable assumptions** wherever necessary and **state the assumptions** made.
(3) Answers to the **same question** must be **written together**.
(4) Numbers to the **right** indicate **marks**.
(5) Draw **neat labelled diagrams** wherever **necessary**.
(6) Use of **Non-programmable** calculators is **allowed**.

1. Attempt any two of the following

10

- a. Explain the concept of key range and key size.
- b. Define the following terms:
 - i. cryptography
 - ii. cryptanalysis
 - iii. brute-force attack
 - iv. symmetric key cryptography
 - v. asymmetric key cryptography
- c. What are transposition techniques? Explain any one with the help of an example.
- d. What are the ethical and legal issues in computer security system?

2. Attempt any two of the following

10

- a. Explain the Cipher Block Chaining mode of the algorithm in detail.
- b. Explain blowfish algorithm and its advantages.
- c. Explain the steps in each round of DES.
- d. Explain the main features of AES; explain its steps at a high level.

3. Attempt any two of the following

10

- a. Explain the basics of digital signature.
- b. Explain the concept of message digest. What are the requirements of the message digest?
- c. Why HMAC cannot be trusted to be used in digital signatures?
- d. Explain the security solution based on the concept of Digital Envelope.

4. Attempt any two of the following

10

- a. What is digital certificate? How is it created?
- b. Write a brief note on cross certification in digital certificates.
- c. What are CRLs (Certificate Revocation Lists)? How are they used?
- d. Write a brief note on PKCS#5 Password Based Encryption (PBE) standard.

5. Attempt any two of the following

10

- a. Explain the functioning of Packet filter firewall. Explain the possible attacks on it.
- b. Explain the advantages and applications of IPSec.
- c. Explain the concept of Dual signature in SET (Secure Electronic Transaction).
- d. What is PGP? Explain how PGP works.

6. Attempt any two of the following

10

- a. Explain authentication method based on Challenge/Response tokens.
- b. How does certificate based authentication work?
- c. Write a brief note on Kerberos.
- d. Explain different approaches of mutual authentication.

