

(2½ hours)

[Total Marks: 75]

- 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 labeled diagrams** wherever **necessary**.  
 (6) Use of **Non-programmable** calculators is **allowed**.

1. **Attempt any two of the following:** 10
  - a. List and explain different types of criminal attacks. Give example of each one.
  - b. Explain with example different approaches to implement security model.
  - c. Write a short note on phishing.
  - d. Explain any two substitution techniques.
  
2. **Attempt any two of the following:** 10
  - a. How subkey is generated for rounds of IDEA algorithm?
  - b. List different cryptography algorithm types. Explain with example.
  - c. Explain double DES algorithm.
  - d. Write the working of RC4 algorithm.
  
3. **Attempt any two of the following:** 10
  - a. Write a short note on digital signature.
  - b. What is message authentication code? Write down disadvantages of hash-based message authentication code.
  - c. Differentiate between symmetric and asymmetric key cryptography.
  - d. Write down difference between MD5 and SHA-1.
  
4. **Attempt any two of the following:** 10
  - a. How digital certificate is created.
  - b. List and explain PKIX services.
  - c. What is the need of self-signed certificate needed?
  - d. Explain different mechanism for protecting private keys.
  
5. **Attempt any two of the following:** 10
  - a. List different email security protocols. Explain any one in detail.
  - b. Write a short note on electronic money.
  - c. How handshake protocol works?
  - d. What is firewall? Explain different types of firewall.
  
6. **Attempt any two of the following:** 10
  - a. How does Kerberos work?
  - b. What is authentication token? Explain how it works. Also list different types of authentication token.
  - c. Explain any one security handshake mechanism.
  - d. Write the working of clear text password.

7. Attempt *any three* of the following:
- a. What is virus? Write various phases of virus.
  - b. Explain Output Feedback algorithm mode.
  - c. Explain how MD5 works.
  - d. Write down the difference between online certificate revocation status checks and simple certificate validation protocol.
  - e. Differentiate between SSL and PLS.
  - f. Write a short note on smart cards.
-