Q. P. Code: 57847

(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.**

- Fraud
- Scams
- Destruction
- Identity Theft
- Intellectual Property Theft
- Brand Theft

b. **Explain with example different approaches to implement security model.**

- No Security
- Security Through obscurity
- Host security
- Network Security

c. **Write a short note on phishing.**
Explanation 5 marks

d. **Explain any two substitution technique.**

- Caesar cipher
- Modiedfied Caesar Cipher
- Homophonic Substitution cipher
- Polygram
- Polyalphabetic
- Playfair
- Monoalphabetic
- Hill Cipher

2. Attempt *any two* of the following: 10

a. **How subkey is generated for rounds of IDEA algorithm?**
Explanation 5 marks

b. **List different cryptography algorithm types. Explain with example.**

- Stream cipher
- Block cipher

c. **Explain double DES algorithm.**
Explanation 5 marks

d. **Write the working of RC4 algorithm.**

Explanation 5 marks

3. **Attempt *any two* of the following:** **10**

a. **Write a short note on digital signature.**
Explanation 5 marks

b. **What is message authentication code? Write down disadvantages of hash-based message authentication code.**
MAC 1 marks
Disadvantages 4 marks

c. **Differentiate between symmetric and asymmetric key cryptography.**
Explanation 5 marks

d. **Write down difference between MD5 and SHA-1.**
\ Explanation 5 marks

4. **Attempt *any two* of the following:** **10**

a. **How digital certificate is created.**
1. key generation
2. Registration
3 verification
4. certificate creation

b. **List and explain PKIX services.**

- Registration
- Initialization
- Certification
- Key pair recovery
- Key generation
- Key update
- Cross certification
- Revocation

c. **What is the need of self signed certificate needed?**
Explanation 5 marks

d. **Explain different mechanism for protecting private keys.**

- Password protection
- PCMCIA cards
- Tokens
- Biometrics
- Smart card

5. **Attempt *any two* of the following:** **10**

a. **List different email security protocols. Explain any one in detail.**

- Privacy Enhanced Mail
- Pretty Good Privacy
- Secure MIME

b. **Write a short note on electronic money.**
Explanation 5 marks.

c. **How handshake protocol works?**

Phase 1: establish security capabilities
Phase 2: server authentication and key exchange
Phase 3 : client authentication and key exchange
Phase 4 : finish

d. **What is firewall? Explain different types of firewall.**

Types:
Packet filter
Application gateways.

6. Attempt *any two* of the following: 10

a. **How does Kerberos work?**

Explanation 5 marks

b. **What is authentication token? Explain how it works. Also list different types of authentication token.**

Explanation 5 marks

c. **Explain any one security handshake mechanism.**

- One way authentication
- Mutual authentication

d. **Write the working of clear text password.**

7. Attempt *any three* of the following: 15

a. **What is virus? Write various phases of virus.**

Virus def 1 mark
Phases:
Dormant
Propagation
Triggering
Execution

b. **Explain Output Feedback algorithm mode.**

Explanation 5 marks

c. **Explain how MD5 works.**

1. padding
2. append length
3. divide the input into 512 bit block
4. initialize chaining variable
5. Process blocks

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.**