(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. **Explain different principles of security.**
Confidentiality
Authentication
Integrity
Non-Repudiation
Access control
Availability

b. **List and explain different types of criminal attacks. Give example of each one.**

Fraud
Scams
Destruction
Identity Theft
Intellectual Property Theft
Brand Theft

c. **List different transposition techniques. Explain any one with example.**
Rail Fence
Simple Columnar
Vernam Cipher
Book Cipher

d. **A and B want to establish a secrete key using the Diffie-Hellman Kay Exchange protocol. Assuming the values as n=11,g=5,x=2 and y=3, find out the values of A,B and the secret key.**

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

a. **Explain cipher feedback mode.**
Explanation 5 marks

b. **Explain DES algorithm.**
Explanation 5 marks

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

d. **Explain the working of RC5.**
Principle of operation
One time initial operation
Details of round

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

a. **Explain with example RSA algorithm.**

1. Choose two large prime numbers P and Q
2. Calculate N = P * Q
3. Select the public key E such that it is not a factor of (P-1) and (Q-1)
4. Select teh private key D such that the following equation is true
   (D*E) mod (P-1)*(Q-1) = 1
5. for encryption calculate the cipher text CT from the plain text PT as follows

$CT = PT^E \bmod N$

6. Send CT as the cipher text to the receiver
7. for decryption calculate the plain text PT from CT as follows

$PT = CT^D \bmod N$

b. **Write down difference between symmetric and asymmetric key cryptography.**

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. **What is message authentication code? Write down disadvantages of hash-based message authentication code.**

MAC 1 marks

Disadvantages 4 marks

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

a. **List and explain various fields in a X.509 digital certificate version 3.**

Version
Certificate serial number
Signature algorithm identifier
Issuer name
Validity
Subject name
Subject public key
Issuer unique identifier
Subject unique identifier
Authority key identifier
Subject key identifier
Key usage
Extended key usage
Private key usage period
Certificate policies
Policy mapping
Subject alternative name
Issuer alternative name
Subject directory attribute
Basic constraints
Name Constraints
Policy Constraints

b. **What is need of self-signed digital certificates and cross certificate?**

Explanation 5 marks

c. **Write down the difference between online certificate revocation status checks and simple certificate validation protocol.**

Differentiation points

- Client request
- Chain of trust
- Checks
- Returned information
- Additional features

d. **List and explain PKIX services.**

Registration

Initialization

Certification

Key pair recovery

Key generation

Key update

Cross certification

Revocation

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

a. **Explain the purchase request transaction of SET.**

1. initiate request
2. initiate response
3. purchase request
4. purchase response

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

Privacy Enhanced Mail
Pretty Good Privacy
Secure MIME

c. **Explain IP Datagram format.**

Explanation 5 marks

d. **List and explain different fields of security association database.**

Sequence number counter
Sequence counter overflow
Anti-replay window
AH authentication
ESP authentication
ESP encryption
IPSec protocol mode
Path maximum transfer unit
Life time

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

a. **What is authentication token? 1 mark**
Explain how it works. 3 mark
1. creation of token
2. use of token
3. server returns an appropriate message to the user.
Also list different types of authentication token. 1 mark

Challenge / response tokens
Time - based token

b. **What is the use of smart cards? Write down the problems and their solutions related to smart card technology.**
Use 1 mark
Problems and solution 4 marks

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

d. **Write a short note on one way authentication.**
Explanation 5 marks

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

a. **List and explain different types of attacks.**
Passive
Active

b. **Explain how subkey is generated in blowfish algorithm.**
Explanation 5 marks

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

d. **List different public key cryptography standards. Explain any two of them.**
PKCS#1 to PKCS#15

e. **What is electronic money? Classify electronic money based on**
i. Tracking of money
ii. Involvement of the bank in the transaction.
Definition 1 mark
i. identified electronic money
anonymous electronic money
ii. online electronic money
offline electronic money

f. **List and explain different approaches to achieve SSO.**
1. scripting
2. agent