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 vernam cipher with example.
b. List and explain types of criminal attacks.
c. Why there is need of security? Explain security models.
d. Explain IP spoofing and IP sniffing in details.

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

a. Explain Double and Triple DES.
b. Explain ECB and CFB algorithm modes in details.
c. Explain details of one round in IDEA.
d. Write note on Blofish.

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

a. Explain in details how symmetric and asymmetric key cryptography can be combined.
b. State and explain with example steps involved with RSA algorithm.
c. How Hash-based Message authentication works?
d. Explain problems with public key exchange.

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

a. List and explain the content of a digital certificate.
b. List and explain fields of a CRL.
c. Explain password based encryption standard in details.
d. Write a note on Blom's scheme.
e.

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

a. Explain how security is implemented in GSM.
b. Draw and explain Authentication Header format.
c. Distinguish between SSL and SET.
d. Write a note on VPN.

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

a. Explain how Kerberos work.
b. Explain how time based tokens works.
c. Write a note on certificate based authentication.
d. Explain one way authentication for carrying out the handshake.

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

a. Explain Diffie Hellman key exchange algorithm with example.
b. Explain processes in each round of AES.
c. Write a note on RSA and Digital Signature.
d. Explain station to station protocol.
e. Explain PGP operations.
f. Write a note on single sign on approaches.