(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. What is the need of security? Discuss different security models.
b. Write a note on Phishing.
c. Discuss the types of attacks from technical point of view.
d. Alice and Bob want to establish a secret key using the Diffie-Hellman Key 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 (K1 or K2).

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

a. Write note on Cipher Feedback (CFB) mode.
b. Differentiate between stream ciphers and block ciphers.
c. Discuss how encryption happens in RC5.
d. Explain the working of Blowfish algorithm.

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

a. Describe the advantages and disadvantages of symmetric and asymmetric key cryptography.
b. What is key wrapping? How is it useful?
c. Discuss the problems with exchanging of public keys?
d. Write a note on ElGamal digital signature

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

a. What is the purpose behind Certification Authority Hierarchy? Explain
b. Describe how cross certification is useful
c. Explain different types of digital certificates.
d. What are the role of Certification Authority and Registration Authority?

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

a. Explain the SSL (Secure Socket Layer) handshake protocol.
b. Differentiate between Secure Socket Layer (SSL) and Secure Electronic Transaction (SET).
c. Write note on Electronic money.
d. How GSM (Global System for Mobile) security does works?

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

a. What are the problems associated with clear text passwords? How can it be overcome?
b. How does Kerberos work?
c. What is reflection attack? How can it be prevented?
d. What is SSO (Signal Sign On)? Explain in brief

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

a. Discuss the Principles of Security
b. Explain the principles of the IDEA algorithm.
c. Discuss the history of asymmetric key cryptography in brief.
d. Explain the concept of Digital Certificate.
e. Explain Time Stamping Protocol.
f. Write a note on Biometric authentication.
