(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. Write a short note on principles of security.
b. Explain simple columnar transposition technique with example.
c. Explain Caesar cipher and modified version of Caesar cipher.
d. List & explain all possible types of attacks on messages.

2. Attempt *any two* of the following: **10**
a. Explain Algorithm Types in detail.
b. Write a short note on DES algorithm.
c. Explain AES in detail.
d. Write a short note on RC5 working.

3. Attempt *any two* of the following: **10**
a. Explain man-in-the-middle attack.
b. Write a short note on digital signatures.
c. Write a short note on SHA algorithm.
d. Write down differences between MD5 and SHA-1.

4. Attempt *any two* of the following: **10**
a. What are the steps involved in creating digital certificates?
b. Write a short note on ways of protecting private keys.
c. What are the PKIX services? Explain in detail.
d. Write a short note on digital certificate revocation checks.

5. Attempt *any two* of the following: **10**
a. Write a short note on TCP/IP protocol suite.
b. What are the types of firewalls?
c. What are two modes in which IPSec operates?
d. Write a short note on SSL.

6. Attempt *any two* of the following: **10**
a. How password authentication mechanism works?
b. Write a short note on certificate based authentication.
c. What are the types of biometric authentication?
d. Explain KDC in detail.

P.T.O.

10204

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

a. Explain following terms :
   1) Cryptography 2) Cryptanalysis 3) Cryptology
   4) Cryptanalyst 5) Brute-force attack.

b. Explain blowfish encryption & decryption in detail.

c. Differentiate between Symmetric & Asymmetric key cryptography.

d. What are the PKCS standards?

e. Write a short note on PGP.

f. What is Mutual Authentication? Explain the implementation ways.
