B.E. Seventh Semester (Information Technology) (C.B.S.)

# Computer System Security

P. Pages : 2 **NKT/KS/17/7499**

Time : Three Hours * 0 1 5 6 * Max. Marks : 80

---

Notes :
1. All questions carry marks as indicated.
2. Solve Question 1 OR Questions No. 2.
3. Solve Question 3 OR Questions No. 4.
4. Solve Question 5 OR Questions No. 6.
5. Solve Question 7 OR Questions No. 8.
6. Solve Question 9 OR Questions No. 10.
7. Solve Question 11 OR Questions No. 12.
8. Assume suitable data whenever necessary.
9. Illustrate your answers whenever necessary with the help of neat sketches.

**1.** a) Define the following terms in brief. **6**

i) Enciphering ii) Deciphering

iii) Cryptanalysis iv) Cryptography

v) Brute-force attack vi) Stegnography

b) Describe S-DES algorithm with diagram. **7**

**OR**

**2.** a) Explain DES algorithm in detail with functionality of S - Boxes and its strengths & weaknesses. **9**

b) "Network security model has no importance in practical approach" comment on the statement. **4**

**3.** a) Discuss IDEA encryption algorithm. **7**

b) Explain Chinese Reminder theorem. **6**

**OR**

**4.** a) "Blowfish algorithm provides cheap level of security". State whether the statement is true or false. Justify your answer. **7**

b) Explain key distribution & random number generator in detail. **6**

**5.** a) Discuss MD5 algorithm and how it is better than MD4. **6**

b) What is hash code? Explain what are the different ways you can use hash function. **8**

**OR**

**6.** a) Two parties would like to share common secret key by using a Diffie - Hellman key exchange algorithm with a common prime number q = 11 and a primitive root $\alpha = 2$ then **4+5**

i) If user A has public key $Y_A = 9$, what is A's private key $X_A$?

iii) If user B has public key $Y_B = 3$, what is the shared secret key.

b) Explain MAC with its properties and requirements in brief. **5**

**7.** a) Differentiate between SHA - 1 and RIPEMD - 160 with detail explanation. **8**

b) Explain the architecture and working principle of Kerberos 5.0. **6**

**OR**

**8.** a) Discuss HMAC in brief with diagram. **6**

b) Explain digital signature standard along with digital signature algorithm with its properties and its requirements. **8**

**9.** a) "If security architecture plays a vital role in data communication" - comment. **6**

b) What is PGP? List the various services it has consisted and explain. **7**

**OR**

**10.** a) Discuss S/MIME in detail. **6**

b) How compression technique is useful and implemented in ZIP. Explain with example. **7**

**11.** a) Discuss SSL handshake protocol in brief. **4**

b) Explain, malicious softwares which requires a host program and which do not require host program. **5**

c) Explain the concept of firewall in brief. **4**

**OR**

**12.** a) Write a short note on **any two.** **6**

i) Web Security ii) Trusted system

iii) Honeypot.

b) Explain various phases of virus lifecycle. **4**

c) Discuss secure electronic transaction in brief. **3**

**********