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

# Computer System Security

P. Pages : 2 **TKN/KS/16/7585**

Time : Three Hours * 0 9 0 7 * 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. Due credit will be given to neatness and adequate dimensions.
9. Assume suitable data whenever necessary.

**1.** a) Explain various categories of security attacks. Also explain passive and active attacks. **8**

b) Encrypt the message "Assume suitable data whenever necessary" With the key "generalization". using play fair cipher. **5**

**OR**

**2.** a) Explain simplified DES algorithm in detail. **7**

b) Explain any three block cipher modes of operation. **6**

**3.** a) Explain characteristics of advanced symmetric block ciphers. **7**

b) Explain a single round operation of CAST-128 algorithm. **6**

**OR**

**4.** a) Explain the types of information that can be derived from traffic analysis attack. What are the approaches to provide traffic confidentiality? **8**

b) Explain Chinese remainder theorem with example. **5**

**5.** a) Differentiate between conventional and public key encryption system. **5**

b) Explain various key management schemes in public key environment. **9**

**OR**

**6.** a) Write short notes on security of hash functions and MACS. **8**

b) What are the authentication requirements in communication network? **6**

**7.** a) Compare following hash algorithms. **8**
i) MD – 5 ii) SHA – 1 iii) RIPEMD – 160.

b) Explain digital signature algorithm in detail. **6**

**OR**

| | | | |
|---|---|---|---|
| **8.** | a) | Explain in detail about X-509 directory authentication service. Describe format of X-509 certificate and certificate revocation. | **8** |
| | b) | What is Kerberos Realm? Write principle differences between Kerberos version 4 and version 5. | **6** |
| **9.** | a) | Explain RADIX-64 conversion technique in detail. | **6** |
| | b) | Explain the concept of S/MIME functionality. | **7** |

**OR**

| | | | |
|---|---|---|---|
| **10.** | a) | Explain ESP (Encapsulating security payload) in detail. | **7** |
| | b) | Explain IP Security architecture in brief. | **6** |
| **11.** | a) | Explain secure electronic transaction protocol in detail. | **8** |
| | b) | Explain the features of Oakley key protocol. | **5** |

**OR**

| | | | |
|---|---|---|---|
| **12.** | a) | Explain Intruders Explain Intrusion detections techniques. | **5** |
| | b) | Differentiate between viruses and worms. | **4** |
| | c) | Explain the concept of Trusted systems. | **4** |

**********