BE/COMP/Sem-VII CBSGS/CSS

19/5/16

QP Code : 31296

(Time: 3hrs) (Marks 80)

1. Question No 1 is compulsory.
2. Attempt any three out of the remaining five questions.

Q1. (a) Explain software flaws with examples **05**
(b) List with examples the different mechanisms to achieve security **05**
(b) Explain with examples, keyed and keyless transposition ciphers **05**
(c) Elaborate the steps of key generation using RSA algorithm **05**

Q2. (a) A and B decide to use Diffie Hellman algorithm to share a key. They chose p=23 and g=5 as the public parameters. Their secret keys are 6 and 15 respectively. Compute the secret key that they share. **10**
(b) Explain working of DES. **10**

Q3. (a) What is access control? How does the Bell La Padula model achieve access control. **10**
Q3. (b) What is a digital signature. Explain any digital signature algorithm in detail. **10**

Q4. (a) Compare packet sniffing and packet spoofing. Explain session hijacking attack. **10**

Q4. (b) Explain working of Kerberos. **10**

Q5. (a) What is a firewall? What are the firewall design principles? **05**

Q5. (b) What are the various ways for memory and address protection **05**

Q5. (c) Explain the significance of an Intrusion Detection System for securing a network. Compare signature based and anomaly based IDS. **10**

Q6. Write in brief about (any four): **20**
i) Email Security.
ii) SSL handshake protocol
iii) IPSec protocols for security
iv) Denial of service attacks
v) IDEA

.....