T.E. (IT) (Sem-V) (CCB) Date -25/11/19

**Duration : 3 Hours** **Total Marks: 80**

**Instructions to the candidates, if any:-**

**N.B. :** (1) Question No. 1 is compulsory.

(2) Attempt any three questions out of remaining five questions.

| **Q. No.** | **Marks** |
|---|---|
| Q.1 (a) Write short note on eavesdropping. | (05) |
| (b) Write short note on Stenography. | (05) |
| (c) Write a short note on Blowfish. | (05) |
| (d) List S/MIME services. | (05) |
| Q.2 (a) Explain Transposition Ciphers with illustrative Example. | (10) |
| (b) Compare and contrast DES and AES. | (10) |
| Q.3 (a) Perform encryption and decryption using RSA algorithm with p=7,q=11,e=17 and M=8. | (10) |
| (b) Describe the Block Cipher Modes in detail. | (10) |
| Q.4 (a) Explain Kerberos Protocol in detail. | (10) |
| (b) What Is PKI. Explain different PKI architectures in detail. | (10) |
| Q. 5 (a) Explain Diffie Hellman Key Exchange with suitable Example. | (10) |
| (b) Explain Needham-Schroeder protocol for secret key distribution with suitable diagram. | (10) |
| Q. 6 Write short notes on **(Any Four)** | (20) |
| i) HMAC vs CMAC | |
| ii) ARP Spoofing | |
| iii) Port Scanning | |
| iv) Honeypot | |
| v) EI-Gamal Algorithm | |
| vi) Session Hijacking | |



21B16FC4CF1CA58890D1D90136626DF1