SC - 179

Total No. of Pages : 1

Seat No.	

T.E. (C.S.E.) (Part - III) (Semester - VI) Examination, November - 2019
INFORMATION SECURITY
Sub. Code: 66862

Day and Date : Wednesday, 20 - 11 - 2019 **Total Marks : 50**

Time : 9.30 a.m. to 11.30 a.m.

Instructions :
1) **Q.3 and Q.6 are compulsory.**
2) **Solve any one out of Q.1 and Q.2.**
3) **Solve any one out of Q.4 and Q.5**

Q1) a) Explain key distribution using Public key Certificates. **[6]**

b) Describe the model for Network Security with neat diagram. **[6]**

Q2) a) Illustrate key generation in DES algorithm with neat diagram. **[6]**

b) State the requirements of MAC. What are the basic uses of MAC? **[6]**

Q3) a) Compare : **[6]**

i) Block Cipher and Stream Cipher.

ii) Confusion and Diffusion.

b) Explain the RSA algorithm. Perform encryption & decryption using RSA algorithm if $p = 5$, $q = 11$, $e = 3$, $M = 9$. **[7]**

Q4) a) Distinguish between Kerberos Version 4 and Version 5. **[6]**

b) Give the participants of SET and also briefly describe the sequence of events in them, that are required for an electronic transactions. **[6]**

Q5) a) How Kerberos works in multiple Realm. **[6]**

b) Explain various services provided by PGP. **[6]**

Q6) a) Explain X-509 Certificate format in detail with diagram. **[6]**

b) Explain in detail ESP Format in IPSEC. **[7]**

⌘⌘⌘

SUK-39954