SF - 234

Total No. of Pages : 2

Seat No.	

T.E. (CSE) (Part - II) (Semester - VI) Examination, November - 2017

INFORMATION SECURITY

Sub. Code: 66862

Day and Date : Tuesday, 07 - 11 - 2017 **Total Marks : 50**

Time : 2.30 p.m. to 4.30 p.m.

Instructions :
1) **Q.3 and Q.4 are compulsory.**
2) **Solve any one out of Q.1, Q.2 and Solve any one out of Q.5, Q.6.**
3) **Assume suitable data wherever necessary.**

Q1) a) List & Explain the security services defined in X.800. **[6]**

b) Explain the DES encryption with neat block diagram. **[6]**

Q2) a) Explain the RSA algorithm. Perform encryption & decryption using RSA algorithm **if p=11, q=3, e=11, M=7** **[6]**

b) What is Message Authentication Code? Explain generation of MAC based on DES. **[6]**

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

i) Symmetric and Asymmetric ciphers

ii) Differential and Linear cryptanalysis

b) Explain Diffie-Hellman key exchange algorithm with example. **[4]**

c) Define the following terms w. r. t Avalanche effect: **[3]**

i) SIC

ii) BIC

iii) GA

P.T.O.

Q4) a) Explain in detail different approaches to Digital Signatures. **[6]**

b) What is certificate format in X.509 standard? **[7]**

Q5) a) Draw general format of PGP message and explain every field of it in detail. **[6]**

b) List types of firewalls. Explain any one in detail. **[6]**

Q6) Write a short note on any two. **[12]**

a) IPSec Authentication Header.

b) SET Participants.

c) Trusted System.

❄ ❄ ❄