Seat No.	

T.E.(C.S.E) (Part-II) (Semester-VI) Examination, May - 2017
INFORMATION SECURITY (Theory)
Sub. Code : 66862

Day and Date : Saturday, 06-05-2017 **Total Marks : 50**
Time : 2.00 p.m. to 4.00 p.m.

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

Q1) a) List and explain the security mechanisms defined in X.800. [6]

b) Explain key generation in DES algorithm with neat diagram. [6]

Q2) a) Explain the RSA algorithm. Perform encryption & decryption using. RSA algorithm if p = 5, q = 11, e = 3, M = 9 [6]

b) State the requirements for a Hash function. Explain Simple Hash Functions. [6]

Q3) a) Compare [6]

i) Block Cipher and Stream Cipher

ii) Confusion and Diffusion

b) Explain Diffie-Hellman key exchange. Also explain in detail man-in-the-middle attack on Diffie-Hellman Key exchange. [7]

Q4) a) Explain Digital Signature Standard using Digital signature algorithm (DSA). [6]

b) What are the differences between Kerberos version 4 and version 5?[7]

SUK-SDG

P.T.O.

Q5) a) Draw the SSL protocol stack. Explain its architecture. **[6]**

b) Describe the different types of Intrusion detection system. **[6]**

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

a) S/MIME

b) SET Participants

c) Unix Password scheme

✈ ✈ ✈

SUK-SDG