SV - 205

Total No. of Pages : 2

Seat No.	

T.E. (CSE) (Part - II) (Semester - VI) Examination, May - 2018

INFORMATION SECURITY

Sub. Code : 66862

Day and Date : Tuesday, 15 - 05 - 2018 **Total Marks : 50**

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

Instructions : 1) **Q. 3 and Q. 6 are compulsory.**

2) **Solve any one out of Q. 1, Q. 2 and Solve any one out of Q. 4, Q. 5.**

3) **Assume suitable data wherever necessary.**

Q1) a) Describe the Security Attacks and explain the model for Network Access Security with neat diagram. [6]

b) List and explain the basic principles of block cipher design. [6]

Q2) a) Describe the RSA algorithm. In a public key system using RSA, you intercept the ciphertext C = 14 sent to a user whose public key is e=7, n=33. [6]

b) In what way, the Diffie Hellman key exchange is prone to the man-in-the-middle attack. [6]

Q3) a) What is Substitution technique? Given a key: **BREAKDOWN** Construct the Playfair matrix & perform the encryption of the following text: **We are discovered**. [6]

b) Explain Simple Hash functions? Explain the security of Hash functions in detail. [7]

P.T.O.

Q4) a) Draw a figure and explain the DSS signing and verifying functions in details. [7]

b) Explain multi realm authentication in Kerberos authentication system. [6]

Q5) a) Give overview of IPSec architecture. [6]

b) Explain design goals of firewalls in detail. [6]

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

a) Distributed Intrusion Detection.

b) Password Management.

c) S/MIME.