SE - 209

Seat No.	

Total No. of Pages : 1

T.E. (CSE) (Semester - VI) Examination, November - 2018
INFORMATION SECURITY
Sub. Code : 66862

Day and Date : Friday, 16 - 11 - 2018 **Total Marks : 50**

Time : 02.30 p.m. to 04.30 p.m.

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

Q1) a) Explain the transposition ciphers with examples. [6]
b) Explain with neat block diagram, a single round of DES algorithm. [6]

Q2) a) How can public key cryptography be used to distribute the secret keys? [6]
b) Explain Diffie Hellman key exchange algorithm Users A and B use the Diffie-Hellman key exchange technique with a common prime q=11 and a primitive root $\alpha = 2$ [6]
i) If user A has a private key YA = 9, what is A's public key XA?
ii) If user B has a public key YB = 3, what is the shared secret key k?

Q3) a) Write short notes on (any two) [6]
i) Steganography
ii) Avalanche effect
iii) RSA algorithm
b) What is message authentication? In what way, are the Hash functions used to provide message authentication. [7]

Q4) a) Compare between the traditional DSS approach and RSA approach in terms of their working. [6]
b) List and define the parameters that define secure socket layer (SSL) session state and ssl connections. [6]

Q5) a) Explain Encapsulating security Payload (ESP) service in IPSec. [7]
b) Describe different firewall configurations. [6]

Q6) a) What is motivation behind Kerberos? State Kerberos requirements. [6]
b) Describe the functions provided by S/MIME [6]

❍❍❍