SV - 210

Total No. of Pages : 2

Seat No.	

T.E. (CSE) (Semester - VI) Examination, May - 2019

INFORMATION SECURITY (Theory)

Sub. Code : 66862

Day and Date : Saturday, 25 - 05 - 2019 **Total Marks : 50**

Time : 09.30 a.m. to 11.30 a.m.

Instructions :
1) **Q.3 is compulsory.**
2) **Solve any one out of Q. 1 and Q.2.**
3) **Solve any two questions from Q. 4, Q.5 and Q.6.**

Q1) a) Differentiate between monoalphabetic and polyalphabetic ciphers? What are the limitations of one-time pad? **[6]**

b) Explain with Block diagram, a single round of DES Algorithm. **[6]**

Q2) a) How certification authorities are useful for distribution of public keys? **[6]**

b) Users A and B use the Diffie-Hellman key exchange technique with a common prime q=71 and a primitive root $\alpha = 7$ **[6]**

i) If user A has a private key XA = 5, what is A's public key YA?

ii) If user B has a private key XB = 12, what is B's public key YB?

iii) What is the shared secret key?

Q3) a) Write short notes on (any 2) : **[6]**

i) Steganography

ii) Hash functions

iii) Differential Cryptanalysis

b) What is message authentication? How to achieve message authentication using hash functions? **[7]**

P.T.O.

Q4) a) How does arbitrated digital signature technique overcome the disadvantage of traditional digital signature. [6]

b) What is dual signature in secure electronic transaction (SET)? What is its purpose? [6]

Q5) a) Discuss the applications and benefits of IPSec. [7]

b) Describe different firewall configurations. [6]

Q6) a) With the help of figure explain the profiles of behavior of intruders and authorized user. [6]

b) Draw the X.509 certificate and explain all its fields. Why does the communicating parties require this certificate. [6]

❖❖❖❖

SUK-32614