Registration No : | | | | | | | | | | |

Total Number of Pages : 02 **B.Tech**

PCS7J001

7th Semester Regular Examination 2018-19

CRYPTOGRAPHY & NETWORK SECURITY

BRANCH : CSE

Time : 3 Hours

Max Marks : 100

Q.CODE : E036

Answer Question No.1 (Part-1) which is compulsory, any EIGHT from Part-II and any TWO from Part-III.

The figures in the right hand margin indicate marks.

Part- I

Q1 Short Answer Type Questions (Answer All-10) **(2 x 10)**

a) Differentiate between confidentiality and integrity.

b) Explain the diffusion and confusion.

c) List all multiplicative inverse pairs in modulus 10.

d) The encryption key in transposition cipher is (3,2,6,1,5,4). Find the decryption key.

e) Define a state in AES. How many states are there in each version of AES ?

f) List four key steps in the creation of a digital signature.

g) What are possible threats to Electronic Money Transfer?

h) Find the multiplicative Inverse of 60 in Z_{101} using Fermats Little Theorem.

i) What is Euler's totient function ?

j) Distinguish between a session and connection with respect to SSL protocol.

Part- II

Q2 Focused-Short Answer Type Questions- (Answer Any EIGHT out of TWELVE) **(6 x 8)**

a) Describe ceaser cipher and monoalphabetic cipher suitable examples.

b) Find the gcd (208, 264) using Euclidian algorithm

c) Distinguish between Symmetric key and Asymmetric key cryptography. Define a trap - door one way function and explain its use in an asymmetric -key-cryptography.

d) Explain the key generation, encryption, decryption of DES algorithm in detail.

e) Using the RSA scheme , let p = 809,q = 751,and d = 23. Calculate the public key e. Then sign and verify the message with M=100.

f) Explain the possible attacks on RSA algorithm.

g) Briefly discuss the effect and causes of viruses.

h) Define the Diffie-Hellman protocol and its purpose. Explain the man in the middle attack in D-H protocol.

i) What is digital signature? Explain RSA digital signature standard briefly.

j) Distinguish between message authentication and entity authentication. Explain diffrent types of password approach.

k) Use the Vigenere cipher with keyword "HEALTH" to encipher the message "Life is all about problem to solve"

l) What do you mean by electronic money?

Part-III

Long Answer Type Questions (Answer Any TWO out of FOUR)

Q3	Discuss any four Substitution Technique and list their merits and demerits.	**(16)**
Q4	Explain the block cipher modes of operation.	**(16)**
Q5	Describe the MD5 message digest algorithm with necessary block diagrams.	**(16)**
Q6	Explain the technical details of firewall and describe any three types of firewall with neat diagram.	**(16)**