Printed Pages: 01 **Subject Code:CSIT371**

Paper Id: **190061** **Roll No:** | | | | | | | | | | |

M TECH
(SEM III) THEORY EXAMINATION 2018-19
CRYPTOGRAPHY

Time: 3 Hours ***Total Marks:100***

Notes: *Assume any Missing Data.*

1. Attempt any four of the following: **(5×4=20)**

(a) State and proof Fermat theorem?
(b) Why confidentially is an important principle of security, describe the ways to achieving it?
(c) Define Euclidean Algorithm and Chinese Remainder Theorem.
(d) What is the difference between Active and Passive attack, Name of active and passive attacks?
(e) What is the difference between Virus and worms?

2. Attempt any two parts of the following: **(10×2=20)**

(a) What is digital signature? What are the requirements for a digital signature? Describe the digital signature algorithm proposed as part of the digital signature standards (DSS). Give proof of the algorithm. Why each signature requires a new value of K (secret number generated per message in the DSA)?
(b) Why the middle portion of triple DES in a decryption rather than encryption? Discuss the strength of DES algorithm and also explain the substitution method including the P-Box. What is purpose of the S-Boxes in DES?
(c) Discuss how different steps of SHA produce a message digest.

3. Attempt any two parts of the following: **(10×2=20)**

(a) What is the motivation for cryptosystems based on finite automata? Describe Ra Rb transformation method.
(b) Caesar's cipher is one of the simplest and most widely known encryption techniques, in which each letter in the original text is replaced by a letter some fixed number of positions down the alphabet. For example, with a shift of 3, the letter a would be replaced by d, b would become e, and so on, the last three letters in the alphabet are replaced by a, b and c respectively. Describe formally (i.e., by means of a transition function) a Turing machine which encrypts (with the shift 3) any word in the alphabet © = {a, b, c, d, e}.
(c) Discuss the idea of Elliptic curve cryptography.

4. Attempt any two parts of the following: **(10×2=20)**

(a) Determine the number of padding bit in MD5 hashing algorithm if length of original message is 51 200 bits.
(b) Explain RSA Algorithm. Find the private key of a user if his key e = 21 and an equal to 3599.
(c) What is a discrete logarithm? Find the discrete logarithms to the base 15, modulo 19.

5. Attempt any two parts of the following: **(10×2=20)**

(a) Write a short note on:
  (i) Secure electronic transaction (SET)
  (ii) IPSec.
  (iii) Intrusion detection.
(b) Explain in details Finite automata and ciphers.
(c) Write a short note on birthday attack problem and firewall.