Reg. No.										

MANIPAL INSTITUTE OF TECHNOLOGY

MANIPAL

A Constituent Institution of Manipal University

III SEMESTER MCA
MAKE UP EXAMINATIONS
DECEMBER 2017

SUBJECT: **INFORMATION AND NETWORK SECURITY – (MCA-5013)**

REVISED CREDIT SYSTEM

(27/12/2017)

Time: 3 Hours MAX. MARKS: 50

Instructions to Candidates:

- Answer **ALL FIVE FULL** questions.
- Missing data may be suitable assumed.

1A.	What is authentication token? Explain how user authentication can be achieved using certificate based authentication mechanism?	**5**
1B.	Describe CFB (Cipher Feedback) and Output Feedback (OFB) modes of operations.	**3**
1C.	What are the different phases of virus during its lifetime?	**2**
2A.	Illustrate the different steps of Data Encryption Standard (DES) with suitable diagrams. Given the 6 input bits of an S-box as 101001, identify the row and column of S-box which would be selected as output in the S-box substitution step.	**5**
2B.	Describe the encryption and decryption rules for Playfair cipher technique. Perform the encryption on the message “CRYPTO IS TOO EASY” with a key “INFOSEC” using Playfair technique.	**3**
2C.	What are the characteristics of cryptographic system?	**2**

3A.	State Chinese remainder theorem and solve the simultaneous congruence using Chinese remainder theorem X = 1 mod 2 X = 2 mod 3 X = 3 mod 5 X = 4 mod 11	**5**
3B.	State Euclidean algorithm in cryptography. Find GCD of (1970, 1066) using Euclidean Algorithm.	**3**
3C.	Differentiate SHTTP and SSL	**2**
4A.	Discuss the message digest creation mechanism in SHA-1 with suitable diagrams.	**5**
4B.	Illustrate the problem of key exchange in symmetric key cryptography with suitable examples. A small private club has only 100 members. How many secret keys are needed if all the members of the club need to send secret messages to each other using symmetric cryptography?	**3**
4C.	Compare HMAC and CMAC.	**2**
5A.	Explain the working of PGP and S/MIME protocol. How do these protocols provide security to emails?	**5**
5B.	Differentiate between packet filters, application-level gateways, circuit-level gateways.	**3**
5C.	Differentiate monoalphabetic and homophonic substitution ciphers with suitable examples.	**2**