Reg. No.									

MANIPAL INSTITUTE OF TECHNOLOGY

MANIPAL

(A constituent unit of MAHE, Manipal)

III SEMESTER M.C.A.

END SEMESTER EXAMINATIONS, NOV 2018

SUBJECT: INFORMATION AND NETWORK SECURITY [MCA 5013]

REVISED CREDIT SYSTEM

(27/11/2018)

Time: 3 Hours MAX. MARKS: 50

Instructions to Candidates:

- Answer **ALL** the questions.
- Missing data may be suitably assumed.

1A.	Describe how a digital signature scheme works with the help of relevant diagrams.	**5**
1B.	What are the three independent measures of cryptography? Give a suitable example for each.	**3**
1C.	Write in brief the four primary security principles related to a user's plain text message.	**2**
2A.	With a neat labelled diagram describe how a hash function can be used for message Authentication.	**5**
2B.	What basic arithmetic and logical functions are used in SHA?	**3**
2C.	List important design considerations for a stream cipher.	**2**
3A.	Describe the requirements for Public-Key Cryptography.	**5**
3B.	State and explain Fermat and Euler's Theorem.	**3**
3C.	Write any two strengths and two weaknesses of RC4 algorithm.	**2**
4A.	State and explain Hashed Message Authentication Code (HMAC) design objectives.	**5**
4B.	Define three levels of impact on organizations or individuals should there be a breach of security (i.e., a loss of confidentiality, integrity, or availability)	**3**
4C.	Find Ø(37) and Ø(125) using Euler's Totient function.	**2**
5A.	Explain the structure and working principles of IPSec Authentication Header with relevant diagrams.	**5**
5B.	Write about the cryptographic services provided by digital signatures.	**3**
5C.	What is the role of a compression function in hashing?	**2**