R

Reg. No.									

Manipal Institute of Technology

(A Constituent Institute of Manipal University)

III SEMESTER M. C. A.
END SEMESTER EXAMINATION – NOV/DEC 2015

SUBJECT: INFORMATION AND NETWORK SECURITY [MCA 5013]

02-12-2015

Time : 3 hours

Max. Marks : 50

Instructions to Candidates

1. Answer ANY FIVE FULL questions.
2. Missing data may be suitably assumed.

1A With a labeled diagram explain any five X.800 Security Services and the Model for Network Security.

1B What are the three independent measures of cryptography? Give a suitable example for each.

1C Encrypt the text "When I thought I spied some land" using Hill Cipher Technique. Assume the key as $\begin{bmatrix}5 & 7\\ 8 & 9\end{bmatrix}$

(5 + 3 + 2)

2A Explain the concept of Digital Envelopes and its applications.

2B Describe the following 3 services provided by digital signatures: Message integrity, Message Authentication, Message Nonrepudiation.

2C What is the significance of padding field in Encapsulated Security Payload?

(5 + 3 + 2)

3A Discuss any 5 parameters associated with each Security Association in IPSec implementation

3B Compare and Contrast MAC and HMAC

3C Discuss the two approaches used for intrusion detection

(5 + 3 + 2)

4A Compare and Contrast various SHA Parameters for SHA-1, SHA-256 and SHA-512

4B Simplified Depiction of Essential Elements of Digital Signature Process

4C Compare and Contrast Weak Collision Resistance and Strong Collision Resistance.

(5 + 3 + 2)

5A Discuss the Certificate creation steps for X.509 digital certificates.

5B Compare functionalities of Tunnel Mode and Transport Mode in Transport Layer Security

5C Apply RSA algorithm for the given data: Take p = 17; Q=17; E= 5; D = 77. Using the given information describe the steps in encryption and decryption of the letter 'F'.

(5 + 3 + 2)

6A Explain any 5 Requirements for Public-Key Cryptography.

6B What basic arithmetic and logical functions are used in SHA?

6C How data access control is done in trusted systems?

(5 + 3 + 2)