Reg. No.										

प्रज्ञानं ब्रह्म

Manipal
INSPIRED BY LIFE

MANIPAL INSTITUTE OF TECHNOLOGY, MANIPAL 576104

(Constituent College of Manipal University)

SECOND SEMESTER M.TECH. (S/W) DEGREE MAKE UP EXAMINATION, JUNE2016

SUBJECT: PROGRAM ELECTIVE I -INFORMATION SECURITY – ICT 558

(REVISED CREDIT SYSTEM)

TIME: 3 HOURS **30/06/2016** **MAX. MARKS: 50**

Instructions to candidates

- Answer any **FIVE FULL** questions.
- Missing data, if any, may be suitably assumed.

1A. For Elgamal cryptosystem, discuss the key generation, encryption and decryption algorithm with proof of working.

1B. Assume a public key for RSA encryption given by the pair (143, 11).

i. Find the private key to the given public key.

ii. Decode the message (111 4 88 57 116 67), assuming the letters were represented by ASCII values.

1C. Differentiate between unconditionally secure and computationally secure encryption scheme with example.

(5+3+2)

2A. Draw the IP Security scenario and discuss the Transport and Tunnel modes of operation.

2B. With relevant messages, discuss Encrypted Key Exchange protocol (EKE)?

2C. Distinguish between MDC and MAC.

(5+3+2)

3A. Discuss different types of typical attacks possible on Authentication Protocols.

3B. How Man-In-The-Middle attack is possible in Diffie-Hellman algorithm? Demonstrate with an example.

3C. What is data origin authentication?

(5+3+2)

4A. Explain the working of handshake protocol in SSL.

4B. What is reflection attack? How it is launched?

4C. Explain the Compression function of MD developed by Ronald Rivest.

(5+3+2)

5A. With relevant messages show how the authentication failure in signature based IKE phase 1 Main mode is possible?

5B. How Needhams password protocol can be realized in the UNIX operating system?

5C. Analyse the Timing Attacks in DES.

(5+3+2)

6A . Discuss the working of Station to Station (STS) protocol. What flaw exists in simplified STS Protocol?

6B. Write the format of X.509 public key certificate. Mention the importance of each field.

6C. Differentiate between Threat and Attack according to RFC2828

(5+3+2)