Reg. No.										

प्रज्ञानं ब्रह्म

Manipal
INSPIRED BY LIFE

MANIPAL INSTITUTE OF TECHNOLOGY, MANIPAL 576104

(Constituent College of Manipal University)

VII SEMESTER B.TECH (IT) DEGREE END SEMESTER EXAMINATIONS,DEC – 2015

SUBJECT: ELECTIVE-IV:E-COMMERCE AND NETWORK SECURITY – ICT 439

TIME: 3 HOURS **03/12/2015** **MAX. MARKS: 50**

Instructions to candidates

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

1A. Write Kerberos V5 Message exchanges.
1B. With a neat diagram explain AES key expansion process.
1C. Differentiate between confusion and diffusion. How these two terms are applicable in cryptography?

[5+3+2]

2A. Discuss elementary SHA operation. How 80-word Input Sequence for SHA-1 processing of a single Block is generated?
2B. With a timing diagram, show the action of SSL Hand Shake Protocol between client and server.
2C. Discuss various access control methods.

[5+3+2]

3A. Consider the following data:
$n = 527$; $f(n) = 480$; $d = 343$; C = 128. Decrypt the cipher text C using RSA algorithm.
3B. Relate various security Services and Mechanisms based on X.800 Specification for Access Control, Digital Signature and Routing control.
3C. Convert the hexadecimal data 3A2E5C into radix-64.

[5+3+2]

4A. How the Card Holders Purchase Request is prepared in the SET Protocol? With a neat diagram, discuss the significance of each message associated in it.
4B. Write packet-filter firewall security policies for the following:
i) Block all the packets transmitting from the inside host OURHOST through the port 25 to the internet.
ii) Allow all the packets transmitting from the outside host THEIRHOST through the port 80 to the inside host OURHOST.
4C. What is a dual homed Bastian host? Discuss the merits and demerits of the same.

[5+3+2]

5A. Let M1 be the bitwise complement of M. If the complement of plaintext block and key is taken then. whether the result of encryption has any impact? Prove your answer.
5B. What are the capabilities of structured documents?
5C. What are the two approaches for intrusion detection?

[5+3+2]

6A. Explain the following:
i) Digital signatures
ii) Digital documents

6B. Explain the different extensions available in X.509 v3 digital Certificates?
6C. Mention the four components of agility?

[5+3+2]