Reg. No.										

प्रज्ञानं ब्रह्म

MANIPAL INSTITUTE OF TECHNOLOGY, MANIPAL 576104

(Constituent College of Manipal University)

SEVENTH SEMESTER B.TECH (IT) DEGREE MAKE UP EXAMINATION, JAN 2016
SUBJECT: ELECTIVE-IV:E-COMMERCE AND NETWORK SECURITY – ICT 439

TIME: 3 HOURS **05/01/2016** **MAX. MARKS: 50**

Instructions to candidates

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

1A. With a neat diagram explain Compression function and primitive logical functions of SHA-1.

1B. Calvin Butterball keeps pet meerkats in his backyard. If he divides them into 5 equal groups, 4 are left over. If he divides them into 8 equal groups, 6 are left over. If he divides them into 9 equal groups, 8 are left over. What is the smallest number of meerkats that Calvin could have?.

1C. Differentiate between a MAC and a Message Digest.

[5+3+2]

2A. Using S-DES, decrypt the string (10100010) using the key (0111111101). Show intermediate results after each function (IP, F_k, SW, F_k, IP^{-1}). Then decode the first 4 bits of the plaintext string to a letter and the second four bits to another letter where we encode A through P in base 2.
(i.e., A=0000, B=0001,…., P=1111).

2B. How Man-In-The-Middle attack is possible in Diffie Hellmann algorithm? Demonstrate with an example..

2C. Why there is a separate change cipherspec protocol existing in SSL and TLS rather than including a change cipherspec message in the handshake protocol?.

[5+3+2]

3A. Using extended Euclidean algorithm find the Multiplicative inverse of 24140 mod 40902.

3B. Discuss the three authentication procedures in X.509 that are used across a variety of applications.

3C. Using PLAYFAIR cipher with a key “MONARCHY”, for the word “HAMAMI” find the receivers interpretation after decryption. [5+3+2]

4A. Explain the Cipher Feed Back and Cipher Block Chaining modes of DES operation with a neat diagram.

4B. Discuss the different phases of a Virus.

4C. Perform Encryption and Decryption using RSA for p=17, q=31,e=7,M=2.

[5+3+2]

5A. Write Kerberos V4 Message exchanges and state the technical deficiencies.

5B. What are the elements of Supply Chain Management Models?

5C. Differentiate between Threat and Attack according to RFC2828?

[5+3+2]

6A. With a neat diagram explain e-commerce framework.

6B. Explain the structure of each round at the encryption site used in AES algorithm.

6C. What are the different types of digital documents?

[5+3+2]