Reg.No										

Manipal Institute of Technology

(Constituent Institute of MAHE – Deemed University)
Manipal – 576 104

SEVENTH SEMESTER B.E. (IT) DEGREE END SEMESTER MAKEUP EXAMINATION – JAN, 2007
SUBJECT: E-COMMERCE & N/W SECURITY– ICT 407.6
(REVISED CREDIT SYSTEM)

TIME: 3 HOURS **MAX.MARKS: 50**

Instructions to Candidates:

- **Answer any 5 FULL questions.**
- **All questions carry equal marks.**
- **Write neat diagrams wherever necessary**

1A. With suitable packet formats explain ESP encryption and authentication in both transport and tunnel mode.

1B. What is passive attack? Explain two types of passive attack in detail.

1C. Write a short note on Trojan horse.

(5+3+2)

2A. With an example explain data compression using ZIP algorithm.

2B. Explain any three cryptanalytic attacks on encrypted messages.

2C. Write a short note on RC5 algorithm.

(5+3+2)

3A. Explain the differences between Kerberos version 4 and version 5 with respect to the environmental shortcomings.

3B. Explain the man-in-middle attack with an example.

3C. In a public key system using RSA, intercept the cipher text C = 10 sent to a user whose public key is e = 5, n = 35. What is the plaintext M?

(5+3+2)

4A. Explain Phase 1 of handshake protocol in SSL.

4B. Briefly explain MIME transfer encodings.

4C. Briefly explain the following:

(i) PRE-AUTHENT (ii) PROXIABLE

(5+3+2)

5A. Briefly explain the packet filter router. What are its advantages and disadvantages?

5B. What is SCM? Write the characteristics of SCM.

5C. Write a short notes on Hypertext documents.

(5+3+2)

6A. Explain the online third party process in detail with a neat block diagram.

6B. Briefly describe about the different types of diffie-hellman key exchange method used in SSL handshake protocol.

6C. Briefly explain about the following e-cash related terms:

(i) blinding (ii) double spending

(5+3+2)

*****