Reg. No.										

MANIPAL INSTITUTE OF TECHNOLOGY, MANIPAL 576104

(Constituent College of Manipal University)

SECOND SEMESTER M.TECH. (S/W) DEGREE END SEMESTER EXAMINATION MAY-2016

SUBJECT: ELECTIVE I - INFORMATION SECURITY – ICT 558

(REVISED CREDIT SYSTEM)

TIME: 3 HOURS **14/05/2016** **MAX. MARKS: 50**

Instructions to candidates

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

1A. Using S-DES, decrypt the cipher text string (10100010) with 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).

1B. Is it possible in SSL for the receiver to reorder SSL record blocks that arrive out of order? If so, explain how it can be done? If not, why?

1C. Differentiate between diffusion and confusion with example.

(5+3+2)

2A. Let KEY1 be the bitwise complement of KEY. If the complement of plaintext block and key is taken then whether the result of encryption has any impact? Prove your answer with a relevant example.

2B. In an RSA System, it is given that e=13 and n=100. Encrypt the message "HOW ARE YOU" using 00 to 25 for letters A to Z and 26 for the space. Use different blocks to make p<n.

2C. What do you mean by Ethical hacking? Why is it important?

(5+3+2)

3A. Explain the working of signature based Internet Key Exchange (IKE) protocol phase 1 in main mode.

3B. Assume that Alice uses Bob's Elgamal Public key (e1=2 and e2=8) to send two messages P=17 and P1=37 using same random integer r = 9. Eve intercepts the cipher text and somehow finds the value of p=17. Show how known plaintext attack is launched by Eve to find the value of P1?

3C. What is the difference between weak and strong collision resistance?

(5+3+2)

4A. Explain the Lowe's attack on the Station to Station (STS) Protocol.

4B. Users A and B want to establish a secret key using Diffie-Hellman key exchange protocol using a common prime q= 353, a primitive root α= 3, A's secret key XA=97 and B's secret key XB=233. Compute:

i.) A's public key

ii.) B's public key

iii.) A's and B's common secret key

4C. How parallel session attack can be launched on the Woo Lam Protocol?

(5+3+2)

5A. With a neat diagram explain the working of RC5 encryption and decryption mechanism.

5B. What do you mean by Security Association? Specify the parameters that identify the Security Association.

5C. Find the possible corrupted bits in the plaintext for the following cases:

i. In Electronic Code Book (ECB) mode, bit 17 in cipher text block 8 is corrupted during transmission.

ii. In Output Feed Back (OFB) mode the entire cipher text block 11 is corrupted during transmission.

(5+3+2)

6A . Explain how HMAC and PRF is calculated in TLS with necessary diagrams.

6B. With relevant steps, discuss the approach used in Advanced Encryption Standard for key expansion.

6C. Discuss the offences and relevant sections under IT ACT 2000 with identified cybercrimes

(5+3+2)