Reg. No.										

Manipal Institute of Technology, Manipal

(A Constituent Institute of Manipal University)

VI SEMESTER B.TECH (COMPUTER SCIENCE AND ENGINEERING)

END SEMESTER EXAMINATIONS, MAY 2016

SUBJECT: CRYPTOGRAPHY AND NETWORK SECURITY [CSE 324]

REVISED CREDIT SYSTEM

11-05-2016

Time: 3 Hours MAX. MARKS: 50

Instructions to Candidates:

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

1A. Explain Vigenere Encryption. Using the Vigenere cipher, encrypt the word "explanation" with the key "leg". What is the weakness of this cipher? How it is overcome in Vernam cipher? 4M

1B. Explain the Feistel encryption and decryption techniques with neat diagram 3M

1C. Define authentication? Explain two types of authentication services. 3M

2A.Explain output feedback (OFB) mode encryption and decryption process with neat diagram. State one advantage and one disadvantage of OFB. 4M

2B. How Pseudorandom number generation is done using Block ciphers? 2M

2C. Describe the following AES transformation functions.

(i) Substitute bytes
(ii) Shift rows
(iii) Mix columns
(iv) Add round key 4M

3A. State and prove Fermat's Theorem. Using Fermat's Theorem, find $3^{201} \bmod 11$. 4M

3B. Users A and B use the Diffie-Hellman key exchange technique with a common prime q=71 and a primitive root α=7. 3M

(i) If user A has private key X_A=5, what is A's public key Y_A?
(ii) If user B has private key X_B=12, what is B's public key Y_B?
(iii) What is the shared secret key?

3C. Explain the various steps in RC4 stream cipher generation with pseudocode. 3M

4A. Define a hash function. Explain the various steps in inducing birthday attack on the hash function. 3M

4B. With neat diagram explain steps of message digest generation using SHA-512. 3M

4C. What are Message Authentication codes? Explain how MAC could be used to provide the following functions. 4M

(i) Message Authentication.

(ii) Message Authentication and confidentiality: authentication tied to plaintext

(iii) Message Authentication and confidentiality: authentication tied to ciphertext.

5A. Explain the design goals for firewall. 2M

5B. What is R64 conversion? Why R64 conversion useful for an email? 3M

5C. Explain with neat diagram overall operation of the SSL record protocol. 5M

6A. What is a computer virus? Explain the various phases that a virus undergoes during its lifetime. 3M

6B. Differentiate transport mode and tunnel mode of Ipsec. 4M

6C Explain the difference between statistical anomaly detection and rule-based intrusion detection. 3M