Reg. No.											

MANIPAL INSTITUTE OF TECHNOLOGY

MANIPAL

A Constituent Institution of Manipal University

I SEMESTER M. TECH (COMPUTER NETWORKING AND ENGINEERING)

END SEMESTER EXAMINATIONS, NOVEMBER 2017

SUBJECT: INFORMATION SECURITY [ICT 5103]

REVISED CREDIT SYSTEM
(21/11/2017)

Time: 3 Hours

MAX. MARKS: 50

Instructions to Candidates:

- Answer ALL the questions.
- Missing data may be suitably assumed.

1A. Write Diffie-Hellman key exchange algorithm. Users A and B use the Diffie-Hellman key exchange technique with a common prime $q=71$ and a primitive root $\alpha=7$.
   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 shared secret key? **(05)**

1B. Explain circuit level gateway and application level gateway highlighting their salient features used for intrusion detection. **(03)**

1C. What are the key metrics used to define disaster recovery in cloud? Explain. **(02)**

2A. List and explain the different parties involved in SET transaction. Describe the payment processing operation using SET protocol in online transaction. **(05)**

2B. Determine the multiplicative inverse of x^3+x+1 in $GF(2^4)$ with $m(x)= x^4+x+1$ **(03)**

2C. Explain challenge-response system of authentication. **(02)**

3A. With neat block diagrams, explain the directory mechanism of providing security to the objects in a computer system. List and explain the disadvantages of this technique **(05)**

3B. Compute 79^{-1} mod 1249. **(03)**

3C. Explain change cipher spec protocol in SSL. **(02)**

4A. List and explain the security problems associated with cloud computing. Also explain the design principles of cloud security. **(05)**

4B. Convert the raw data 4D61727920686164 into radix 64. (03)

4C. What is X.509 digital certificate? List the difference between different versions of X.509 digital certificate. Also mention any two applications where digital certificate is used to authenticate the users. (02)

5A. Write Kerberos version 4 authentication dialog and list the limitations. How these limitations are overcome in version 5? Explain. (05)

5B. Explain how 2-phase update protocol can be used for data consistency in a banking transaction. (03)

5C. Write a function to expand key in AES encryption algorithm. (02)