K. J. SOMAIYA INSTITUTE OF MANAGEMENT STUDIES AND RESEARCH, Vidyavihar, Mumbai- 400077

Program: ***MCA (Batch2016-19), Sem-V***
Subject: Information Security Management
(End Term Examination)

Maximum Marks: 50 **Time: 3 Hrs.** **26/11/2018**

Instructions

(1) Question No.1 is compulsory.

(2) Answer **any four** from Q.2 to Q.7.

(3) Draw diagrams wherever necessary.

(4) Mixing up the sub questions are not allowed.

(5) Basic calculator is allowed.

QUESTION 1 (Any Two) **(10 Marks)**

(a) Explain about PKI.

(b) Differentiate symmetric and asymmetric key cryptography.

(c) Explain the major protocols in SSL.

(d) Explain the architecture of IPsecurity**.**

QUESTION 2

(a) What is digital signature? What are the properties a digital signature should have? **(05 Marks)**

(b) Discuss different types of firewalls. **(05 Marks)**

QUESTION 3

Explain any two message digest algorithms in detail. **(10 Marks)**

QUESTION 4

(a) Explain reflection attack with suitable diagram. **(05 Marks)**
(b) List key features of SET. **(05 Marks)**

.

QUESTION 5

(a) With a block diagram explain the DES algorithm. **(05 Marks)**

(b) Write the steps involved in constructing a secure mail using PGP. **(05 Marks)**

QUESTION 6

(a) Explain RSA algorithm and show encryption and decryption of the following message: p=11, q=5, e=3, PT=9. **(05 Marks)**

(b) What are properties of a hashing function.Illustrate about birthday paradox problem. **(05 Marks)**

QUESTION 7

(a) Briefly explain Diffie-Hellman key exchange. Justify that Diffie Hellman key exchange is vulnerable to man in the middle attack. **(05 Marks)**

(b) Users A and B use the Diffie Hellman Key Exchange technique with a common prime $q = 71$ and primitive root $\alpha = 7$. If user A has a private key $X_A = 5$, what is A's public key Y_A. **(05 Marks)**

----------End of Paper----------