Seat No: _____ Enrollment No: _____

PARUL UNIVERSITY

FACULTY OF ENGINEERING & TECHNOLOGY

M.Tech., Summer 2017 - 18 Examination

Semester: 2 **Date: 28/05/2018**
Subject Code: 03205184 **Time: 02:00 pm to 04:30 pm**
Subject Name: Information and Network Security **Total Marks: 60**

Instructions:
1. All questions are compulsory.
2. Figures to the right indicate full marks.
3. Make suitable assumptions wherever necessary.
4. Start new question on new page.

Q.1 A) What are the key factors in designing secure encryption algorithm? Discuss them with your justification. **(05)**

B) Which scheme produces random output that bears no statistical relationship to the plaintext? What are the fundamental difficulties with them? **(05)**

C) Give the Feistel cipher structure and give its design criteria. **(05)**

Q.2 **Answer the following questions**. (Attempt any three) (Each five mark) **(15)**

A) What is HMAC

B) Explain following terms:

Non repudiation, Buffer overflow, Incomplete Mediation, Race Conditions, Malware

C) Explain Key generation algorithm in AES

D) Explain RC4 algorithm.

Q.3 A) Explain X.509 Certificates with diagram. Justify the need of digital Certificates. **(07)**

B) Explain a method of exchanging symmetric key using asymmetric method. **(08)**

OR

B) Explain RSA algorithm. In a public-key system using RSA, you intercept the cipher text C = 10 sent to a user whose public key is e = 5, n = 35.What is the plaintext M **(08)**

Q.4 A) Explain Secure Hash Algorithm (SHA-512) in detail. What is its requirement? **(07)**

OR

A) Write a short note on ElGamal Digital Signature Scheme. **(07)**

B) What is Extended Euclidian Algorithm? Find multiplicative inverse of 550 in GF(1759) **(08)**