Seat No: _____ Enrollment No: _____

PARUL UNIVERSITY

FACULTY OF ENGINEERING & TECHNOLOGY

M.Tech. Winter 2017 - 18 Examination

Semester: 1 **Date: 04/01/2018**
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) Draw and explain HMAC. **(05)**

B) List out block cipher modes of operations and explain any one in detail. **(05)**

C) Use Playfair cipher substitution technique and find out cipher text for the following given key and plaintext. **(05)**

Key = HELLOWORLD

Plaintext=HIDE THE GOLD

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

A) Discuss man in the middle attack in Diffie-Hellman key exchange.

B) Write the necessary condition to satisfy Groups, Rings and Fields.

C) Find the Inverse of integer value 31 when mod value is 3480 with Extended Euclid Algorithm.

D) List out type of attacks and explain any two active security attacks.

Q.3 A) Discuss SHA-1 in detail. **(07)**

B) Explain DES key generation process in detail. **(08)**

OR

B) Explain various steps of AES. **(08)**

Q.4 A) Discuss X.509 Certificate in detail. **(07)**

OR

A) Discuss Elliptic Curve Cryptography. **(07)**

B) Explain the concept of Digital Signature and discuss Digital Signature Standard. **(08)**