Seat No:______________ **Enrollment No:______________**

PARUL UNIVERSITY

FACULTY OF IT & COMPUTER SCIENCE

BCA/ IMCA Summer 2018 – 19 Examination

Semester: 5	**Date: 26/10/2018**
Subject Code: (05101304/ 05301304)	**Time: 02:00pm to 04:30pm**
Subject Name: Network Security	**Total Marks: 60**

Instructions:

1. All four 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 Answer the followings.(All are compulsory)

A. Write in one or two lines. **(05)**

1. What is firewall?
2. What is cryptography?
3. What is cipher text?
4. What is decryption?
5. What is data communication network?

B. Give the sentence true or false. (Each of 01 marks and all are compulsory) **(10)**

1. Decryption is reverse process of encryption.
2. Passive attack means no modification.
3. Plain text means converted message of sender.
4. Confidentiality is related with non disclosure of anything.
5. Stream cipher mean process of bit by bit process.
6. Asymmetric key cryptography means single key has been used.
7. Full form of DES : Data Encryption System
8. DES is having 16 round of procedure.
9. AES generates 64 bit block ciphertext.
10. Firewall is software which can control the incoming and outgoing traffic.

Q.2 Answer the followings. (3 Mark Questions.) (Any five) **(15)**

1. Draw feistel structure and give short explanation.
2. Explain symmetric key and asymmetric key encryption with figure.
3. Explain bifurcation of cryptography methods according to keys , methods , process.
4. Explain block chaining modes.(Any three)
5. Explain 3DES in detail with justification.
6. Explain digital signature with figure.

Q.3 Answer the following. (Any three) **(15)**

1. Explain RSA algorithm with its steps of encryption and decryption.
2. Write a short note on Hash function.
3. Draw figure of Public key infrastructure with short explanation of its components.
4. Write a short note on IPsec.

Q.4 Answer the following.

A. Write a short note on DES. **(05)**

B. Write a short note on AES. **(10)**

OR

B. Write a short note on OSI security architecture with its three components. (Attacks, services and mechanism) **(10)**