Seat No: _____ **Enrollment No: _____**

PARUL UNIVERSITY

FACULTY OF IT & COMPUTER SCIENCE

BCA Summer 2017 – 18 Examination

Semester: 5 **Date: 06/06/2018**
Subject Code: 05101304 **Time: 02: 00 pm to 04: 30 pm**
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.

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

1. What is cryptography?
2. What is virus?
3. What is cipher text?
4. What is plain text?
5. What is encryption?

B) Give the sentence true or false. **(10)**

1. Encryption means converting cipher text into plain text.
2. Active attack means no modification.
3. Cryptography means study of breaking cipher text.
4. Integrity is ensuring modification.
5. Cryptology contains two fields.
6. Symmetric key cryptography means single key has been used.
7. Block cipher means process on group of bits.
8. DES is having 16 round of procedure.
9. Phishing is the attempt to obtain sensitive information.
10. Firewall is software which cannot control the incoming and outgoing traffic.

Q.2 Answer the followings. (Attempt any 5) **(15)**

1. Explain CIA model in detail.
2. Explain symmetric key and asymmetric key encryption schemes in detail.
3. Explain feistel structure in detail.
4. Explain MAC in detail.
5. Explain 3DES in detail.
6. Explain VPN in detail.

Q.3 Answer the following. (Attempt any 3) **(15)**

1. Write a short note on digital signature
2. Write a short note on hash function.
3. Write a short note on AES algorithm.
4. Write a short note on 5 block chaining modes.

Q.4 Answer the following.

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

B) Write a short note on public key infrastructure. **(10)**

OR

B) Do encryption and Decryption with RSA algorithm with below mentioned details **(10)**
p=7 and q=11 (e=13 , m=2)