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

# PARUL UNIVERSITY

## FACULTY OF IT & COMPUTER SCIENCE

## BCA Summer 2018 – 19 Examination

**Semester: 5** **Date: 08/05/2019**
**Subject Code: 05101304** **Time: 10.30 am To 1.00 pm**
**Subject Name: 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 Answer the followings.**

**A. Write short notes.** **(05)**

1. Define : Confidentiality
2. Define : Cryptography
3. Define: Digital Signature
4. Define: Trojan Horse
5. Define: Denial of service

**B. Multiple choice type questions/ Give the sentence true or false. (Each of 01 marks)** **(10)**

1. In asymmetric key cryptography, the private key is kept by whom when A is sending message to B_____
   a) A
   b) B
   c) Both
   d) all the connected devices to the network
2. Message must be encrypted at sender side and decrypted at the
   a) Sender Side
   b) Site
   c) Receiver side
   d) Conferencing
3. MAC stands for
   a) Message authentication code
   b) Message arbitrary connection
   c) Message authentication control
   d) Message authentication cipher
4. Data encryption standard (DES) is _____type of algorithm?
   a) block cipher
   b) stream cipher
   c) bit cipher
   d) none of the mentioned
5. AES uses a _____ bit block size and a key size of _____ bits in 12 round.
   a) 128; 128
   b) 64; 128
   c) 256; 128
   d) 128; 192
6. Like DES, AES is also uses Feistel Structure.
   a) True
   b) False

7. Cryptanalysis is used_____
   a) to find some insecurity in a cryptographic scheme
   b) to increase the speed
   c) to encrypt the data
   d) none of the mentioned
8. Find the correct-option for the following plaintext_____
   HQFUBSWHG WHAW
   a) ABANDONED LOCK
   b) ENCRYPTED TEXT
   c) ABANDONED TEXT
   d) ENCRYPTED LOCK
9. Caesar Cipher is an example of
   a) Poly-alphabetic Cipher
   b) Mono-alphabetic Cipher
   c) Multi-alphabetic Cipher
   d) Bi-alphabetic Cipher
10. DES follows_____
   a) Hash Algorithm
   b) Caesars Cipher
   c) Feistel Cipher Structure
   d) SP Networks

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

1. Explain message authentication code.
2. Explain block cipher and stream cipher.
3. Explain hash function.
4. Explain the triple DES scheme and justify reason for encryption decryption encryption.
5. Explain Digital Signature.
6. Explain OSI attacks.

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

1. What is security Services? Explain any three types of security services.
2. Explain Symmetric and Asymmetric Cryptography.
3. Calculate cipher text in case of RSA if p=3, q=11,e=3,M=5.
4. Explain IPsec with its mode.

**Q.4 Answer the following.**

A. Explain network security model with cryptography. **(05)**

B. Explain feistel structure with example and write short note on DES. **(10)**

**OR**

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