Enrol. No. | S | R | H | U | | | | | | | | | Regn. No. | D | D | | | | | | | | | | |

END SEMESTER EXAMINATION, JUNE - 2019
BCA SIXTH SEMESTER

COURSE CODE: BCA308 **COURSE TITLE: NETWORK SECURITY**

[Time allotted: Three hours] **[Max. Marks: 100]**

Note: *Attempt all Sections & Questions.*

Section (A)

Q.1. Attempt all questions. **(2 x 10 = 20)**

a. What does it mean to say that b is a divisor of a?
b. What are the roles of the public and private key?
c. What is the difference between modular arithmetic and ordinary arithmetic?
d. What is the difference between a block cipher and a stream cipher?
e. What is the purpose of the X.509 standard?
f. What is steganography?
g. Explain the SSL handshake protocol.
h. What is Euler's totient function?
i. What is a primitive root of a number?
j. What is a message authentication code?

Section (B)

Q.2. Attempt any 5 questions. **(7 x 5 = 35)**

a. Using the Vigenere cipher, encrypt the word 'cryptography' using the key 'house'.
b. What is the purpose of the S-boxes in DES?
c. Why is SHA more secure than MD5? Explain.
d. Determine- **(4+3)**
i) gcd(36939, 15246) **ii)** gcd(5264, 15472)
e. What is firewall? Explain Packet filters firewall with a diagram.
f. What services are provided by the SSL Record Protocol?
g. What is digital signature? What requirements should a digital signature scheme satisfy?

Section (C)

Attempt any 3 questions. **(15 x 3 = 45)**

Q.3. **a.** Differentiate between active attacks and passive attacks. **7**
b. What is a 'warm'? What is the significant difference between a 'warm' and a 'virus'? **8**

Q.4. **a.** Briefly explain Diffie-Hellman key exchange. **8**
b. What is an elliptic curve? What is the zero point of an elliptic curve? **7**

Q.5. **a**. What characteristics are needed in a secure hash function? **7**
b. What is the role of a compression function in a hash function? **8**

Q.6. **a.** Using Fermat's theorem, find 5^{301} mod 11. **7**
b. In a public-key system using RSA, you intercepted the ciphertext C = 8 sent to a user whose public key is e = 13, n = 33. What is the plaintext M? **8**

Q.7. **a.** What entities constitute a full-service Kerberos environment? Briefly describe the overview of Kerberos. **10**
b. In the context of Kerberos, what is a realm? **5**

****