

Roll No.

BCA-601(N)

B. C. A. (Sixth Semester) EXAMINATION, Sept., 2020

(New Course)

Paper First

COMPUTER NETWORK SECURITY

Time : Three Hours]

[Maximum Marks : 75

Note : Attempt questions from all Sections as directed.

Inst. : The candidates are required to answer only in serial order. If there are many parts of a question, answer them in continuation.

Section—A

(Short Answer Type Questions)

Note : All questions are compulsory. Each question carries 3 marks.

1. (A) Explain the following terms :
 - (i) Access control
 - (ii) Data confidentiality
- (B) Write in short about different types of possible active attacks.

P. T. O.

- (C) What is a transposition cipher ? Explain with an example.
- (D) What do you understand by Network Security Attack ?
- (E) Explain the term Denial of Service.
- (F) Write short notes on public keys and private keys.
- (G) Write the difference between block cipher and stream cipher.
- (H) List the properties of Modulo operator.
- (I) Define a group with its properties.

Section—B

(Long Answer Type Questions)

Note : Attempt any *two* questions. Each question carries 12 marks.

- 2. Explain RSA algorithm with example.
- 3. "Authentication, integrity, non-repudiation is achieved using public key encryption technique." Justify the statement.
- 4. Explain Hill Cipher, Caesar Cipher and Affine Cipher in details.
- 5. Explain the difference between AES and DES Ciphers.

Section—C

(Long Answer Type Questions)

Note : Attempt any *two* questions. Each question carries 12 marks.

- 6. What are security protocols ? Discuss *four* benefits of IPSec as a security protocol.

[3]

7. What do you mean by firewalls ? Discuss the need of firewall in VPN along with its types.
8. Explain the type of encryption/decryption method. Differentiate between symmetric and asymmetric encryption.
9. What is Kerberos ? Explain Kerberos authentication system.
10. Explain the SNMP architecture in detail.