

Roll No. 6002842

BCA-601(N)

B. C. A. (Sixth Semester) EXAMINATION, May, 2019

(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

2 each

Note : All questions are compulsory.

1. What are *four* categories of active attacks ? Just name them.
2. What are different types of data confidentiality ?
3. What do you understand by Non-repudiation ?
4. What do you understand by Cipher ? What is block cipher ?

Section—B

8 each

Note : Attempt any *seven* questions from this Section.

5. What are technical deficiencies of Kerberos ver. 4 ?

(A-95) P. T. O.

[2]

6. Compare various threats ; on the web, their consequences and countermeasures against them.
7. What services Pretty Good Privacy (PGP) provides ? Elaborate them
8. What is Intrusion ? How is it detected ?
9. What is secure hash function ? What properties should it possess ?
10. What are the various types of attacks on encrypted message ? Explain in details.
11. Explain Diffie-Hellman Key Exchange.
12. Explain triple DES (3DES).
13. What are different types of Firewalls ? Explain all in short.

Section—C

11 each

Note : Attempt any *one* question from this Section.

14. What do you understand by IPSecurity (IPSec.) ? What are its applications and benefits ?
15. Explain in detail the handshake protocol. What key exchange methods are supported ?

BCA-601(N)

2,000

(A-95)