EVN–2700

B.C.A. VI Semester
Session 2023–24

NETWORK SECURITY

Paper : II (BCA–602)

Time : 2:30 Hours]   [Max. Marks : 70

Note : Attempt any *five* questions. All questions carry equal marks.

Q. 1. (a) Explain the Various attacks.

     (b) What is firewall ? How does it works ?

Q. 2. (a) Discuss Digital Signature.

     (b) What do you mean by Cryptography ? List Various techniques.

Q. 3. (a) Specify the four categories of security threats.

     (b) Why network need security ?

Q. 4. (a) Compare Subsititution And Transpostion.

     (b) Explain the Palyfair cipher and Vernam cipher in details.

Q. 5. (a) Explain the OSI security architecture.

     (b) Define integrity and non repudiation.

Q. 6. (a) Explain Data Encryption Standard (DES) in detail.

     (b) Explain RSA algorithm in detail with an example.

Q. 7. (a) Explain (any *two*) of the following :

     (i) ceaser cipher

     (ii) Mono alphabetic cipher 3.one time pad cipher

     (b) Define the classes of message authentication function. Message encryption : The entire cipher text would be used for authentication. Message Authentication Code : It is a function of message and secret key produce a fixed length value. Hash function : Some function that map a message of any length to fixed length which serves as authentication.

****