

H

Roll No.

TBC-603/TBI-604

**B. C. A./B. SC. (IT) (SIXTH SEMESTER)
MID SEMESTER**

EXAMINATION, April, 2023

NETWORK SECURITY AND CYBER LAWS

Time : 1½ Hours

Maximum Marks : 50

Note : (i) Answer all the questions by choosing any *one* of the sub-questions.

(ii) Each sub-question carries 10 marks.

1. (a) What is network security ? Why network security is required ? Explain about the security services. (CO1)

OR

- (b) Explain about convention encryption model in detail. (CO1)
2. (a) What do mean by Block Cipher ? Explain Block Cipher principles. (CO1-2)

P. T. O.

(2) TBC-603/TBI-604

OR

- (b) In a RSA cryptosystem, the public key of a given user is $e = 17$ $n = 3937$, calculate the private key of this user. Encrypt the message M-15. Show with decryption, how the receiver will get the original message ? (CO1-2)
3. (a) What is Public-Key Cryptography ? Illustrate the principles of Public-Key Cryptosystems. (CO2)

OR

- (b) State the difference between block cipher and stream cipher. (CO2)
4. (a) With suitable example, explain the RSA Algorithm in detail. (CO3)

OR

- (b) List the block cipher modes of operation and explain any *one* block cipher modes of operation. (CO3)

(3)

5. (a) What are the various key distribution methods in key management ? Explain key distribution method. (CO4)

OR

- (b) Write short notes on the following : (CO4)
- (i) Steganography
 - (ii) DES
 - (iii) Modern Block Ciphers