OR

(b) "Man in the middle attack" is one major weakness of public key cryptosystems. If yes then why, if not then why not ?

10 Marks (CO1/CO2)

5. (a) ATM are designed so that users will provide a PIN no. and a card to access their bank accounts. Describe the degree of importance of confidentiality, integrity and authentication associated in such system and possible security mechanisms to enhance them. 10 Marks (CO1/CO2)

OR

(b) What are the elements of key management in public key cryptography ? Explain in brief. 10 Marks (CO1/CO2)



H Roll No. .....

# TBC–603/TBI–604

## B. C. A./B. SC. (IT)

## (SIXTH SEMESTER)

## MID SEMESTER EXAMINATION,

## April/May, 2022

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 question carries 10 marks.

1. (a) What is the concern any network will feel after a threat and an attack ? Differentiate. Explain which one going to harm the system the most in detail.

10 Marks (CO1/CO2)

*P. T. O.*

OR

(b) If A is encrypting a message by B's public key and B is decrypting the same with its own private key, what form of cryptography is being done in this scenario ? Explain in detail.

10 Marks (CO1/CO2)

2. (a) If the input bit block is 64 and the key is 21, generate the cipher text by using s-des algorithm. 10 Marks (CO1/CO2)

OR

(b) What is asymmetric key encryption ? Explain in detail, what are the benefits it provides over symmetric key encryption.

10 Marks (CO1/CO2)

3. (a) What is the significance of permutation and substitution phase in DES algorithm ? Which one is used in initial rounds and why ? Explain in detail.

10 Marks (CO1/CO2)



OR

(b) What was the main reason behind generating public key cryptosystems ? Explain in detail. Which part of security services going to be affected in these systems ? 10 Marks (CO1/CO2)

4. (a) In an organization the main server is getting requests from many users and responding hem simultaneously, but after some time the system went into a halt state affecting the whole working of a firm. To overcome this the firm started allowing one request at a time from a user to the main server but after some time the system again went into halt state.

10 Marks (CO1/CO2)

(a) What is the main reason behind system halt in both cases ? Explain.

(b) How both the scenarios going to affect the information system ? Differentiate in points.