KLS Gogte Institute of Technology, Belagavi
Department of Computer Science and Engineering

Internal Assessment Test I

Academic Year: 2020-21 **Subject: Information and Network security (18CS652)**
Semester: VI (PE) **Max. Marks: 25** **Duration: 1 Hr 15 Mins** **Date: 2/6/2021**

NOTE: ANSWER ANY FIVE QUESTIONS (5*5=25)

DRAW DIAGRAMS WHEREVER NECESSARY

1. Apply Playfair Cipher to encrypt and decrypt the message "**BREAK THE COVID CHAIN**" using "**STAYHOMESTAYSAFE**" as key. [L3,CO1,PO1]

2. Apply Hill Cipher to get the plain text from " **CEMTQIVQ**" using key [L3, CO1, PO1]

3. Describe the **Feistel** Encryption process**.** [L2,CO1,PO1]

4. Construct the public key cryptosystem model for **sender C** and **receiver D** to provide **authentication** and **secrecy.** [L3, CO2, PO1]

5. Apply double transposition technique to encrypt the message **"HIDE THE GOLD IN THE TREE STUMP"** using "**3 1 2 5 6 7 4"** as key. [L3,CO1,PO1]

6. Explain the key ingredients of public-key encryption. [L2,CO2,PO1]

7. Explain the possible approaches to attack the RSA algorithm. [L2,CO3,PO1]