THADOMAL SHAHANI ENGINEERING COLLEGE

T.E. Sem V- IT (July-December 2022)

COMPUTER NETWORK SECURITY

PT1- Question Bank

1.	Define the terms: Vulnerability, threat and attack	CO1
2.	Define the security goals.	CO1
3.	List the attacks threatening confidentiality.	CO1
4.	Numericals on Playfair Cipher, Vigenère Cipher , Transposition cipher, RSA	CO1, CO2
5.	Define any five security mechanisms you have studied.	CO1
6.	Draw and explain the internal structure of single round of DES algorithm.	CO2
7.	Differentiate between DES and AES.	CO2
8.	Differentiate between block cipher and stream cipher.	CO1
9.	Compare cryptography and steganography.	CO1
10.	Explain with diagram the steps of Digital Signature Generation and verification	CO2
11.	Classify the cryptosystem into various categories and name at least one algorithm in each category.	CO1
12.	Compare Asymmetric and symmetric cryptosystem	CO1
13.	Describe the key generation process in RSA.	CO2
14.	With a neat diagram explain CBC/CFB/OFB/Counter mode of operation of a block cipher. State its advantages and disadvantages if any.	CO2
15.	With a neat diagram explain the structure of one round of AES.	CO2

Dr. Shachi Natu
(Subject Incharge)