

ASSIGNMENT-1

SUBJECT: INFORMATION AND NETWORK SECURITY

BRANCH: COMPUTER ENGINEERING

SEMESTER: 7

Questions		Learning Level	Marks
Q.1	Define the following terms: a. Data Confidentiality b. Non-repudiation c. Authentication d. Data integrity	U	4
Q.2	Use the Playfair cipher to encipher the message "The key is hidden under the door pad" using the key "GUIDANCE".	A	5
Q.3	Encrypt the message "Money helps to build infrastructure" using the hill cipher with key [9 4 , 5 7] Show your calculations and results.	A	3
Q.4	Using Vigenère cipher, encrypt the word "cryptography" using the key "house".	A	3
Q.5	How security of polyalphabetic cipher is improved over monoalphabetic cipher?	N	4
Q.6	What are the differences between block ciphers and stream ciphers? Explain block ciphers principals in brief.	N	3
Q.7	What is the difference between diffusion and confusion?	U	3