CHAROTAR UNIVERSITY OF SCIENCE AND TECHNOLOGY		
DEPARTMENT OF COMPUTER SCIENCE AND TECHNOLOGY		
CSE312: CRYPTOGRAPHY AND NETWORK SECURITY		
ACADEMIC YEAR: 2024-25		
CIE - 1		
Total Marks : 50 , Effective Marks : 10		
1	Encrypt the plaintext "HELP" using the Hill cipher with the key matrix: $K = \begin{vmatrix} 6 & 24 & 1 \\ 13 & 16 & 10 \\ 20 & 17 & 15 \end{vmatrix}$ Using the cipher text, Recover the original plaintext.	3
2	If the ciphertext "WKVUIBGKP" was encrypted using a Vigenère cipher with a key length of 3, describe the steps to identify the key.	3
3	Construct a Playfair cipher matrix with the keyword "SECURITY" (excluding 'J') and encrypt the plaintext "HELLO WORLD". Explain the steps in detail.	3
4	The ciphertext "BMODZBXDNABEKUDMUIXMMOUVIF" was encrypted using the Playfair cipher with the key "MONARCHY". Decrypt the ciphertext and recover the original plaintext.	3
5	Let message = “Anna”, and k = 3, find the ciphertext using Caesar.	2
6	Demonstrate encryption and decryption process in hill cipher. Consider m = “sh” and key = hill”.	3
7	Encrypt the message “this is an exercise” using additive cipher with key = 20. Ignore the space between words. Decrypt the message to get the original plaintext.	3
8	What is a monoalphabetic cipher? Examine how it differs from Caesar cipher	3
9	Differentiate between monoalphabetic substitution and polyalphabetic substitution with example.	3
10	Using rail fence cipher, encrypt the text “meet me after the toga party” using the key 4 3 1 2 5 6 7	3
11	Use playfair cipher to encrypt the message “THE HOUSE IS BEING SOLD TONIGHT’’ with the key ‘GUIDANCE’.	3

12	Encrypt the text “CRNS” using Hill Cipher with the key K = 9 4 5 7	3
13	Use Autokey system of Vigenere cipher to encrypt the message “meet me after the toga party” using the key “largest”.	3
14	Using double stage columnar transposition technique, encrypt the text “Cryptography and Network Security” using the key “43125”.	3
15	A message is encrypted first using a Caesar cipher with a shift of 3, and then the resulting cipher-text is encrypted using a columnar transposition cipher with the key **"SECRET"**. The plaintext is: THE QUICK BROWN FOX Task: - Encrypt the plaintext step-by-step. Provide the final Cipher-text. Decrypt the Cipher-text and verify your result.	3
16	Investigate and write a report (500 words) on how substitution and transposition ciphers were used in World War II. Provide examples and analyse their effectiveness.	3
17	Explore how frequency analysis and Kasiski examination can be applied to break substitution and polyalphabetic ciphers. Include practical examples in your explanation.	3