2170709 – Information and Network Security

B.E Semester: 7 – IT (GTU)

Unit – 1

1	Explain data confidentiality, data authentication and data integrity
2	Describe mono alphabetic cipher.
3	Explain playfair cipher with example.
4	Explain one time pad cipher with example. Explain the one time pad scheme.
5	Explain columnar transposition Cipher technique.
6	Briefly explain any two active security attacks.
7	Discuss the following terms in brief: - brute force attack – cryptography
8	• Explain playfair cipher substitution technique in detail. Find out cipher text for the following given key and plaintext. Key = ENGINEERING Plaintext=COMPUTER • Let the keyword in playfail cipher is "keyword". Encrypt a message "come to the window" using playfair cipher. • ExplainPlayfair Cipher in detail. Find out cipher text for the following given plain text and key. Key = GOVERNMENT Plain text = PLAYFAIR • Construct a Playfair matrix with the key "engineering". And encrypt the message "test this process". • Construct a playfair matrix with the key "occurrence". Generate the cipher text for the plaintext "Tall trees" • Using playfair cipher encrypt the plaintext "Why, don't you?". Use the key "keyword". • Encrypt the Message "Surgical Strike" with key "GUJAR" using PLAYFAIR technique. • Encrypt the following message using playfair cipher. Message: COMSEC means communications security Keyword: Galois • Construct 5 X 5 playfair matrix for the keyword "OCCURANCE".
9	Write differences between substitution techniques and transposition techniques.
10	(1) Discuss the following terms in brief. - authentication - data integrity
11	What are the principal elements of public-key cryptosystem? Explain in brief.
12	Define Cryptography and Cryptanalysis. Draw and explain conventional cryptosystem.
13	List and explain various types of attacks on encrypted message.
14	Given key K= $\begin{bmatrix} 17 & 17 & 5 \\ 21 & 18 & 21 \\ 2 & 2 & 19 \end{bmatrix}$ and plaintext ="ney". Find out the ciphertext applying Hill Cipher. Is Hill cipher strong against ciphertext only attack or known plaintext attack? Justify the answer. **07**
15	How cryptanalyst can exploit the regularities of the language? How digrams can solve this problem? Use the key "hidden" and encrypt the message "Message" using playfair cipher.

Prof. Priyanka Panchal
Assistant Professor
IT Dept.,
MBIT