

	Harcourt Butler Technical University Kanpur			I MID SEM (2023-24)		
Branch	MCA		Program	MCA		
Course Name	Cryptography and Network Security		Semester	IV		
Course Code	ECA-582		Year	II		
Time:	1.00 Hr		Maximum Marks	15		
Knowledge Level (KL)	K1: Remembering	K3: Applying		K5: Evaluating		
	K2: Understanding	K4: Analyzing		K6: Creating		
Note: Answer All Questions						
Q. No	Questions			Marks	COs	KL
1	Discuss about Playfair cipher technique? Let the plaintext is “COMMUNICATION” and the keyword is “COMPUTER”, find ciphertext using Playfair technique.			3	CO1	K3
2	Differentiate between Electronic Code Book (ECB) and Cipher Block Chaining (CBC) modes of operation.			3	CO1	K4
3	Draw a block diagram of DES (Data Encryption Standard) algorithm. Also explain its functionality.			4	CO1	K2
4	Find the GCD of (2740, 1760) using Euclid’s Algorithm.			2	CO2	K3
5	Discuss about Euler’s and Fermat’s theorem with example.			3	CO2	K2

Course Outcomes	CO1	Understand and deploy cryptographic technique to secure data in networks
	CO2	Analyze the vulnerabilities in any computing systems and design a security solution.
	CO3	Understand and use standard algorithms for confidentiality, integrity and authenticity.
	CO4	Apply various key distribution and management schemes in network system.
	CO5	Apply security protocols in various IT applications.