	Harcourt Butler Technical University **Kanpur**		**END** **SEM** **EXAM** **(2023-24)**
Branch	**MCA**	Program	**MCA**
Course Name	**Cryptography and Network Security**	Semester	**IV**
Course Code	**ECA-582**	Year	**II**
Time	**02:30 Hr**	Maximum Marks	**50**

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	**Attempt both questions.**			
(a)	Discuss the two problems with the one-time pad?	**2**	**CO1**	K2
(b)	Differentiate between block cipher and stream cipher?	**2.5**	**CO1**	K4
(c)	Explain the purpose of S-boxes in DES.	**2.5**	**CO1**	K2
(d)	Discuss the modes of operations of block cipher.	**3**	**CO1**	K2
2.	**Attempt both questions.**			
(a)	Briefly explain RSA algorithm. In a public key system using RSA, the intercepted ciphertext C=10 sent to a user whose public key is e=5, n=35. What is the plaintext M?	**5**	**CO2**	K5
(b)	Explain the essential requirements that must a public key cryptosystem fulfill to be a secure algorithm? Also, discuss three broad categories of applications of public key cryptosystem.	**5**	**CO2**	K4
3.	**Attempt both questions.**			
(a)	Explain the sequence of steps to create message digest using SHA-512 (Secure Hash Algorithm) algorithm with suitable diagram.	**5**	**CO3**	K3
(b)	Why Message Authentication is required? Discuss working of MAC (Message Authentication Code) with suitable block diagram.	**5**	**CO3**	K2
4.	**Attempt both questions.**			
(a)	Explain Digital Certificate? Give the format of X.509 certificate showing the important elements of the certificate. How is an X.509 certificate revoked?	**5**	**CO4**	K4
(b)	Explain the sequence of steps involved in the message generation and reception in Pretty Good Privacy (PGP) with block diagram.	**5**	**CO4**	K2

5.	**Attempt both questions.**			
(a)	Briefly describe the sequence of events that are required for a Secure Electronic Transaction (SET). Also discuss the concept of dual signature in context of SET.	**5**	**CO5**	K3
(b)	Elaborate the term ‘system security’? Also discuss viruses and related threats to system security.	**5**	**CO5**	K4

Course Outcomes	**CO1**	Understanding and deploy cryptographic techniques to secure data in networks
	CO2	Analyze the vulnerabilities in any computing system 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.