CBCS SCHEME

USN | | | | | | | | | | |

22MCA261

Second Semester MCA Degree Examination, Dec.2023/Jan.2024
Cryptography and Network Security

Time: 3 hrs. Max. Marks: 100

Note: 1. Answer any FIVE full questions, choosing ONE full question from each module.
2. M : Marks , L: Bloom's level , C: Course outcomes.

		Module – 1	M	L	C
Q.1	a.	List and explain the specific security mechanisms.	10	L1,2	CO1
	b.	Describe one time pad substitution with an example.	6	L2	CO1
	c.	Write a note on steganography.	4	L1	CO1
		OR			
Q.2	a.	With a neat diagram, explain the model of network security.	6	L2	CO1
	b.	List and explain OSI security services.	10	L1,2	CO1
	c.	Encrypt the message RESOURCE, with key MONARCHY using play fair cipher.	4	L3	CO1
		Module – 2			
Q.3	a.	With a neat diagram, explain the DES algorithm.	10	L2	CO2
	b.	Discuss double DES and triple DES. Also explain the meet in the middle attack.	10	L2	CO2
		OR			
Q.4	a.	Explain electronic code book mode and cipher block chaining modes of DES.	10	L2	CO4
	b.	Explain feistal cipher structure for encryption. Also list the parameters and design features.	10	L2	CO2
		Module – 3			
Q.5	a.	How Millar-Rabin algorithm is used for primality testing? Test n = 29 using the same for primality.	10	L4	CO2
	b.	Describe the RSA algorithm.	6	L2	CO3
	c.	Find $\phi(1000)$.	4	L3	CO3
		OR			
Q.6	a.	Consider q = 23, α = 5, X_A = 3, X_B = 7, Find the secret key using diffie hellman key exchange. Also explain the man in the middle attack.	10	L3	CO3
	b.	Perform the encryption and decryption using RSA algorithm of p = 17, q = 11, d = 23 and M = 10.	10	L3	CO3
		Module – 4			
Q.7	a.	List and explain message authentication requirements and functions.	10	L1,2	CO4
	b.	Explain message digest generation using SHA – 512.	10	L2	CO4
		OR			
Q.8	a.	What is MAC? Explain the basic uses of MAC using diagram.	10	L2	CO4
	b.	What is Hash value? Explain the two simple hash functions.	10	L2	CO4

Module – 5					
Q.9	**a.**	Describe the X.509 certificate format.	**10**	**L2**	**CO5**
	b.	Discuss the digital signature algorithm.	**10**	**L2**	**CO5**
OR					
Q.10	**a.**	Explain the key distribution scenario with a neat diagram.	**10**	**L2**	**CO5**
	b.	Discuss the Schnorr digital signature scheme.	**10**	**L2**	**CO5**

* * * * *