CBCS SCHEME

USN | | | | | | | | | |

22MCA261

Second Semester MCA Degree Examination, June/July 2023
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.	Explain different cipher methods for plaintext cryptography, obtain the ciphertext for substitution cipher 1 using 4 characters.	10	L2	CO1
	b.	Define security services. Explain the different categories and services of security services.	10	L2	CO1
		OR			
Q.2	a.	Explain any two substitution techniques with example.	10	L2	CO1
	b.	With neat diagram, explain a model for Network Security.	10	L2	CO1
		Module – 2			
Q.3	a.	With neat diagram, explain classical Feistel Network.	10	L2	CO2
	b.	Explain Data Encryption Standard (DES) with example.	10	L2	CO2
		OR			
Q.4	a.	Explain Block Cipher design principles.	10	L2	CO2
	b.	Describe in detail Deffie – Hellman key exchange algorithm.	10	L2	CO2
		Module – 3			
Q.5	a.	i) Explain Euler's Theorem with example ii) Describe Fermat's Theorem.	10	L2	CO3
	b.	Explain Chines Remainder Theorem solve the problem for Chines remainder where $X \equiv 3 \mod 4$ $X \equiv 2 \mod 2$ $X \equiv 4 \mod 5$	10	L2	CO3
		OR			
Q.6	a.	Perform encryption and decryption algorithm using RSA algorithm for the following : $p = 3 ; q = 11 ; e = 7 ; \mu = 5$ $p = 5 ; q = 11 ; e = 3 ; \mu = 9$	10	L2	CO3

	b.	List and explain principles of public key cryptosystems.	10	L2	CO3
		Module – 4			
Q.7	a.	Explain Secure Hash Algorithm (SHA).	10	L2	CO4
	b.	With neat diagram explain Hash function.	10	L2	CO4
		OR			
Q.8	a.	With neat diagram, explain Message Authentication Function.	10	L2	CO4
	b.	Explain the two security of MACS.	10	L2	CO4
		Module – 5			
Q.9	a.	With neat diagram, explain Generic model of Digital signature process.	10	L2	CO5
	b.	With a neat diagram, explain DSS approach.	10	L2	CO5
		OR			
Q.10	a.	Explain key distribution scenario for transport key control scheme.	10	L2	CO5
	b.	Explain the technique used for distribution of public keys.	10	L2	CO5

* * * * *