Reg. No. : | | | | | | | | | | | | |

Question Paper Code: U7202

B.E./B.Tech. DEGREE EXAMINATION, NOV 2024

Seventh Semester

Computer Science and Engineering

21UCS702-CRYPTOGRAPHY AND CYBER SECURITY

(Regulations 2021)

Duration: Three hours | Maximum: 100 Marks

PART A - (10 x 2 = 20 Marks)

1.	Define cryptography.	CO1 -U	
2.	Define Steganography.	CO1 -U	
3.	Write the Euclidean Algorithm.	CO1 -U	
4.	Explain Hierarchical Multiple KDCs.	CO1 -U	
5.	Why is asymmetric cryptography bad for huge data? Specify the reason.	CO1 -U	
6.	State Fermat's little theorem.	CO1 -U	
7.	Create a simple authentication dialogue used in Kerberos.	CO1 -U	
8.	Define the term message digest.	CO1 -U	
9.	Which are the elements of cyber crime?	CO1 -U	
10.	List the need for information Security.	CO1 -U	

PART – B (5 x 16= 80 Marks)

11.	(a)	Explain the Characteristics of Modern Cryptography and working Principle.	CO1 -U	(16)	
		Or			
	(b)	(i) Discuss the substitution Techniques in detail.(8)	CO1 -U	(16)	
		(ii) Discuss the Transposition Techniques in detail.(8)			
12.	(a)	Describe Modulo Arithmetic operations and properties in detail.	CO1 -U	(16)	
		Or			
	(b)	Describe DES algorithm with neat diagram and explain the steps.	CO1 -U	(16)	

13.	(a)	Perform encryption and decryption using RSA algorithm for p=17, q=11,e=7 m=88.	CO2 -App	(16)
		Or		
	(b)	Users A and B use the Diffie-Hellman key exchange technique, a common prime q=11 and a primitive root alpha=7. Calculate the shared secret key.	CO2 -App	(16)
14.	(a)	Explain in detail about X.509 authentication services	CO1 -U	(16)
		Or		
	(b)	Explain Client Server Mutual authentication with example flow diagram.	CO1 -U	(16)
15.	(a)	Explain the traditional problems associated with Cyber Crime	CO1 -U	(16)
		Or		
	(b)	Define Cloud Computing and discuss its relationship with cybercrime	CO1 -U	(16)