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

Question Paper Code: U5G02

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

Fifth Semester

Computer Science Engineering

(Artificial Intelligence and Machine Learning)

21UAM502 INTRODUCTION TO CRYPTOGRAPHY AND CYBER SECURITY

(Regulations 2021)

Duration: Three hours | Maximum: 100 Marks

PART A - (10 x 2 = 20 Marks)

1.	Distinguish Passive and Active attack with an Example.	CO1 U	
2.	What is meant by Eavesdropping?	CO1 U	
3.	Write about the Strength of DES.	CO1 U	
4.	Differentiate symmetric key and Asymmetric Key Encryption.	CO1 U	
5.	What is the difference between symmetric key cryptography and public key Cryptography?	CO1 U	
6	Why is asymmetric cryptography bad for huge data? Specify the reasons	CO1 U	
7	List the types of functions that may be used to produce an authenticator.	CO1 U	
8	Show how SHA is more secure than MD5	CO1 U	
9	What are the categories of cybercrime?	CO1 U	
10	What is Cloud Security? What are the Challenges of Advanced Cloud Security?	CO1 U	

PART – B (5 x 16= 80 Marks)

11.	(a)	Construct a play fair matrix with the key “MONARCHY”. Using that matrix encrypt the message “Instrumentsz” and write the rules to perform the encryption and decryption.	CO2 App	(16)
		Or		
	(b)	Encrypt and Decrypt the message “ATTACKATDAWN” using the key “Lemon” using Vigenere Cipher.	CO2 App	(16)

12.	(a)	Explain in detail Data Encryption Standard with Example.	CO1 U	(16)
		Or		
	(b)	Explain in detail Advanced Encryption Standard and Evaluation Criteria for AES.	CO1 U	(16)
13.	(a)	Apply Chinese Reminder Theorem to solve $X \equiv 8 \bmod 9$, $X \equiv 3 \bmod 20$ and also write the step by step procedure to solve the problem.	CO2 App	(16)
		Or		
	(b)	Perform encryption and decryption to the system with p=7, q=11, e=17, M=8 using RSA Algorithm and also write the step by step procedure to solve the problem.	CO2 App	(16)
14.	(a)	Explain various methods involved in Authentication of the source. Write about how the Integrity of the Message is ensured without Source Authentication.	CO1 U	(16)
		Or		
	(b)	Explain in detail Kerberos and Write the entities constitute a full-service Kerberos environment?	CO1 U	(16)
15.	(a)	Explain in detail Classification of Cyber Crimes.	CO1 U	(16)
		Or		
	(b)	Explain in detail Cloud Security	CO1 U	(16)