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

Question Paper Code: R5G02

B.E./B.Tech. DEGREE EXAMINATION, NOV 2025

Fifth Semester

CSE (Artificial Intelligence and Machine Learning)

R21UAM502 - INTRODUCTION TO CRYPTOGRAPHY AND CYBER SECURITY

(Regulations R2021)

Duration: Three hours | Maximum: 100 Marks

Answer ALL Questions

PART A - (10 x 2 = 20 Marks)

1.	Define Active attack with an Example.	CO 1- U
2.	Encrypt the plain text "COMPUTER SCIENCE" with the key=241653 using row Transposition technique.	CO2-App
3.	Write about the Strength of DES.	CO 1- U
4.	Define Public key cryptography	CO 1- U
5.	Illustrate Primality test	CO2-App
6.	Using Diffie–Hellman with p=23, g=5,a=4 and Bob selects b=3. Find the shared secret key.	CO2-App
7.	Define Digital signature. What are the properties of Digital Signature?	CO 1- U
8.	A user wants to send a signed message to a server. Explain how a digital signature can be applied to ensure authentication and integrity, and mention its properties.	CO2-App
9.	What are the classifications of Cyber Crimes?	CO 1- U
10.	An online shopping website is vulnerable to SQL Injection. What two security measures would you apply to protect the database from such attacks?	CO2-App

PART – B (5 x 16= 80 Marks)

11.	(a)	Encrypt and Decrypt the message “HELLO” using the key “THE” using Vigenere Cipher and write the Procedure for Encryption and Decryption.	CO1- U	(16)

Or

	(b)	Explain what substitution techniques are in cryptography, and describe any four types of substitution techniques with suitable examples.	CO1- U	(16)
12.	(a)	Determine the GCD using Euclid's algorithm.	CO2- App	(4)
		i) To find d=gcd (a,b)= gcd(710,310)		(4)
		ii) To find d=gcd (a,b)= gcd(1970,1066)		(4)
		iii) Determine the GCD of (24140, 16762)		(4)
		iv) To find d =gcd(a,b)=gcd(55,22)		
		Or		
	(b)	Explain how the RC4 stream cipher uses permutation in its generation processes.	CO2- App	(16)
13.	(a)	Find the value of X for the given set of Congruent equations using Chines Remainder Theorem $x \equiv 1 \bmod 5$ $x \equiv 2 \bmod 6$ $x \equiv 3 \bmod 7$	CO2- App	(16)
		Or		
	(b)	To Find the P=7, Q=11, E=7, M=9 to Perform encryption and decryption using RSA	CO2- App	(16)
14.	(a)	Describe the performance of Symmetric Key Distribution using Asymmetric Encryption.	CO1- U	(16)
		Or		
	(b)	Demonstrate how a Message Authentication Code can be applied to secure these messages.	CO1- U	(16)
15.	(a)	Explain briefly about Spyware. What are its features, types, harmful effects, and preventive measures?	CO1- U	(16)
		Or		
	(b)	What do you mean by Web Security? Explain in simple terms the common threats to web applications, the technologies used for protection, and some basic ways to apply web security measures.	CO1- U	(16)