Reg. No.												

Question Paper Code	12229

B.E. / B.Tech. - DEGREE EXAMINATIONS, NOV / DEC 2023

Seventh Semester

Computer Science and Engineering

CS8792 - CRYPTOGRAPHY AND NETWORK SECURITY

(Regulations 2017)

Duration: 3 Hours Max. Marks: 100

PART - A (10 × 2 = 20 Marks)

Answer ALL Questions

		Marks, K-Level, CO
1.	Differentiate cryptography from cryptanalysis.	*2,K2,CO1*
2.	Define avalanche effect.	*2,K1,CO1*
3.	What are the three main encryption algorithms?	*2,K1,CO2*
4.	List out the components of encryption algorithm.	*2,K1,CO2*
5.	Define Reversible mapping.	*2,K1,CO3*
6.	Find gcd (1970, 1066) using Euclid's algorithm.	*2,K2,CO3*
7.	State Weak collision resistance.	*2,K1,CO5*
8.	List the authentication message requirements.	*2,K1,CO5*
9.	List the three classes of Intruders.	*2,K1,CO6*
10.	List the benefits of IPSec.	*2,K1,CO6*

PART - B (5 × 13 = 65 Marks)

Answer ALL Questions

11.	a)	(i) Explain different types of security attacks.	*7,K2,CO1*
		(ii) Discuss the network security model with a neat diagram.	*6,K2,CO1*
		OR	
	b)	(i) Describe the various security mechanisms.	*8,K2,CO1*
		(ii) Discuss level of security at multiple levels.	*5,K2,CO1*
12.	a)	List and explain the various substitution cipher techniques with suitable examples.	*13,K2,CO2*
		OR	
	b)	Explain any two transposition techniques and give suitable example for each technique.	*13,K2,CO2*
13.	a)	What do you mean by AES? Diagrammatically illustrate the structure of AES and describe the steps in the AES encryption process with example.	*13,K2,CO3*

OR

b) Explain in detail about symmetric key cryptography and its components with a neat block diagram. *13,K2,CO3*

14. a) Explain how message authentication is performed by Message Authentication Code (MAC) with neat diagrams. *13,K2,CO5*

OR

b) Write short notes on *13,K2,CO5*
(a) HMAC.
(b) CMAC.

15. a) Explain the operational description of PGP and PGP cryptographic functions in detail with suitable block diagrams. *13,K2,CO6*

OR

b) Explain Intrusion Detection System (IDS) in detail with suitable diagram. *13,K2,CO6*

PART - C (1 × 15 = 15 Marks)

16. a) Illustrate the RSA Algorithm and estimate the encryption and decryption values for the RSA algorithm parameters. P=7, Q=11, E=17, M=8. *15,K3,CO4*

OR

b) Discuss and demonstrate the Chinese Remainder Theorem and find X for the given set of congruent equations X≡2 mod 3, X≡3 mod 5 and X≡2 mod 7. *15,K3,CO4*