Reg. No.												

Question Paper Code	12588

B.E. / B.Tech. - DEGREE EXAMINATIONS, APRIL / MAY 2024

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 active attacks and passive attacks.	*2*	*K2*	*CO1*
2.	Define CIA Triad.	*2*	*K1*	*CO1*
3.	List out the two types of Encryption Techniques.	*2*	*K1*	*CO2*
4.	What is brute force attack?	*2*	*K1*	*CO2*
5.	State advantages of counter mode.	*2*	*K1*	*CO3*
6.	Give the strengths of Triple DES.	*2*	*K2*	*CO3*
7.	Write the Fermat's Theorem. Give example.	*2*	*K2*	*CO4*
8.	Define Euler Totient Function ø(n).	*2*	*K1*	*CO4*
9.	Differentiate transport and tunnel mode in IPsec.	*2*	*K2*	*CO6*
10.	List the three classes of Intruders.	*2*	*K1*	*CO6*

PART - B (5 × 13 = 65 Marks)

Answer ALL Questions

11.	a) i) Discuss the network security model with a neat diagram.	*6*	*K2*	*CO1*
	ii) Describe the various security mechanisms.	*7*	*K2*	*CO1*
	OR			
	b) i) What is Steganography? Briefly examine any three Techniques.	*6*	*K2*	*CO1*
	ii) Differentiate symmetric cryptography from asymmetric key cryptography.	*7*	*K2*	*CO1*
12.	a) i) Apply Caesar cipher and k=5 decrypt the given Cipher text "YMJTYMJWXNIJTKXNQJSHJ".	*7*	*K3*	*CO2*
	ii) Apply Vigenere cipher, encrypt the word "explanation" Classical cryptosystems and its types using the key "leg".	*6*	*K3*	*CO2*
	OR			
	b) Illustrate the concept of Hill cipher and encrypt the message "PAY" using a hill cipher with the following key matrix and show the decryption to get the original plain text.	*13*	*K3*	*CO2*

$$K = \begin{matrix} 17 & 17 & 5 \\ 21 & 18 & 21 \\ 2 & 2 & 19 \end{matrix}$$

13. a) Describe DES algorithm with neat diagram and explain each of the steps. *13 K2 CO3*

OR

b) Write short notes on the following terms: *13 K2 CO3*
Groups
Rings
Fields
Finite fields

14. a) Explain the Key generation, encryption, and decryption in ElGamal. *13 K2 CO4*

OR

b) Explain in detail about public key cryptography and its components with suitable block diagram. *13 K2 CO4*

15. a) Describe how Secure Electronic Transaction (SET) protocol enables e-transactions. Explain its components. *13 K2 CO6*

OR

b) Explain how Secure/Multipurpose Internet Mail Extension is supported in Electronic mail security with S/MIME messages. *13 K2 CO6*

PART - C (1 × 15 = 15 Marks)

16. a) What is Kerberos? Explain how Kerberos version 4 provides authenticated Services. *15 K2 CO5*

OR

b) What is Digital Signature? Explain how it is created at the sender end and retrieved at the receiver end and differentiate digital signature from digital certificate. *15 K2 CO5*