Reg. No.												

Question Paper Code	12607

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

Seventh Semester

Computer Science and Engineering

20ITPC701 - CRYPTOGRAPHY AND NETWORK SECURITY

Regulations - 2020

Duration: 3 Hours Max. Marks: 100

PART - A (10 × 2 = 20 Marks)

Answer ALL Questions

		Marks	*K – Level*	*CO*
1.	What is meant by Denial of Service attack? Is it Active Attack or Passive Attack?	*2*	*K1*	*CO1*
2.	Let message = "Anna", and k = 3, find the cipher text using Caesar.	*2*	*K2*	*CO1*
3.	Define Ring with an example.	*2*	*K1*	*CO2*
4.	Find GCD (2740, 1760) using Euclidean Algorithm.	*2*	*K2*	*CO2*
5.	Find the GCD of (2740, 1760) using Euclid's Algorithm.	*2*	*K2*	*CO3*
6.	State Fermat's little theorem.	*2*	*K1*	*CO3*
7.	What is MAC? Mention the requirement of MAC.	*2*	*K1*	*CO4*
8.	What is asymmetric key cipher?	*2*	*K1*	*CO4*
9.	Differentiate Virus and Worm.	*2*	*K2*	*CO5*
10.	What do you mean by IP Security policy?	*2*	*K1*	*CO5*

PART - B (5 × 13 = 65 Marks)

Answer ALL Questions

11.	a)	Let message = "graduate", Key = "word", find cipher text using play fair cipher.	*13*	*K2*	*CO1*
		OR			
	b)	Explain OSI Security Architecture model with neat diagram.	*13*	*K2*	*CO1*
12.	a)	Describe DES algorithm with neat diagram and explain the steps.	*13*	*K2*	*CO2*
		OR			
	b)	What do you mean by AES? Diagrammatically illustrate the structure of AES and describe the steps in AES encryption process with example.	*13*	*K2*	*CO2*
13.	a)	Find the secret key shared between user A and user B using Diffie-Hellman algorithm for the following q=353; α (primitive root) =3, XA=45 and XB=50.	*13*	*K3*	*CO3*
		OR			

K1 – Remember; K2 – Understand; K3 – Apply; K4 – Analyze; K5 – Evaluate; K6 – Create

b) Summarize Chinese Remainder theorem and find X for the given set of congruent equation using CRT. $X \equiv 1 \pmod{5}$ $X \equiv 2 \pmod{7}$ $X \equiv 3 \pmod{9}$ $X \equiv 4 \pmod{11}$. *13 K3 CO3*

14. a) How Hash function algorithm is designed? Explain their features and properties. *13 K2 CO4*

OR

b) Explain briefly about the architecture and certification mechanisms in Kerberos and X.509. *13 K2 CO4*

15. a) Draw IPSec Authentication Header and write short notes on each element of the Header. *13 K2 CO5*

OR

b) Illustrate the various types of firewalls with neat diagrams. *13 K2 CO5*

PART - C (1 × 15 = 15 Marks)

16. a) Evaluate the performance of PGP. Compare it with S/MIME. *15 K3 CO6*

OR

b) Describe the working of SET with neat diagram. *15 K3 CO6*