Reg. No.												

Question Paper Code	12219

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

Seventh Semester

Computer and Communication Engineering

20CCPW701 - CRYPTOGRAPHY AND NETWORK SECURITY WITH LABORATORY

(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.	Draw a matrix that shows the relationship between security services and security mechanisms.	*2,K1,CO1*
3.	Specify the design criteria of block cipher.	*2,K2,CO2*
4.	Give the five modes of operation of block cipher.	*2,K2,CO2*
5.	What do you mean by one way property in hash function?	*2,K1,CO4*
6.	How a security of a MAC function expressed?	*2,K1,CO4*
7.	List four general categories of schemes for the distribution of public keys.	*2,K1,CO5*
8.	Assume the client C wants to communicate with server S using Kerberos procedure. How can it be achieved? Write the authentication dialogue.	*2,K2,CO5*
9.	Justify the following statement: With a Network Address Translation (NAT) box, the computers on the internal network do not need global IPV4 addresses in order to connect to the internet.	*2,K2,CO6*
10.	State the difference between threat and attacks.	*2,K2,CO6*

PART - B (5 × 13 = 65 Marks)

Answer ALL Questions

11.	a)	Explain the network security model and its important parameter with a neat block diagram.	*13,K2,CO1*
		OR	
	b)	Explain various substitution techniques ciphers in detail.	*13,K2,CO1*
12.	a)	(i) Draw the functionality diagram (functionality in one round) of DES with the number of bits in each flow of data.	*7,K2,CO2*
		(ii) Explain the bitwise XOR operation which is involved in RC4.	*8,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) (i) Summarize CMAC algorithm and its usage. *7,K2,CO4*
(ii) Describe any one method of effective implementation of HMAC. *6,K2,CO4*

OR

b) (i) Explain in detail message authentication code and its requirements. *7,K2,CO4*
(ii) Illustrate the security of hash functions and MACs. *6,K2,CO4*

14. a) Explain PKI management model and its operations with the help of a diagram. *13,K2,CO5*

OR

b) Explain briefly about the architecture and certification mechanisms in kerberos and X.509 standard. *13,K2,CO5*

15. a) Discuss authentication header and the format of IPSec ESP Packet in detail. *13,K2,CO6*

OR

b) Explain the technical details of firewalls and describe any three types of firewalls with a neat diagram. *13,K2,CO6*

PART - C (1 × 15 = 15 Marks)

16. a) Alice and Bob agreed to use RSA algorithm for the secret communication. Alice securely choose two primes, p=5 and q=11 and a secret key d=7. Find the corresponding public key. Bob uses this public key and sends a cipher text 18 to Alice. Find the plain text. *15,K3,CO3*

OR

b) User A & B exchanges the key using Diffie Hellman algorithm. Assume α=5 q=83 XA=6 XB=10. Find YA, YB, K. *15,K3,CO3*