VIT
Vellore Institute of Technology
CHENNAI

Reg. Number: 21BCE5972

Continuous Assessment Test – II - APRIL 2024

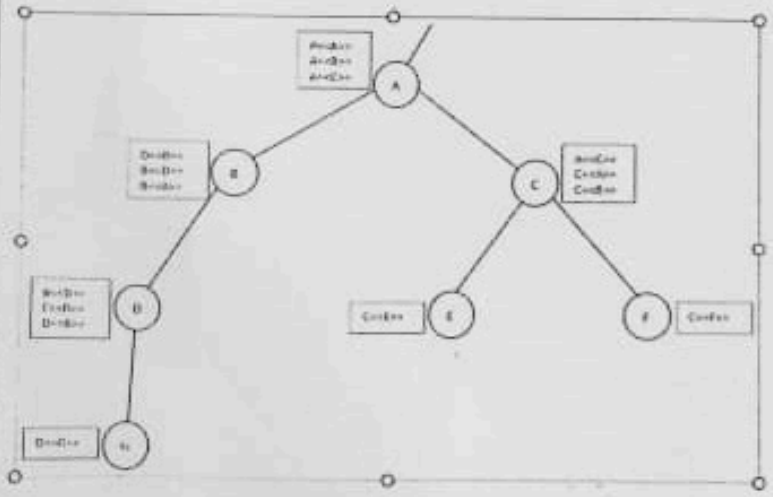
Programme	:	B.Tech	Semester	:	Winter 2023-2024
Course Code & Course Title	:	**BCSE309L-Cryptography and Network Security**	Class Number	:	CH2023240501438 CH2023240501461 CH2023240501468 CH2023240501444 CH2023240501448 CH2023240501477 CH2023240501483 CH2023240501453 CH2023240501490 CH2023240501495 CH2023240501501 CH2023240501458
Faculty	:	Dr.X.Anita Dr.P.Subbulakshmi Dr.Bhuvaneswari Amma N G Dr.Mary Shyamala L Dr.Vatchala S Dr.S.Sobitha Ahila Dr.Rajesh R Dr.Tapabrata Roy Dr.Karthika V Dr.Balasaraswathi Dr.Kanthimathi S Dr.Valarmathi K	Slot	:	**F2+TF2**
Duration	:	**1 1/2 Hours**	Max. Marks		**50**

Answer all questions

Q. No	Sub Sec.	Description	Marks
1		In a secure electronic voting system, users utilizing the large prime integer q=89 and generator a=5, here we consider two participants. Voter A selects X_A=47 and the Verifier B chooses X_B=25. In this scenario, Voter A casts a vote with hash 63 and generates a signature using a random value K=29. Verifier B Verifies the signature through an appropriate algorithm to ensure the authenticity and integrity of the vote in the context of a secure voting system.	10
2	i)	Compute the two public keys and the common session key for the Diffie Hellman Key Exchange (DHKE) scheme with the parameters p = 23, X_A = 3, X_B = 6 and α has been chosen	10

9/13

	ii)	as the second primitive root of p. pool. (8 Marks) In the Diffie-Hellman key exchange protocol, the private keys are chosen from the set {2, 3, …, p-2}. Why are the values 1 and p−1 excluded? Describe the weakness of these two values. (2 Marks)	
3		Integrity of a message sent by head of xyz company can be verified using MD5 Algorithm. Message sent by the head was 4 ASCII characters "bcse". Determine the following values of input 512 bit block. **Note: ASCII value of "a=97"** (normal) a. Message "bcse" (convert each ASCII character into 8 bit binary). (2 Marks) b. Total no of zeros padded with input 512 bit block and 64bit message length in binary (2 Marks) c. Write the binary words M_0 to M_{15} after Splitting the 512-bit Message into sixteen 32-bit words. (3 Marks) d. Find the value for function H(B, C, D) used at third round for its initial operation with given input word. Word A = 99 AB CD AF Word B = 01 23 45 67 Word C = FE DC BA 98 Word D = 76 54 32 10 (3 Marks)	b=> 98 c=>99 s=> 115 e=> 101 10
4		You are the chief information security officer (CISO) of a financial institution that operates globally, with branches in multiple countries. The organization relies heavily on secure communication channels for its day-to-day operations, including online banking services, internal communications, and interbank transactions. Due to recent cybersecurity	

		incidents in the banking sector, your CEO has tasked you with strengthening the organization's security posture, particularly in the area of authentication and data encryption. As the CISO of the financial institution, with the following CA hierarchy (Figure 1) a. Explain how a forward certificate is used in the context of X.509 authentication. Also identify the forward certificates of CA 'B' repository. (3 Marks) b. What is a reverse certificate, and how does it differ from a forward certificate? Also Identify the reverse certificates of CA 'A' repository. (3 Marks) c. Discuss how user G establish the certification path to user F. (2 Marks) d. Discuss how user E establish the certification path to user G. (2 Marks)  **Figure 1: CA Hierarchy**	10
5		Given the cryptosystem parameters are $E_{11}(1, 7)$ and $G = (3, 2)$. B's private key is $n_a = 2$. a. Find B's public key P_B. (2 Marks)		

		b. A wishes to encrypt the message $P_m = (10, 7)$ and chooses the random value k = 5. Determine the ciphertext C_m (4 Marks) c. Show the calculation by which B recovers P_m from C_m (4 Marks)	10