Reg. No. : | | | | | | | | | | | | |

Question Paper Code: U2304

M.E. DEGREE EXAMINATION, MAY 2023

Second Semester

Computer Science and Engineering

21PCS204 – NETWORK SECURITY

(Regulations 2021)

Duration: Three hours | Maximum: 100 Marks

Answer ALL Questions

PART A - (5 x 20 = 100 Marks)

1.	(a)	(i) Encrypt the message "PAY" using hill cipher with the following key matrix and show the decryption to get the original plaintext. KEY=$\begin{bmatrix} 17 & 17 & 5 \\ 21 & 18 & 21 \\ 2 & 2 & 2 \end{bmatrix}$ (ii) Given Cipher text "YMJTYMJWXNIJTKXNQJSHJ", the message is encrypted by Caesar cipher and k=5. Try to decrypt the message.	CO2-App	(20)
		Or		
	(b)	In the RSA cryptosystem encryption is performed using C ≡ Me (mod N), where N = pq for suitably chosen large primes p, q, and gcd(e, φ(N)) = 1. In a chaining attack on RSA, given a ciphertext C ≡ Me (mod N) the atacker computes, C e (mod N), Ce 2 (mod N), . . . , Ce k (mod N), unless C ≡ C e k (mod N) is obtained. That is, k is the least positive integer that specifies the cycle. Explain why the attacker can always find k ∈ [1, N − 1] so that C ≡ C e k (mod N). Hint: Recall that RSA is an encryption algorithm and therefore bijective, i.e. M1 6= M2 cannot be mapped to the same ciphertext.	CO2-App	(20)
2.	(a)	For Diffie-Hellman algorithm, two publicaly known numbers are prime number 353 and primitive root of it is 3. A selects the random integer 97 and B selects 233. Compute the public key of A and B. Also compute common secret key.	CO2- App	(20)
		Or		

	(b)	(i) Identify the possible threats for RSA algorithm and list their counter measures. (ii) Perform decryption and encryption using RSA algorithm with p=3, q=11, e=7 and N=5.	CO2- App	(20)
3.	(a)	Users A and B use the Diffie Hellman key exchange technique, a common prime q=11 and a primitive root alpha=7. (i) If user A has private key XA=3.What is A's public key YA? (ii) If user B has private key XB=6 What is B's public key YB? (iii) What is the shared secret key? Also write the algorithm. (iv) How man in middle attack can be performed in Diffie Hellman algorithm.	CO2-App	(20)
		Or		
	(b)	(i) A Box contains gold coins. If the coins are equally divided among three friends, two coins are left over, If the coins are equally divided among five friends, three coins are left over If the coins are equally divided among seven friends, two coins are left over. If the box holds smallest number of coins that meets these conditions, how many coins are there?	CO2-App	(20)
4.	(a)	A taxicab was involved in a fatal hit-and-run accident at night. Two cab companies, the Green and the Blue, operate in the city. You are told that ● 85% of the cabs in the city are Green and 15% are Blue. ● A witness identified the cab as Blue. The court tested the reliability of the witness under the same circumstances that existed on the night of the accident and concluded that the witness was correct in identifying the color of the cab 80% of the time. What is the probability that the cab involved in the incident was Blue rather than Green?	CO2- App	(20)
		Or		
	(b)	Apply SSL protocol for server and client authentication.	CO2- App	(20)

5.	(a)	Apply Secure Electronic Transaction for E-Banking Application for card holders purchase request and verification by the merchants.	CO2-App	(20)
		Or		
	(b)	Explore the Concept of intrusion detection and the different types of detection mechanisms, in detail.	CO2-App	(20)