ROLL NUMBER 1 9 B E C 0 4 8

Dr. MAHALINGAM
COLLEGE OF ENGINEERING AND TECHNOLOGY

Affiliated to Anna University, Chennai; Approved by AICTE ; Accredited by NAAC with Grade A++
Accredited by NBA - Part (Mech, Auto, Civil, EEE, ECE, ISE and CSE)
Udumalai Road, Pollachi - 642 003. Tel: 04259-226000/01/02 Fax: 04259 226070 www.mcet.in

Question Paper Code: 221EC005 QRN Code: 2210104 Regulations: 2019

B.E./B.Tech., DEGREE EXAMINATION, NOV / DEC 2022

SEVENTH SEMESTER– B.E. ELECTRONICS AND COMMUNICATION ENGINEERING

19ECEN1010 – CRYPTOGRAPHY AND NETWORK SECURITY

Duration: Three hours **Answer ALL questions** Maximum: 100 marks

PART – A (10 x 2 = 20 marks)		CO No.	Revised Bloom's Cognitive Level	
			Question	CO
1.	Differentiate active attack from Passive attack.	CO1	Ap	Ap
2.	Apply brute force attack to determine the plain text for the cipher text "PRZZBPP" produced by Caesar cipher.	CO1	Ap	Ap
3.	Find the value of $\phi(21)$.	CO2	Ap	Ap
4.	Compare Conventional and Public key encryption.	CO2	Ap	Ap
5.	List the advantages of MAC.	CO3		An
6.	State one way property and collision resistance of hash functions.	CO3	R	An
7.	Differentiate X.509 certificate with PGP certificate	CO4	U	U
8.	List the properties of PGP.	CO4	R	U
9.	State the role of honey pots in attracting the intruder.	CO5	R	Ap
10.	Worms or virus, which one is more dangerous Justify.	CO5	Ap	Ap

PART – B (5 x 16 = 80 marks)			Marks	CO No.	Revised Bloom's Cognitive Level	
					Question	CO
11.(a)		Perform play fair cipher to encrypt the following plain text "LEAVE AT TEN" using the key "NETWORK SECURITY". Explain the rules of the algorithm.	16	CO1	U	Ap
		Or				
11.(b)		Explain the steps involved in the encryption and decryption process in DES algorithm.	16	CO1	U	Ap
12.(a)		In a public key system using RSA, interpret the cipher text C=10 sent to a user whose public key is e=5, n=35. Find the plaintext M.	16	CO2	Ap	Ap
		Or				
12.(b)		Users A and B use the Diffie–Hellman key exchange technique a common prime n=23 and primitive root g=5 are used. If user A has private key X_A=6, what is A's public key Y_A. If user B has private key X_B=15, what is B's public key Y_B. What is the shared secret key.	16	CO2	Ap	Ap
13.(a)		Analyze the MD5 message digest algorithm importance in security and explain it with an example.	16	CO3	An	An
		Or				
13.(b)	(i)	Analyze whether one can use Hash algorithm to produce authentication.	8	CO3	An	An
	(ii)	A sender uses hash value of a message to provide message authentication and confidentiality. Explain How a receiver verifies authentication and confidentiality. Write your comments.	8			

14.(a)		Explain the architecture of the authentication service Kerberos.	16	CO4	U	U
		Or				
14.(b)		Compare Transport mode and Tunnel mode operation in IPsec. Choose the best mode which will be suitable for virtual private network. Give your comments	16	CO4	U	U
15.(a)		Discuss the need of firewall for computer networks. Describe various types of firewalls in detail.	16	CO5	U	Ap
		Or				
15.(b)		Consider the following fragment: legitimate code if data is Friday the 13th; crash_computer(); legitimate code Identify the type of malicious software from the above code.Describe the various malicious programs and classification of viruses.	16	CO5	U	Ap

Sl. No.	Cognitive Level	Code	Order	% in Question Paper
1	Remember	R	Lower Order	84%
2	Understand	U		
3	Apply	Ap		
4	Analyze	An	Higher Order	16%
5	Evaluate	E		
6	Create	C		