ROLL NUMBER	2	0	B	E	C	0	2	4

Dr. MAHALINGAM COLLEGE OF ENGINEERING AND TECHNOLOGY

Udumalai Road, Pollachi, Coimbatore District 642003

Establishment in 1998 | Approved by AICTE | Affiliated to Anna University

An Autonomous Institution Since 2011

(A DIVISION OF MIA EDUCATIONAL INSTITUTIONS)

Question Paper Code: 230EC004 QRN Code: 2300108 Regulation: 2019

B.E./B.Tech., DEGREE EXAMINATION, NOV' / DEC' 2023

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.	"Passive attacks are very difficult to detect" Justify this statement.	CO1	U	Ap
2.	How many keys are required for two people to communicate via a cipher?	CO1	U	Ap
3.	User A and B exchange the key using Diffie-Hellman algorithm. Assume α=5 q=11 X_A=2 X_B=3. Find the value of Y_A, Y_B and k.	CO2	Ap	Ap
4.	List the properties of Congruences.	CO2	R	Ap
5.	Mention the role of compression function in hash function?	CO3	U	An
6.	Outline about Birthday attack.	CO3	U	An
7.	Illustrate the services provided by IPSec.	CO4	U	U
8.	Summarize about the technical deficiencies of Kerberos v4.	CO4	U	U
9.	Recall the different phases a virus go through his lifetime in network security?	CO5	R	Ap
10.	Outline Intrusion Detection System.	CO5	R	Ap

		PART – B (5 x 16 = 80 marks)	Marks	CO No.	Revised Bloom's Cognitive Level	
					Question	CO
11.(a)		Encrypt the following using play fair cipher using the keyword MONARCHY ."SWARAJ IS MY BIRTH RIGHT". Use X as blank space.	16	CO1	Ap	Ap
		Or				
11.(b)	(i)	Draw the general structure of DES and explain the encryption and decryption process.	10	CO1	U	Ap
	(ii)	Mention the strengths and weakness of DES algorithm.	6	CO1	U	Ap
12.(a)	(i)	Calculate X for the given set of congruent equations X≡2 mod 3, X≡3 mod 5 and X≡2 mod 7 and state the Chinese remainder theorem.	8	CO2	Ap	Ap
	(ii)	Outline the Fermat's theorem with example.	8	CO2	U	Ap
		Or				
12.(b)	(i)	Perform decryption and encryption using RSA algorithm with p=3, q=11, e=7 and N=5.	8	CO2	Ap	Ap
	(ii)	What are the requirements and applications of public key? Compare conventional with public key encryption.	8	CO2	U	Ap
13.(a)	(i)	Summarize the types of attacks addressed by message authentication and discuss the two levels of functionality that comprise a message authentication mechanism.	8	CO3	U	An

	(ii)	Explain the process of deriving eighty 64-bitwords from 1024 bits for processing of a single blocks and also discuss single round function in SHA-512 algorithm and also Show the values of W16, W17, W18 and W19.	8	CO3	Ap	An
		Or				
13.(b)		Describe about Hash Function features and properties and How its algorithm is designed?	16	CO3	U	An
14.(a)		Outline how does PGP provide confidentiality and authentication service for e-mail and file storage applications with necessary diagrams.	16	CO4	U	U
		Or				
14.(b)	(i)	Elaborate the requirements of Kerberos and discuss its version.	8	CO4	U	U
	(ii)	Analyze the Cryptographic algorithms used in S/MIME and explain S/MIME certification processing procedures.	8	CO4	U	U
15.(a)		Elaborate Worms and viruses related to system level security.	16	CO5	U	Ap
		Or				
15.(b)		Write short notes on i)IP spoofing attack i)Intrusion detection system .	16	CO5	U	Ap

Sl. No.	Cognitive Level	Code	Order	% in Question Paper
1	Remember	R	Lower Order	100
2	Understand	U		
3	Apply	Ap	Higher Order	-
4	Analyze	An		
5	Evaluate	E		
6	Create	C		