Priyadarshini College of Engineering, Nagpur
Sessional Examination (2023-24) Odd Semester
B. Tech. Seventh Semester (Computer Technology) (C. B. C. S.)
Cryptography and Network Security

P. Pages: 2
Time: Three Hours

PCE/WS/23/BTCT701T
Max. Marks: 70

Notes:

1) All questions carry marks as indicated.
2) Solve Question 1 or Question 2
3) Solve Question 3 or Question 4
4) Solve Question 5 or Question 6
5) Solve Question 7 or Question 8
6) Solve Question 9 or Question 10
7) Due credit will be given to neatness and adequate dimensions.
8) Assume suitable data wherever necessary.
9) Illustrate your answers whenever necessary with the help of neat sketches.

Que. No.		Questions	CO	BL	Marks
1	a)	Explain the model for Network Security.	CO1	2	7
	b)	Illustrate the encryption and decryption process using Hill Cipher for: Plain Text : ATTACK Keyword : BCCF	CO1	3	7
		OR			
2	a)	Apply Extended Euclid algorithm to compute GCD (99,78). Show all the computations.	CO1	3	7
	b)	State the different substitution encryption techniques. Encrypt the following plaintext using Playfair cipher: Plain Text : CHANDRAYAAN Keyword : MONARCHY	CO1	3	7
3	a)	Differentiate between block cipher and stream cipher.	CO2	2	5
	b)	Explain Key Calculation Procedure in Simplified DES algorithm. Illustrate your answer by considering user input key as 00011 00111.	CO2	3	9
		OR			
4)	a)	What are the block cipher modes of operation of DES? Explain in detail.	CO2	2	5
	b)	Explain in detail about DES encryption and decryption algorithm.	CO2	2	9

5) Give the stepwise illustration of RSA algorithm to perform encryption and decryption procedure for following data: CO3 3 14

Plain Text	:	10
Prime No. P	:	11
Prime No. Q	:	17
Parameter e	:	7

OR

6 a) Explain in detail about the working of Diffie-Hellman key exchange algorithm. CO3 2 7

b) Apply the Chinese Remainder Theorem to solve following congruent equations. CO3 3 7

$X \equiv 2 \pmod 3$
$X \equiv 3 \pmod 5$
$X \equiv 2 \pmod 7$

7 a) Explain in detail about X.509 directory authentication service. CO4 2 7

b) Explain MD5 message digest algorithm with example. CO4 2 7

OR

8 a) Explain in detail about the hash functions and their security. CO4 2 7

b) What is Kerberos? Explain briefly about it. CO4 2 7

9) a) What is firewall? What are its type? Explain in brief. CO5 2 7

b) Explain in detail about SQL injection? CO5 2 7

OR

10 a) Discuss in detail about application gateway firewall. CO5 2 7

b) Explain in detail about PGP. CO5 2 7

35
35
105