U.S.N | | | | | | | | | | |

P.E.S. College of Engineering, Mandya - 571 401

(An Autonomous Institution affiliated to VTU, Belagavi)

Seventh Semester, B.E. - Computer Science and Engineering

Semester End Examination; February - 2022

Cryptography and Network Security

Time: 3 hrs *Max. Marks: 100*

Course Outcomes

The Students will be able to:
CO1: Define cryptography and its principles
CO2: Explain Cryptography algorithms
CO3: Illustrate Public and Private key cryptography
CO4: Understand Key management, distribution and certification
CO5: Implementation authentication protocols and analyze IPSec

Note: ***I) PART - A*** *is compulsory.* ***Two*** *marks for each question.*
II) PART - B*: Answer any* ***Two*** *sub questions (from a, b, c) for Maximum of* ***18 marks*** *from each unit.*

Q. No.		Questions	Marks	BLs	COs	POs
		I : PART - A	**10**			
I	a.	Distinguish between Block and Stream cipher.	2	L2	CO1	PO2
	b.	What are the counter measures for timing attacks in RSA?	2	L2	CO2	PO2
	c.	What is a nonce? How nonce is used in key distribution?	2	L2	CO3	PO2
	d.	Differentiate between Transport mode and Tunnel mode.	2	L2	CO4	PO3
	e.	What are the benefits of IPSec?	2	L2	CO5	PO3
		II : PART - B	**90**			
		UNIT - I	**18**			
1	a.	Differentiate between; i) Active and passive attacks ii) Data confidentiality and Data integrity iii) Substitution and Transposition	9	L2	CO1	PO1,5
	b.	Use the play fair cipher to encipher the message "Life is full of surprises". The secret key can be made by filling the first and part of the second row the word "GUIDANCE" and filling the rest of the matrix with the rest of the alphabet. (Note: ignore the space in between words)	9	L3	CO1	PO1,5
	c.	Explain the structure of DES in detail.	9			
		UNIT - II	**18**	L2	CO5	PO3
2	a.	Generate public and private keys by using RSA cryptosystem. Given N = 77, e = 13, Encrypt the message m = 5 using RSA algorithm. Decrypt the same.	9	L3	CO2	PO1,2,4

Contd... 2

b.	Explain Diffie-Hellman key exchange algorithm / protocol in detail. And also Illustrate how this protocol suffers Man-in-the-Middle attack?	9	L2	CO2	PO1,2,3
c.	Differentiate between conventional and public key cryptosystem.	9	L3	CO2	PO1,2,4
	UNIT - III	**18**			
3 a.	Explain the step involved in the distribution of unique master key by using KDC.	9	L2	CO3	PO1,2,3
b.	Explain the various ways of distributing public keys.	9	L2	CO3	PO1,2,3
c.	Investigate the short comings of Kerberos version-4.	9	L2	CO3	PO1,2,3
	UNIT - IV	**18**	L2	CO3	PO2
4 a.	Explain SSH protocol stack.	9	L2	CO4	PO1,6
b.	Discuss the phases of operation of IEEE 802.11i.	9	L2	CO4	PO1,6
c.	Explain the Handshake protocol of SSL.	9	L2	CO4	PO1,6
	UNIT - V	**18**			
5 a.	Explain the important services provided by PGP.	9	L2	CO5	PO1,3
b.	Write a note on;				
	i) ESP header	9	L2	CO5	PO1,3
	ii) Authentication Header protocol				
c.	Explain the working of S/MIME.	9	L2	CO5	PO1,3

* * * *