PVP 19

Code: 19IT3701

IV B.Tech - I Semester – Regular Examinations - DECEMBER 2022

CRYPTOGRAPHY AND NETWORK SECURITY
(INFORMATION TECHNOLOGY)

Duration: 3 hours Max. Marks: 70

Note: 1. This question paper contains two Parts A and B.
2. Part-A contains 5 short answer questions. Each Question carries 2 Marks.
3. Part-B contains 5 essay questions with an internal choice from each unit. Each question carries 12 marks.
4. All parts of Question paper must be answered in one place.

BL – Blooms Level CO – Course Outcome

PART – A

		BL	CO
1. a)	What are the key principles of security?	L2	CO1
1. b)	What is meant by one-way property in hash function?	L2	CO1
1. c)	What is meant by life time of a key?	L2	CO1
1. d)	What is difference between SSL and TLS?	L2	CO1
1. e)	Why is IPsec important?	L2	CO1

PART – B

			BL	CO	Max. Marks
UNIT-I					
2	a)	Discuss the weaknesses of DES in the view of its design principles and cipher keys.	L2	CO1	6M

	b)	How do you convert a block cipher into a stream cipher by using the Cipher Feedback (CFB) mode? Explain	L2	CO1	6M
OR					
3	a)	Illustrate different mechanisms used to implement different security services.	L2	CO1	6M
	b)	What is a security attack? Explain different types of active and passive attacks.	L2	CO1	6M
UNIT-II					
4	a)	Explain SHA algorithm with example.	L2	CO1	6M
	b)	How message authentication code works?	L2	CO1	6M
OR					
5	a)	Differentiate MAC and hash function.	L2	CO1	6M
	b)	Discuss about the digital signature and its types.	L2	CO1	6M
UNIT-III					
6	a)	Explain in detail the technique used in symmetric key cryptography.	L2	CO2	6M
	b)	Illustrate the 4 methods of public key distribution.	L3	CO4	6M
OR					
7	a)	Explain any two algorithms used in asymmetric encryption with an example.	L2	CO2	8M
	b)	Discuss issues of key distribution in cryptography.	L2	CO2	4M

UNIT-IV					
8	a)	Which algorithm is used in SSL and TLS? How Does SSL Encryption Works.	L3	CO3	8M
	b)	Explain the TLS Architecture.	L2	CO3	4M
OR					
9	a)	What is HTTPS? Explain the concept of connection initiation and closure in HTTPS.	L2	CO3	6M
	b)	Differentiate SSH1 and SSH2.	L3	CO4	6M
UNIT-V					
10	a)	What is S/MIME and how does it work?	L2	CO3	6M
	b)	Illustrate the differences between transport and tunnel modes in Encapsulating Security Payload.	L3	CO4	6M
OR					
11	a)	Show the Cryptographic algorithms used in S/MIME.	L3	CO4	8M
	b)	Demonstrate the five principal services provided by PGP.	L3	CO4	4M