USN | | | | | | | | | | |

RV COLLEGE OF ENGINEERING®

(An Autonomous Institution affiliated to VTU)

VI Semester B. E. Examinations August 2022

Information Science and Engineering

CRYPTOGRAPHY AND NETWORK SECURITY

Time: 03 Hours ***Maximum Marks: 100***

Instructions to candidates:

1. Answer all questions from Part A. Part A questions should be answered in first three pages of the answer book only.
2. Answer FIVE full questions from Part B. In Part B question number 2, 7 and 8 are compulsory. Answer any one full question from 3 and 4 & one full question from 5 and 6.

PART-A

1	1.1	Differentiate between substitution cipher and transposition cipher.	02
	1.2	List the components of encryption algorithm.	02
	1.3	Compare stream cipher and block cipher with example.	02
	1.4	Discuss the key expansion procedure in AES.	02
	1.5	Define an elliptic curve.	02
	1.6	State the requirements of a digital signature.	02
	1.7	List out the services provided by PGP.	02
	1.8	Compare SSL and TLS.	02
	1.9	State the benefits of IP Security.	02
	1.10	List the design goals of firewalls.	02

PART-B

2	a	Differentiate between monoalphabetic cipher and polyalphabetic ciphers and give an example for each.	08
	b	Discuss in detail on different types of security attacks and services in detail.	08
3	a	Describe DES algorithm with neat diagram and explain the steps.	08
	b	Write short notes on i. Playfair cipher ii. Vigenere cipher.	08
		OR	
4	a	Illustrate the working of simplified DES scheme encryption in detail.	08
	b	With an example, justify why the middle portion of 3-DES a decryption rather than an encryption.	08
5	a	Explain Diffie-Hellman key exchange algorithm in detail.	08
	b	Describe the digital signature algorithm and show how singing and verification is done using DSS.	08

		OR	
6	a	Illustrate the working of RSA and choose an application of your choice for RSA and show how encryption and decryption is carried out.	10
	b	With a neat sketch, explain the Elliptic curve cryptography with an example.	06
7	a	Discuss PGP cryptographic functions in detail with suitable block diagram.	08
	b	Describe the methodology involved in computing the keys in SSL/TLS protocol.	08
8	a	Explain in detail about the types of firewalls and mention the design criteria of a firewall to protect the host machines in an educational institution.	10
	b	Discuss Intrusion Detection System (IDS) in detail with suitable diagram.	06