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

RV COLLEGE OF ENGINEERING®

(An Autonomous Institution affiliated to VTU)

V Semester B. E. Examinations June-2023 (Makeup)

Computer Science and Engineering

NETWORK PROGRAMMING AND 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	List all the states the server would have visited before moving to the established state.	01
	1.2	Mention the functions used to make communication happen between two systems following different architectures?	02
	1.3	When does accept() system call return with respect to three-way handshake for connection establishment?	02
	1.4	When the first argument for the socket() is *AF_LOCAL*, list all the valid *type* argument for the socket() system call.	02
	1.5	The 'level' parameter in the getsockopt and setsockopt functions refers to _____.	01
	1.6	Assume two *TCP* clients that are about to start at the same time, _____ optname is used to in setcockopt *API* to make local address reuse.	01
	1.7	The equivalent system call/s for sendto() used in *UDP* applications to system calls used in *TCP* applications are _____.	02
	1.8	What is the situation under which the client gets blocked forever in its call to recvfrom()? Write one method to overcome?	02
	1.9	If a client knows www.google.com to connect to google server, _____ record is used to get its equivalent *IPv6* address.	01
	1.10	Alice has generated two keys, public key PU_A and private key PR_A, Bob has generated two keys, public key PU_B and private key PR_B how she should encrypt the messages to have both confidentiality and authentication?	02
	1.11	*DES* uses a key generator to generate how many round keys of what length?	01
	1.12	Define IPSec and its usage.	02
	1.13	How are client and server authenticated in *SSL*?	01

PART-B

2	a	Differentiate between TCP, UDP and $SCTP$ protocols.	06
	b	With a neat diagram, explain TCP state transition diagram showing normal transition between client and server. With server using piggybacking.	10
3	a	Explain all the socket function calls with the syntax in sequence that are called by the process that makes a passive connection with a neat diagram.	08
	b	Write a TCP socket program to implement an Echo server/Echo client to read the input from the file instead of stdin and also write the output to a different file instead of stdout.	08
		OR	
4	a	Discuss the system calls that are used to get the local and foreign protocol addresses with the relevant syntax and a program example in detail.	08
	b	What are concurrent Servers? How they are different from iterative servers? Explain with programs.	08
5	a	Applications deal with names not with addresses; discuss the functions and structures that are helpful to determine the host details.	06
	b	Write a program to design a UDP echo server which echoes the message back to the UDP client by changing its case.	10
		OR	
6	a	Discuss the importance and usage of resolver code in DNS both in case of its presence as a system library and as a built in into the application with a neat diagram.	08
	b	Write a C program to get the pending errors related to a socket. Is it possible to customize the errors? Justify your answers.	08
7	a	Explain the essential steps to be followed if Bob wishes to send a confidential message to Alice using public key cryptography with the help of an example.	06
	b	Suppose that two parties A and B wish to set up a common secret key ($D-H$ key) between themselves using the Diffie-Hellman key exchange technique. They agree on 7 as the modulus and 3 as the primitive root. Party A chooses 2 and party B chooses 5 as their respective secrets. Show the detailed steps at each party to find the shared secret key.	06
	c	Discuss how to encrypt multiples blocks using RSA for the text "RVCE" using the, if $p = 11, q = 19, e = 17$ with a neat diagram and steps.	04
8	a	Considering the organization into picture, discuss the major security threats and consequences for the mobile devices.	08
	b	With a neat diagram, discuss various components of 802.11 networks. Also discuss various transition types of the wireless devices.	08