RV UNIVERSITY Go, change the world an initiative of RV EDUCATIONAL INSTITUTIONS	**School of Computer Science & Engineering** **B.Tech(H) Program** **Academic Year: Jan-May 2025** **Semester 6 Version 2.0**

COURSE DESIGN, DELIVERY AND ASSESSMENT

Course Code: CS3403	**Course Name:** Network Security	
Semester: 6	**Area:** Major Data Science	**SEE Type:** Theory (30 Marks)
Level:	**Credits: 4 (**3: 0: 2)	**Contact Hours:** 75 Hours
Prerequisite (Course/Skill/Knowledge): ● Sem 4: CS2120: Computer Networks		

Course Faculty:

Sl#	Section	Course Faculty Name	Contact: Email/Contact Number	Sign with Date
1	A	Prof. Sheba Pari N	shebapari@rvu.edu.in 9480526218	
2	B	Prof. Chandramouleeswaran Sankaran (Mouli)	chandramouleeswarans@rvu.edu.in 9845539435	
3	C	Prof. Chandramouleeswaran Sankaran (Mouli)	chandramouleeswarans@rvu.edu.in 9845539435	

Course Lead (Name, Sign, Date): Prof. Chandramouleeswaran Sankaran (Mouli)

1. Course Context & Overview

The course aims to provide a broad coverage of some new advanced topics in the field of computer networks and network security. The course mainly focuses on working principles of TCP, RIP and OSPF protocols, RTP, QoS, cryptographic algorithms and cyber security essentials. Students through hands-on lab exercises and simulations gain theoretical concepts as well as practical experience on networks technologies and security.

2. Course Contents

Unit 1: Transmission Control Protocol (TCP) **12 Hours**

Recap of Classless Interdomain routing, subnet masking: Variable length subnet mask, Transmission control protocol (TCP), Automatic repeat request and retransmission, Sliding windows: TCP Service Model, reliability, header and flag. Motivation behind the congestion control in TCP, Router-centric vs host-centric, TCP Connection management, half-close, simultaneous open/close: ISN, Timeout, TCP Options, Path MTU: TCP State transitions: Reset segments, TCP Server operations: TCP Dataflow, interactive communication, Nagle Algorithm: TCP Flow control, window management. Various TCP congestion control protocols, DCCP, QUIC, DASH and its relevance with respect to applications.

Unit 2: Routing Protocols and SDN **12 Hours**

Distance-vector (RIP): Open Shortest Path First (OSPF): Router implementation and performance, Fabrics: Interdomain Routing- Global Internet, Routing areas: Interdomain Routing (BGP), AS relationships and policies: IPv6 Intro, Address space allocation, format, auto config: IP Multicast addresses and routing. Introduction to Software Defined Networking (SDN) and the recent trends on SDN.
Approaches: Rule-based and statistical.

Unit 3: VPN and QoS **6 Hours**

Destination based Forwarding, Explicit routing and VPN tunnels: Mobile IP and routing among mobile devices: Remote Procedure Call: Real-Time Protocol (RTP) and RTCP: Congestion control and Queuing disciplines, RED: Quality of Service, Resource reservation protocol, Differentiated Services.

Unit 4:Basics of Cryptography **8 Hours**

Basics of cryptography -cryptographic hash functions - symmetric and public-key encryption -public key cryptography principles & algorithms - cipher block modes of operation - Secure Hash Functions – HMAC

Unit 5: Networking Tools: **7 Hours**

Network defence tools: Firewalls, VPNs, Intrusion Detection, and filters - Email privacy: Pretty Good Privacy and S/MIME - Network security protocols in practice-Introduction to Wireshark-SSL -IPsec, and IKE -DNS security- Secure Socket Layer and Transport Layer Security – Secure Electronic Transaction. Access control checks, Virus and Malware detection. Cloud Security aspects of cloud and bigdata**.**

Course Outcomes: After completing the course, the students will be able to:	
CO1	Analyze the working principles and characteristics of TCP and its role in providing reliable networking applications.
CO2	Analyze the implementation details of RIP and OSPF routing protocols adapted by large enterprise networks.
CO3	Explain various multimedia transport protocols and the need for QoS in networks
CO4	Describe the working principles and the purpose of cryptographic algorithms used to provide secure communication
CO5	Apply IP security and Web security concepts in real-life scenarios for creating secure networks

Assessment Methodologies

(Tick✓ the Relevant Methodologies)

Assignments✓	Closed book tests✓	Open book tests
Case study	Student Presentation✓	Mini projects / Model Building✓
MOOC	Quiz✓	Peer Review✓

Textbooks (With ISBN No)

1. Peterson and Davie, Computer Networks a systems approach, Morgan Kaufmann, 6th Edition, 2019, ISBN: 978-0123850591.
2. William Stallings, Network Security Essentials (Applications and Standards), Pearson Education, 6th edition, 2021, ISBN: 978-9352866601.
3. Stallings, Cryptography and network Security, PHI/Pearson, 7th edition, 2017, ISBN: 978-1-292-15858-7.

Reference Material (With ISBN No)

1. Kevin R Fall and W Richard Stevens, TCP/IP Illustrated, Volume 1: the Protocols, PEARSON, 5th Edition, 2012, ISBN: 9780123850591.
2. Peterson, Brakmo, and Davie, TCP Congestion Control: A Systems Approach, Ver 1.1-Dev, online material.
3. Kurose and Ross, Computer Networking, A Top-Down Approach, PEARSON, 7th Edition, 2017, ISBN: 978-0-13-359414-0.
4. Computer Networks and Internet Protocols by IIT Kharagpur – **Course link.**

3. CO Mapping: Cognitive Levels, Knowledge Category, Contact & Activity Hours

Sl.No	Course Outcomes	Cognitive Level	Knowledge Category	PO	Class Conceptual hours	Class Activity Hours	Weightage of CO%
1	Analyze the working principles and characteristics of TCP and its role in providing reliable networking applications.	Analyze	Procedural	1,2,3,5,6, 7,11,12	12	6	20
2	Analyze the implementation details of RIP and OSPF routing protocols adapted by large enterprise networks	Analyze	Procedural	1,2,3,4,5, 6,12	12	6	20
3	Explain various multimedia transport protocols and the need for QoS in networks	Analyze	Procedural	1,2,3,4,5, 6,12	6	6	20
4	Describe the working principles and the	Apply	Procedural	1,2,3,4,5, 6,7,8,12	8	6	20

	purpose of cryptographic algorithms used to provide secure communication						
5	Apply IP security and Web security concepts in real-life scenarios for creating secure networks	Apply	Procedural	1,2,3,4,5, 6,7,8,12	7	6	20
	TOTAL: 75 Contact Hours (15 Weeks)				45	30	

4. Course Plan

Note: Lab activities will evolve throughout the course, with a Network Security lab introduced and utilized by the midpoint of the course.

Week 1	Outcome	Topics	Activity Based Teaching Learning Process
Week 1	CO1	Classless Interdomain routing, VLSM and its benefits Introduction to TCP and Sockets	Interactive Lecture: PowerPoint presentation, Quiz instant feedback through interactive quizzes
		Construct networks using switches and routers by configuring them	Hands-On Demo: Using WSL and Wireshark to analyses the packets between Windows and WSL (Ubuntu).
Week 2	CO1	TCP/UDP Ports and TCP Header TCP: Flow Control and Checksum TCP Header: Control Bits	Interactive Lecture: PowerPoint presentation Hands-on: Using Wireshark to analyze packets and TCP Header.

		Construct VLANs and perform inter-VLAN routing using switches	Hands on: Configuring IP address on desktops and sending files.
Week 3	CO1	TCP Features TCP: Connection Establishment	Interactive Lecture: PowerPoint presentation Quiz instant feedback through interactive quizzes
	CO1	Traffic congestion control related simulations on Cisco packet tracer.	Hands on: Using CISCO packet tracer to capture the SYN and FIN flags
Week 4	CO1	TCP: Half-open, Half-close, Reset TCP: Nagle's Algorithm Congestion Control Protocols (DCCP, QUIC, DASH)	Interactive Lecture: PowerPoint presentation Quiz instant feedback through interactive quizzes
	CO2	Understand the concept and operation of RIP using packet tracer	Hands on: Using CISCO packet Tracer to analyze RIP.
Week 5	CO2	Forwarding Vs Routing IP Routing Static Routing	Interactive Lecture: PowerPoint presentation Quiz instant feedback through interactive quizzes
	CO2	Construct multiple networks and understand the operation of OSPF Protocol using packet tracer	Hands on: Using CISCO packet Tracer to analyze OSPF.
Week 6	CO2	Routing Metrics and Costs Distance Vector Routing DVR: Solutions to Count to Infinity	Interactive Lecture: PowerPoint presentation Quiz instant feedback through interactive quizzes
	CO3	Configure IPSec to open a VPN tunnel between two machines on different networks	Hands on: Simulating VPN through CISCO packet Tracer
Week 7	CO2	DVR: Solutions to Count to Infinity Link State Routing: OSPFInternet Domains and Autonomous Systems	Interactive Lecture: PowerPoint presentation Quiz instant feedback through interactive quizzes

	CO3	Perform real-time network traffic analysis and data packet logging.	Hands on: Simulating through CISCO packet Tracer
Week 8	CO2	ASN and Border Gateway Protocol, IPv6 Introduction. IP multicasting. Software Defined Networking (Invited talk) VPN	
Week 9		Mobile IP, Remote Procedure Call: Real-Time Protocol (RTP) and RTCP: Congestion control and Queuing disciplines	
Week 10		Random Early Detection (RED) Quality of Service, Resource reservation protocol, Differentiated Services.	
Week 11		Basics of cryptography -cryptographic hash functions - symmetric and public-key encryption -public key cryptography principles & algorithm.	
Week 12		cipher block modes of operation - Secure Hash Functions – HMAC. Network defence tools: Firewalls, VPNs, Intrusion Detection, and filters - Email privacy: Pretty Good Privacy and S/MIME	

Week 13		Network security protocols in practice-Introduction to Wireshark-SSL -IPsec, and IKE -DNS security- Secure Socket Layer	
Week 14		Transport Layer Security – Secure Electronic Transaction. Access control checks, Virus and Malware detection. Cloud Security aspects of cloud and bigdata.	

5. Partial Delivery

Sl.No:	Description	Topics Beyond Syllabus/ Industry Visit/ Guest Lectures/ Technical Talks/ Workshops/ NPTEL etc.
1.	Software Defined Networking will be delivered by Mr. **Sanjay Padubidri, Director (Business Development),** Intel Technology India Private Limited, Bengaluru.	Guest Lecture (online mode) Note: CIE2 will include questions from this invited lecture.
2.	Advanced Computer Networks, IIT Indore, IIT Gandhi nagar- Course - Swayam – NPTEL.- Course link:	NPTEL
3.	IBM Skill Build courses, "Cybersecurity Fundamentals" (7 hours)- (Questions on this course will be included as part of CIE-1)	IBM Skill Build

6. Instructional Methodologies (Tick the relevant)

Blackboard & chalk ✓	PowerPoint presentations ✓	Student seminars
Mini-Projects ✓	Industry Guest Lectures ✓	Flipped Classroom ✓
Web resources ✓/certification	MOOC ✓	Any other (Specify) Other methods will be adopted as per nature and requirements of the cohort

7. Assessment Methodologies - Indirect (Tick the relevant)

Student Feedback on Course (Exit Survey) ✓	Feedback from Industry Expert✓
Feedback from Alumni	If any other (Please Specify)

8. Course Outcomes to Program Outcome Mapping

Program Outcome / Course Outcome		PO1	PO2	PO3	PO4	PO 5	PO 6	PO 7	PO 8	PO 9	PO 10	PO 11	PO 12
CO1	Analyze the working principles and characteristics of TCP and its role in providing reliable networking applications.	3	3	2	-	2	1	1	-	-	-	-	2
CO2	Analyse the implementation	2	3	2	1	2	1	-	-	-	-	-	2

	details of RIP and OSPF routing protocols adapted by large enterprise networks												
CO3	Explain various multimedia transport protocols and the need for QoS in networks	2	3	2	2	2	1	-	-	-	-	-	1
CO4	Describe the working principles and the purpose of cryptographic algorithms used to provide secure communication	2	3	3	3	2	2	1	-	-	-	-	1
CO5	Apply IP security and Web security concepts in real-life scenarios for creating secure networks	2	3	3	3	2	1	1	-	-	-	-	1

9. Justification of CO-PO Mapping [For all the CO's]

CO1: Analyze the working principles and characteristics of TCP and its role in providing reliable networking applications.

PO	Level of Correlation	Justification
PO1	High	Understanding the principles of TCP and its role in providing reliable network communication requires solid engineering knowledge.
PO2	High	Analyzing TCP's mechanisms and diagnosing issues in real networking applications requires deep problem-solving skills.
PO3	Medium	Designing reliable networking applications and systems using TCP protocols requires knowledge to address issues like congestion control, flow control, and maintaining end-to-end reliability.
PO5	Medium	Using tools like Wireshark, CISCO packet tracer and hardware to analyze TCP traffic and understand how it ensures reliable data transmission in network applications is an important skill at a medium complexity level.
PO6	Low	Understanding the societal impact of reliable networking, such as the importance of TCP in applications like email, web browsing, and online transactions, is a foundational understanding.
PO7	Low	While TCP plays a crucial role in network reliability, the environmental impact is less relevant in the context of analyzing its working principles.
PO12	Medium	Recognizing the importance of staying updated with new developments in TCP is required.

CO2: Analyze the implementation details of RIP and OSPF routing protocols adapted by large enterprise networks

PO	Level of Correlation	Justification
PO1	Medium	Analyzing the implementation of RIP and OSPF requires solid engineering knowledge of how these protocols operate, their behavior in large networks, and their impact on network performance.
PO2	High	This outcome requires higher-level problem analysis, such as troubleshooting routing issues, assessing scalability, and optimizing the performance of RIP/OSPF in enterprise networks
PO3	Medium	Designing solutions for large enterprise networks with RIP and OSPF protocols involves advanced design skills for network topologies, redundancy, and optimization, aligning with Level 2.
PO4	Low	Investigating the detailed performance of RIP and OSPF in different network setups requires basic problem-solving skills and analysis of network issues.
PO5	Medium	Using simulation tools Cisco Packet Tracer to analyze RIP/OSPF configurations and performance falls into medium complexity, as it involves application of knowledge and tools.
PO6	Low	Understanding the broader societal impact of network routing protocols like RIP and OSPF is a lower-level task, mainly recognizing how these protocols affect communication and business.
PO12	Medium	This outcome is important for students to continue learning about new routing protocols, this would be considered a medium-level understanding.

CO3: Explain various multimedia transport protocols and the need for QoS in networks

PO	Level of Correlation	Justification
PO1	Medium	The student will need to understand the technical details of various multimedia transport protocols and the importance of QoS for network optimization, requiring solid engineering knowledge.
PO2	High	This outcome requires students to analyze the real-world challenges in multimedia transport (e.g., packet loss, jitter) and assess QoS requirements in different network scenarios.
PO3	Medium	Designing a network solution that incorporates multimedia transport protocols and provides proper QoS features requires medium skills.
PO4	Medium	Investigating the performance of multimedia protocols under different network conditions and ensuring adequate QoS would involve solving medium level networking problems related to real-time data.
PO5	Medium	Using tools to analyze and simulate multimedia transport (such as Wireshark or NetFlow) and QoS settings requires application of technical skills at a medium complexity level.
PO6	Low	Explaining the societal impact of multimedia communication (e.g., video conferencing, online streaming) and the importance of QoS in ensuring the availability of reliable services in networks is at a basic level.
PO12	Low	Recognizing the importance of continually learning about new multimedia protocols and QoS technologies is crucial, but at this point, it involves a fundamental understanding.

CO4: Describe the working principles and the purpose of cryptographic algorithms used to provide secure communication

PO	Level of Correlation	Justification
PO1	Medium	Cryptographic algorithms requires medium level of knowledge of computational theory, algorithms, and engineering.
PO2	High	Understanding how encryption solves confidentiality issues, how hashing maintains data integrity, and how key exchange ensures secure communication requires problem analysis and solution design skills.
PO3	High	Cryptographic algorithms are essential in designing secure systems, so this outcome is mapped highly to cryptographic principles.
PO4	High	Cryptographic systems require complex investigations to evaluate the strength of encryption algorithms, investigate potential vulnerabilities, and test how cryptographic methods prevent data breaches or attacks.
PO5	Medium	Cryptographic algorithms are implemented using modern tools, libraries, and protocols so this outcome is medium level.
PO6	Medium	Cryptography has significant societal and environmental impacts, such as securing online communications, preventing cybercrime, and protecting personal privacy; this is a secondary application to the direct technical aspects of cryptography.
PO7	Low	Understanding the ethical implications of cryptographic practices is important but secondary to technical knowledge in this domain. Hence low level.
PO12	Low	Cryptography is an ever-evolving field, and staying up to date with new algorithms and cryptographic attacks is key to continued professional development, which is reflected here.

CO5: Apply IP security and Web security concepts in real-life scenarios for creating secure networks

PO	Level of Correlation	Justification
PO1	Medium	Understanding the underlying principles of IPsec and web security requires a medium level of engineering knowledge as it requires implementation of cryptographic protocols and security measures that protect systems and data.
PO2	High	Network security and web security solutions require effective problem analysis to identify potential vulnerabilities and threats.
PO3	High	Implementing IPsec for securing IP traffic between systems and designing web security strategies is central to system design and development.
PO4	High	Investigating network security issues involves understanding IPsec configurations and security protocols which is crucial in identifying weaknesses in systems.
PO5	Medium	Modern tools are vital in implementing both IPsec (and web security solutions so the level is medium.
PO6	Low	Protecting sensitive data such as personal information, financial details, and organizational data helps maintain privacy, but these concepts are often secondary in addressing broader societal issues.
PO7	Low	Ethical concerns around the balance between privacy and security in web applications are required at a low level.
PO12	Low	Staying current with evolving technologies is necessary, but the focus on continual learning is secondary to direct application in secure network design.

10. Assessment Plan

Internal Assessment Plan: 70 Marks				
Sl#	**Component**	**Marks**	**Type of Assessment**	**Timeline**
Continuous Internal Evaluation -1 (20 Marks)				
1	CO1	10	Graded Component 1 (Theory)	Week 3
2	CO2	10	Assignment1- 8 marks IBM Skill dev – 2 marks	Week 5
Continuous Internal Evaluation - 2 (25 Marks)				
3	CO1 - C04	25	Mid Sem Examination (Theory)	Week 9
Continuous Internal Evaluation - 3 (25 Marks)				
4	CO1 - CO5	10	Practical Component – Lab Assignments	Week 14, 15
		15	Mini Project	

Mid Sem Assessment Pattern: 25 Marks		
Sl#	**Content**	
Part A- 5 Marks (1-mark questions)		
1	5 Questions of 1 mark each	5
Part B- 20 Marks (2 marks questions)		
2	10 questions with 2 marks each	20

SEE Assessment Pattern: 30 Marks		
Sl#	**Content**	
Part A - 10 Marks		
1	5 Questions of 2 marks each	10
Part B - 20 Marks		
2	10 Questions of 2 marks each	20

11. Rubrics for Assessment Components

Assessment Component	Type of Component	Rubrics for Assessment
1.	Quiz	Quiz will be conducted for 10 marks. Each right answer carries one mark each. No negative marking for wrong answers.
	Assignment	Hands-On test will be conducted for 10 marks. Students work individually on their assigned tasks.
2.	Mid Sem	Test will be conducted for 25 marks and will be evaluated according to Scheme of Evaluation prepared by team of course faculty.
3.	Practical Component	Lab Assignments = 10 marks Mini Project + viva = 10 + 5 marks
4.	SEE	Test will be conducted out of 30 marks and will be evaluated according to Scheme of Evaluation prepared by team of course faculty.

12. Detailed Rubrics of Assessment Components

PART A

Lab Marks Rubrics(10 Marks)

#	Criteria	Measuring Methods	Excellent	Good	Poor
1	Understanding of problem statement. (2 Marks)	Observations	Student exhibits thorough understanding of requirements for the problem (2 M)	Student has sufficient understanding of requirements for the problem. (1 M)	Student does not have a clear understanding of requirements for the problem. (0 M)
2	Execution (2 Marks)	Observations	Student demonstrates the execution of the program with optimized code and shows the output Appropriate validations with all test cases are handled. (2 M)	Student demonstrates the execution of the program without optimization of the code and shows the output. (1 M)	Student has not executed the program. (0 M)

3	Results and Documentation (2 Marks)	Observations	Documentation with appropriate comments and output is covered in data sheets and manual. (2 M)	Documentation with only few comments and only few output cases is covered in data sheets and manual. (1 M)	Documentation with no comments and no output cases is covered in data sheets and manual. (0 M)
4	Quiz (Max: 4 marks)				

PART B	Mini Project Rubrics (15 Marks)			
Parameters	**Excellent (5)**	**Good (4)**	**Satisfactory (2-3)**	**Not Satisfactory (1)**
Problem-Solving (5 Marks)	Uses advanced problem-solving skills to create innovative and effective solutions.	Uses good problem-solving skills to create effective solutions.	Uses basic problem-solving skills with partially effective solutions.	Uses poor problem-solving skills with ineffective or incorrect solutions.

Project demonstrations and viva voce (5 Marks)	Present the whole project in organized manner and competently address the and handle the questions from audiences. Show the demonstration without struggling.	Present the whole project in organized manner and competently address the and handle the questions from audiences. Show the demonstration with struggling.	Present the whole project in un organized manner and competently address the and handle the questions from audiences.	Presentation is not clear and lacked in answering the questions
Report (5 marks)	All the required information is included, report is organized according to the templates and submitted with the dead line.	Most of the required information is included, report is organized according to the templates and submitted with the dead line.	Necessary information is included with some irrelevant information. Report partially follows the given template and submission exceeded the given dead line.	The report is not organized and important information is missing. submission exceeded the given dead line.

13. Course Policy

- All the students
  - should bring their personal computers (fully charged) to the classroom.
  - should have an RVU mail ID.
  - should be able to connect to both RVCE and RVU WiFi.
- Use of mobile phones is not allowed during class hours. Also, they should not be connected to WiFi.
- In general, late submission by one day, without prior permission, will result in a penalty of 25%. Late submission beyond two days will not be accepted.
- Being late by more than 5 minutes in the first session and by more than 2 minutes in the remaining sessions will not be given attendance. Also, latecomers are required to not disturb others in the classroom.

Reviewed By (Name, Affiliation & Date):

Program Head (Name, Sign, Date): **SoCSE Dean (Sign & Date)**

Version History	Prepared by	Date	Remarks
1:0	Prof. Sheba Pari	9 Jan 25	Ref: Course Design document
2:0	Prof. Chandramouleeswaran Sankaran (Mouli)	12 Jan 25	Updated the syllabus, CIE components and formatting

******