RV UNIVERSITY Go, change the world an initiative of RV EDUCATIONAL INSTITUTIONS	School of Computer Science & Engineering	
	Program	**B.Tech (H)**
	Academic Year	**2024 – 25**
	Academic Term	**Jan 25 – May 25**

COURSE SYLLABUS

Semester: VI

Network Security
Category : MAJOR COMPUTER SCIENCE CORE
(Theory and Lab)

Course Code	:	CS3403	**CIE**	**:**	**70 Marks**
Credits **L:T:P Hours**	:	4 3:0:2	**SEE**	**:**	**30 Marks**
Total Hours	:	45 L + 30 P	**SEE Duration :**	**:**	**2:00 Hours**

Prerequisite:

Sem 4: CS2120 – Computer Networks

Course 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.

Unit I	12 Hrs

Transmission Control Protocol (TCP):

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 II	12 Hrs
Routing Protocols and SDN: 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.	
Unit III	**6 Hrs**
VPN and QoS: 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 IV	**8 Hrs**
Basics of Cryptography: 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 V	**7 Hrs**
Networking Tools: 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:-	
CO 1	Analyse the working principles and characteristics of TCP and its role in providing reliable networking applications.
CO 2	Analyse the implementation details of RIP and OSPF routing protocols adapted by large enterprise networks
CO 3	Explain various multimedia transport protocols and the need for QoS in networks
CO 4	Describe the working principles and the purpose of cryptographic algorithms used to provide secure communication
CO 5	Apply IP security and Web security concepts in real-life scenarios for creating secure networks

Text Books	
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 Materials	
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.

Lab Plan (30 Hours)

a) Lab exercises will be conducted in the newly built Network Security Lab (A-Block, Room No. 301).

b) The lab will be having network equipment that include L2 and L3+ switches with each team of students having dedicated access to them.

c) Students will be given hands-on experience to crimp the Ethernet cables for their experiments using the crimp tool and also to check the connections using LAN tester.

d) Each team will be given two Desktops to configure the network devices and interconnect them based on the configuration set on the devices and test them by verifying the network connections between the hosts on different networks.

LABORATORY ACTIVITIES

Sl. No.	Activities – TBD
1.	Construct networks using switches and routers by configuring them - HW lab
2.	Construct VLANs and perform inter-VLAN routing using switches
3.	Traffic congestion control related simulations on Cisco packet tracer.
4..	Understand the concept and operation of RIP using packet tracer
5.	Construct multiple networks and understand the operation of OSPF Protocol using packet tracer
6.	Configure IPSec to open a VPN tunnel between two machines on different networks
7.	Perform real-time network traffic analysis and data packet logging using Snort
8.	Implement Firewall rules using snort
9.	Generate the network attack and detect the attack using Snort
10.	Analyse SSL/TLS and IPsec/IKE traffic using Wireshark
11.	Use Java code to implement cryptographic algorithms

******