(DEEMED TO BE UNIVERSITY)

NETWORK PROTOCOLS AND SECURITY

23EC2210R

LAB WORKBOOK

TEAM NPS

NETWORK PROTOCOLS AND SECURITY – 23EC2210R

(DEEMED TO BE UNIVERSITY)

NETWORK PROTOCOLS AND SECURITY

Course Code: 23EC2210R

Student ID	
Student Name	
Branch	
Section	
Academic Year	
Semester	

Table of Contents

Regular:

A.Y. 2024-25 LAB CONTINUOUS EVALUATION

Sl. No.	Date	Experiment Name	Pre-Lab (10M)	In-Lab (25M)			Post-Lab (10M)	Viva Voce (5M)	Total (50M)	Faculty Signature
				Program / Procedure (5M)	Data and Results (10M)	Analysis & Inference (10M)				
For Regular, Advanced and Peer Mentors:										
1.		Introduction to the laboratory and the tool used Cisco packet tracer								
2.		Execute the following networking commands like ipconfig, tracert, telnet, netsh, ping, nslookup and netstat in the command prompt with simple topology.								
3.		Configuration of basic switch setup using Huawei/Cisco network switch								
4.		Construction of Different VLANS and TRUNKING using cisco packet tracer								
5.		Configuration of Encapsulation dot 1Q using cisco packet tracer								
6.		Implementation of Smart home using Cisco packet tracer and verify the configuration								
7.		Configuration of ARP and Static Routing using Cisco network switch and verify the connectivity								

Sl. No.	Date	Experiment Name	Pre-Lab (10M)	In-Lab (25M)			Post-Lab (10M)	Viva Voce (5M)	Total (50M)	Faculty Signature
				Program / Procedure (5M)	Data and Results (10M)	Analysis & Inference (10M)				
8.		Configuration of RIP and OSPF using Cisco network switch and verify the connectivity								
9.		Configuration of Network address translation in Cisco packet tracer and verify the configuration								
10.		Configure the Standard and Extended Access Control List using cisco packet tracer and verify the configuration								
11.		Configuration of SMTP, FTP, DNS, HTTP and DHCP in Cisco packet tracer and verify the connection								
12.		Write a python program for Transposition Technique using Rail fence Technique and columnar Technique.								
13		Write a python program to implement of RSA Algorithm								
14		Write a python program to implement of S-DES Algorithm								

Experiment #	<TO BE FILLED BY STUDENT>	**Student ID**	<TO BE FILLED BY STUDENT>
Date	<TO BE FILLED BY STUDENT>	**Student Name**	<TO BE FILLED BY STUDENT>

Lab 1: Introduction to the laboratory and the tool used Cisco packet tracer

Date of the Session:___/___/____ Session Time:____to_____

Learning outcome:

- Understand the purpose and importance of using a network simulation tool like Cisco Packet Tracer.
- Gain familiarity with the user interface and basic functionality of Cisco Packet Tracer.
- Learn how to navigate and explore the virtual network environment within Cisco Packet Tracer.
- Acquire knowledge of the various networking devices and components available in Cisco Packet Tracer and their respective functions.

Pre-Lab Task:

1. What is the purpose of a laboratory in the context of networking and IT?

2. Why is it important to familiarize yourself with the tools and equipment used in a networking laboratory?

3. What is Cisco Packet Tracer, and what is its primary function?

4. What are the key features and capabilities of Cisco Packet Tracer?

Experiment #	<TO BE FILLED BY STUDENT>	**Student ID**	<TO BE FILLED BY STUDENT>
Date	<TO BE FILLED BY STUDENT>	**Student Name**	<TO BE FILLED BY STUDENT>

In Lab Task:

Lab 1: Introduction to the laboratory and the tool used Cisco packet tracer

Writing space for the Problem: (For Student's use only)

Experiment #	<TO BE FILLED BY STUDENT>	**Student ID**	<TO BE FILLED BY STUDENT>
Date	<TO BE FILLED BY STUDENT>	**Student Name**	<TO BE FILLED BY STUDENT>

Experiment #	<TO BE FILLED BY STUDENT>	**Student ID**	<TO BE FILLED BY STUDENT>
Date	<TO BE FILLED BY STUDENT>	**Student Name**	<TO BE FILLED BY STUDENT>

VIVA-VOCE Questions (In-Lab):

1. What is the purpose of a laboratory environment in networking education?
2. Why is it beneficial to use a network simulation tool like Cisco Packet Tracer?
3. Describe some advantages of using Cisco Packet Tracer over physical equipment for network simulations.
4. How does Cisco Packet Tracer replicate real-world networking scenarios?
5. What are the key components and tools available in Cisco Packet Tracer?

Experiment #	<TO BE FILLED BY STUDENT>	**Student ID**	<TO BE FILLED BY STUDENT>
Date	<TO BE FILLED BY STUDENT>	**Student Name**	<TO BE FILLED BY STUDENT>

Post Lab Task:

1. What is the purpose of a laboratory in networking, and why is it important to practice with tools like Cisco Packet Tracer?

2. How can Cisco Packet Tracer be used to simulate network environments and test different networking scenarios?

3. What are the key features and capabilities of Cisco Packet Tracer that make it a valuable tool for network simulation and learning?

4. How can you create a basic network topology using Cisco Packet Tracer, and what are the essential components needed for a functioning network?

Evaluator Remark (if Any):	**Marks Secured: _____out of 50**
	Signature of the Evaluator with Date

Experiment #	<TO BE FILLED BY STUDENT>	**Student ID**	<TO BE FILLED BY STUDENT>
Date	<TO BE FILLED BY STUDENT>	**Student Name**	<TO BE FILLED BY STUDENT>

Lab 2: Execute the following networking commands like ipconfig, tracert, telnet, netsh, ping, nslookup and netstat in the command prompt prompt with simple topology.

Date of the Session:___/___/____ Session Time:____to_____

Learning outcome:

- Understand the purpose of ipconfig and use ipconfig to display network configuration information for a Windows computer.
- Learn how to use ping to test network connectivity to a remote host.
- Learn how to use tracert and netstat to trace the route taken by network packets to a destination.
- Understand the purpose of nslookup (Name Server Lookup) and use nslookup to query DNS servers for information about domain names and IP addresses.

Pre-Lab Task:

1. Ensure you have access to a Windows computer or virtual machine where you can practice the various DOS commands.

2. Review fundamental networking concepts like IP addresses, DNS, and routing. Understand what these commands are used for and why.

3. Before starting the lab, use ping to verify that your Windows machine has network connectivity. This will also help you practice the ping command.

4. Familiarize yourself with the syntax and basic usage of each command. You don't need to memorize them, but knowing the basics helps.

Experiment #	<TO BE FILLED BY STUDENT>	**Student ID**	<TO BE FILLED BY STUDENT>
Date	<TO BE FILLED BY STUDENT>	**Student Name**	<TO BE FILLED BY STUDENT>

In Lab Task:

Lab 2: Executing the commands ipconfig, tracert, telnet, netsh, ping, nslookup and netstat in the command prompt

Writing space for the Problem: (For Student's use only)

1. **ipconfig command**

2. **ping command**

3. **tracert command**

4. telnet command

5. netsh command

6. nslookup command

7. netstat command

Experiment #	<TO BE FILLED BY STUDENT>	**Student ID**	<TO BE FILLED BY STUDENT>
Date	<TO BE FILLED BY STUDENT>	**Student Name**	<TO BE FILLED BY STUDENT>

VIVA-VOCE Questions (In-Lab):

1. What is the primary purpose of the ipconfig command?
2. How does tracert determine the route a packet takes to reach a destination host?
3. What is netsh, and how is it used for configuring network settings?
4. Describe the primary function of the nslookup command.
5. What is the role of the netstat command in a network environment?

Experiment #	<TO BE FILLED BY STUDENT>	**Student ID**	<TO BE FILLED BY STUDENT>
Date	<TO BE FILLED BY STUDENT>	**Student Name**	<TO BE FILLED BY STUDENT>

Post Lab Task:

1. Describe a situation where you might use the tracert command in a real-world networking problem.

2. Provide an example of a specific network configuration task that you performed using the netsh command during the lab. What were the steps involved in accomplishing this task?

3. Describe the types of information you obtained from the netstat command during the lab.

Evaluator Remark (if Any):	**Marks Secured: _____out of 50**
	Signature of the Evaluator with Date

Experiment #	<TO BE FILLED BY STUDENT>	**Student ID**	<TO BE FILLED BY STUDENT>
Date	<TO BE FILLED BY STUDENT>	**Student Name**	<TO BE FILLED BY STUDENT>

Lab 3: Configuration of basic switch setup using Huawei/Cisco network switch.

Date of the Session:_____/___/____ **Session Time:____to_____**

Learning outcome:

- Identify and understand the physical components of a Huawei network switch, such as ports, LEDs, and console interfaces.
- Understand the concept of user authentication and password management.
- Develop the ability to navigate the switch's CLI, including using basic commands to view system information and switch status.
- Understand the essential settings, such as hostname, IP address, and gateway to make the switch accessible on the network
- Develop an understanding of best practices for switch configuration and management to ensure a stable and secure network.

Pre-Lab Task

1. Review the documentation and manuals for the specific Huawei or Cisco switch model you will be working with. Familiarize yourself with its features, capabilities, and command-line interface (CLI).

2. Describe the basic components and ports found on a Huawei network switch, and explain their functions.

3. Give some common network switch configurations that need to be considered before setting up a switch, such as VLANs, port security, and spanning tree protocol?

Experiment #	<TO BE FILLED BY STUDENT>	**Student ID**	<TO BE FILLED BY STUDENT>
Date	<TO BE FILLED BY STUDENT>	**Student Name**	<TO BE FILLED BY STUDENT>

4. To connect a Huawei network switch to other networking devices, such as routers, servers, and computers?

In Lab Task:

Basic switch setup using Huawei network switch

Writing space for the Problem :(For Student's use only)

Device Configuration details

Device Type	Device Name(Label)	IP Address	Subnet Mask

Experiment #	<TO BE FILLED BY STUDENT>	**Student ID**	<TO BE FILLED BY STUDENT>
Date	<TO BE FILLED BY STUDENT>	**Student Name**	<TO BE FILLED BY STUDENT>

Switch Configuration Commands:

Experiment #	<TO BE FILLED BY STUDENT>	**Student ID**	<TO BE FILLED BY STUDENT>
Date	<TO BE FILLED BY STUDENT>	**Student Name**	<TO BE FILLED BY STUDENT>

VIVA-VOCE Questions (In-Lab):

1. What is the purpose of a network switch, and how does it differ from other networking devices?
2. Describe the steps involved in the initial setup of a Huawei network switch.
3. How do you connect to a Huawei switch for configuration purposes?
4. What is the default login username and password for a Huawei switch?
5. Explain the process of assigning an IP address to a Huawei switch.

Experiment #	<TO BE FILLED BY STUDENT>	**Student ID**	<TO BE FILLED BY STUDENT>
Date	<TO BE FILLED BY STUDENT>	**Student Name**	<TO BE FILLED BY STUDENT>

Post Lab Task:

1. What is the purpose of a network switch, and why is it an essential component in a computer network?

2. Describe the basic setup process for a Huawei network switch, including the necessary connections and initial configurations.

3. What are the different types of interfaces available on a Huawei switch, and how can they be used to connect devices in a network?

Evaluator Remark (if Any):	**Marks Secured: _____out of 50**
	Signature of the Evaluator with Date

Experiment #	<TO BE FILLED BY STUDENT>	**Student ID**	<TO BE FILLED BY STUDENT>
Date	<TO BE FILLED BY STUDENT>	**Student Name**	<TO BE FILLED BY STUDENT>

Lab 4: Construction of different VLANS and TRUNKING using cisco packet tracer

Date of the Session:___/___/____ **Session Time:____to_____**

Learning Outcome:

- Students should be able to explain what VLANs are and understand their purpose in network segmentation
- Understand how VLANs can improve network performance, security, and management.
- Configure VLANs on network switches, including creating, modifying, and deleting VLANs.
- Understand the concept of VLANs (Virtual Local Area Networks) and their significance in network segmentation and management.
- Understand and configure trunk ports on switches to allow the passage of VLAN traffic between switches.

Pre-Lab Task:

1. Identify the number of VLANs you need, their purpose, and the devices that will be part of each VLAN?

2. Ensure you have access to the necessary equipment, including the network switch that supports VLANs and trunking.

3. Plan the IP addressing scheme for your network, including IP subnets and subnet masks and Allocate IP addresses for your devices within each VLAN.

Experiment #	<TO BE FILLED BY STUDENT>	Student ID	<TO BE FILLED BY STUDENT>
Date	<TO BE FILLED BY STUDENT>	Student Name	<TO BE FILLED BY STUDENT>

In Lab Task: Construction of different VLANS and TRUNKING using cisco packet tracer

Creating different VLANs (Virtual LANs) and configuring trunking between switches are common tasks in networking, and they can be effectively simulated using Cisco Packet Tracer. Here are the steps involved in constructing different VLANs and trunking using Cisco Packet Tracer:

Construction of Different VLANs:

1. Open Cisco Packet Tracer:

- Launch the Cisco Packet Tracer application on your computer.

2. Create the Network Topology:

- Add the required network devices to the workspace. For VLANs, you'll need multiple switches. Connect them using appropriate cables.

3. Access Switches:

- Double-click on each switch to access the device configuration.

4. Enter Global Configuration Mode:

- Enter global configuration mode using the following command:

  Switch> enable Switch# configure terminal

5. Create VLANs:

- Use the following command to create VLANs. Replace **<vlan_id>** with the desired VLAN ID.

  Switch(config)# vlan <vlan_id>

6. Assign VLAN Names:

- Optionally, assign names to the VLANs for better identification:

Switch(config-vlan)# name <vlan_name>

7. Assign VLANs to Switch Ports:

- Navigate to individual switch interfaces and assign them to specific VLANs:

  Switch(config)# interface <interface_type> <interface_number>

  Switch(config-if)# switchport mode access

  Switch(config-if)# switchport access vlan <vlan_id>

- Repeat this process for each switch interface and VLAN.

8. Verify VLAN Configuration:

- Use the following commands to verify your VLAN configuration:

  Switch# show vlan Switch# show interfaces switchport

Experiment #	<TO BE FILLED BY STUDENT>	**Student ID**	<TO BE FILLED BY STUDENT>
Date	<TO BE FILLED BY STUDENT>	**Student Name**	<TO BE FILLED BY STUDENT>

Configuration of Trunking:

1. Connect Two Switches:

- Ensure that two switches are connected. Use a straight-through cable between their trunking interfaces.

2. Configure Trunking on the Interface:

- Access the configuration mode of the interface connected to the other switch and configure it as a trunk port:

  Switch(config)# interface <interface_type> <interface_number>

  Switch(config-if)# switchport mode trunk

3. Set Allowed VLANs:

- Optionally, restrict the allowed VLANs on the trunk to improve security:

  Switch(config-if)# switchport trunk allowed vlan <vlan_list>

- Replace **<vlan_list>** with a comma-separated list of VLAN IDs.

4. Verify Trunk Configuration:

- Use the following command to verify the trunk configuration:

  Switch# show interfaces trunk

5. Repeat for Additional Switches:

- If you have more switches, repeat the trunking configuration between them, connecting the trunking interfaces.

6. Test Connectivity:

- Connect devices to the VLANs on different switches and verify that they can communicate across the network.

By following these steps, you can construct different VLANs and configure trunking between switches using Cisco Packet Tracer.

Experiment #	<TO BE FILLED BY STUDENT>	**Student ID**	<TO BE FILLED BY STUDENT>
Date	<TO BE FILLED BY STUDENT>	**Student Name**	<TO BE FILLED BY STUDENT>

Writing space for the Problem: (For Student's use only)

Device Configuration details

Device Name(Label)	Interface	IP Address	Subnet Mask	Default Gateway address

Experiment #	<TO BE FILLED BY STUDENT>	Student ID	<TO BE FILLED BY STUDENT>
Date	<TO BE FILLED BY STUDENT>	Student Name	<TO BE FILLED BY STUDENT>

VLAN configuration in Switches
Switch-A

Experiment #	<TO BE FILLED BY STUDENT>	Student ID	<TO BE FILLED BY STUDENT>
Date	<TO BE FILLED BY STUDENT>	Student Name	<TO BE FILLED BY STUDENT>

VLAN configuration in Switches
Switch-B

Experiment #	<TO BE FILLED BY STUDENT>	**Student ID**	<TO BE FILLED BY STUDENT>
Date	<TO BE FILLED BY STUDENT>	**Student Name**	<TO BE FILLED BY STUDENT>

VIVA-VOCE Questions (In-Lab):

1. Explain the concept of trunking. How does it differ from access ports on a network switch?
2. What are the advantages and disadvantages of using VLANs in a network design?
3. Can you describe the process of creating a new VLAN on a network switch?
4. How do you assign ports to a specific VLAN on a network switch?
5. How can you verify that your VLAN and trunking configurations are working correctly??

Experiment #	<TO BE FILLED BY STUDENT>	**Student ID**	<TO BE FILLED BY STUDENT>
Date	<TO BE FILLED BY STUDENT>	**Student Name**	<TO BE FILLED BY STUDENT>

Post Lab Task:

1. Were the VLAN configurations on the network switch error-free, and did they match your pre-lab plan?

2. How does this lab experiment align with real-world scenarios or challenges related to network design and VLAN configuration?

3. How did you configure trunk ports to carry traffic for multiple VLANs?

Evaluator Remark (if Any):	**Marks Secured: _____out of 50**
	Signature of the Evaluator with Date

Experiment #	<TO BE FILLED BY STUDENT>	**Student ID**	<TO BE FILLED BY STUDENT>
Date	<TO BE FILLED BY STUDENT>	**Student Name**	<TO BE FILLED BY STUDENT>

Lab 5: Configuration of Encapsulation dot 1Q using cisco packet tracer

Date of the Session:___/___/____ **Session Time:____to_____**

Learning outcome:

- Learners will learn how to configure the Encapsulation dot1Q protocol, which is used to tag VLAN information on Ethernet frames.
- Understand the importance of VLAN tagging and how it enables VLAN communication across different network devices..

Pre-Lab Task:

1. What is the purpose of encapsulation dot1Q in networking, and why is it commonly used in Ethernet networks?

2. Explain the concept of VLAN tagging and how it is achieved using encapsulation dot1Q.

3. Discuss the advantages and benefits of using encapsulation dot1Q in a network environment, such as improved scalability, flexibility, and security.

Experiment #	<TO BE FILLED BY STUDENT>	**Student ID**	<TO BE FILLED BY STUDENT>
Date	<TO BE FILLED BY STUDENT>	**Student Name**	<TO BE FILLED BY STUDENT>

In Lab Task:

Configuration of Encapsulation dot 1Q using cisco packet tracer

Writing space for the Problem:(For Student's use only)

Device Configuration details

Device Name(Label)	Interface	IP Address	Subnet Mask	Default Gateway address

Experiment #	<TO BE FILLED BY STUDENT>	**Student ID**	<TO BE FILLED BY STUDENT>
Date	<TO BE FILLED BY STUDENT>	**Student Name**	<TO BE FILLED BY STUDENT>

VIVA-VOCE Questions (In-Lab):

1. What is encapsulation dot1Q, and what is its purpose in networking?
2. What is the significance of the VLAN ID in encapsulation dot1Q?
3. Explain the differences between encapsulation dot1Q and other trunking protocols, such as ISL (Inter-Switch Link).
4. How does encapsulation dot1Q support VLAN tagging and segmentation of traffic?
5. How can you remove the encapsulation dot1Q configuration from an interface if needed?

Experiment #	<TO BE FILLED BY STUDENT>	**Student ID**	<TO BE FILLED BY STUDENT>
Date	<TO BE FILLED BY STUDENT>	**Student Name**	<TO BE FILLED BY STUDENT>

Post Lab Task:

1. Describe the network topology you used for configuring Encapsulation dot1Q using Cisco Packet Tracer.

2. What steps or commands did you use to enable and configure VLAN tagging?

3. Explain the purpose and significance of VLAN tagging using Encapsulation dot1Q.

Evaluator Remark (if Any):	**Marks Secured: _____out of 50**
	Signature of the Evaluator with Date

Experiment #	<TO BE FILLED BY STUDENT>	**Student ID**	<TO BE FILLED BY STUDENT>
Date	<TO BE FILLED BY STUDENT>	**Student Name**	<TO BE FILLED BY STUDENT>

Lab 6: Implementation of Smart home using Cisco packet tracer and verify the configuration

Date of the Session:___/___/____ Session Time:____to_____

Learning outcome:

- Understanding IoT Concepts and Gain a solid understanding of IoT and its applications in smart homes
- Configure Cisco routers and switches to create a functional network for the smart home.
- Learners will gain a comprehensive understanding of Smart Home technology and its applications.
- Learners will develop skills in designing network infrastructures that support Smart Home implementations

Pre-Lab Task:

1. Mention the concept of a smart home and its benefits.

2. Give some examples of devices or systems that can be incorporated into a smart home setup?

3. Discuss the importance of network infrastructure in enabling a smart home environment.

Experiment #	<TO BE FILLED BY STUDENT>	**Student ID**	<TO BE FILLED BY STUDENT>
Date	<TO BE FILLED BY STUDENT>	**Student Name**	<TO BE FILLED BY STUDENT>

Home Automation Basics – Beginners Guide

Although not many people can see the need for having their smart fridge connected to the Internet, most people will find the ability to remotely control lights, security cameras and other home appliances very useful. If you are thinking about adding smart devices to your home then this guide to smart homes and home automation will give you a good basic understanding of how smart devices are connected and how they are controlled.

What is Home Automation?

Home automation or **domestics** is building automation for a home, called a **smart home** or **smart house**. It involves the control and automation of lighting. Home automation is one of several areas of the IOT (internet of things), and is often called **Home IOT**.

There are three distinct levels of home automation.

1. Monitoring
2. Control
3. Automation

Monitoring

The ability to view status of systems i.e

- What is the temperature?
- Is the door locked?
- Is The Light on or off

Control

The ability to change the state of a systems i.e

- Turn up the heating.
- Lock the Door
- Turning the light on or off

Automation

The ability to change the state of a system automatically in response to an event. i.e.

- Turn on the heating if the outside temperature falls below a certain temperature.
- Turn the lights off when no one is a home.

Currently most smart home systems are at the **control level.**

Smart Home – Automation System Components

A home automation system will consist of

- End Devices like switches, sensors ,lights, locks etc
- Connection devices like hubs and Gateways.
- A Network or networks e.g. Wi-Fi, Zigbee etc
- Internet connection – maybe optional

Experiment #	<TO BE FILLED BY STUDENT>	**Student ID**	<TO BE FILLED BY STUDENT>
Date	<TO BE FILLED BY STUDENT>	**Student Name**	<TO BE FILLED BY STUDENT>

Local Control and Cloud Control

All homes should be able to be controlled locally from within the home. This doesn't mean that they should have manual switches, but that they should be controllable across a local network. They should also **IMO** be controllable and **fully functional** without an Internet connection. In other words if you loose the Internet connection you should still be able to turn your lights on and off. Unfortunately not all systems will operate without an Internet connection. This article is worth reading.

As a General rule of thumb **Zwave** and **Zigbee** networks and devices will operate without an Internet connection. **Wi-Fi devices** will generally **require** an Internet connection. If the device is controllable directly using a smart phone then it requires an Internet connection. This reddit discussion is worth reading.

The Role of the Cloud In Smart Homes

Many Internet devices especially **Wi-Fi devices** are dependent on an Internet connection, and cloud services to function. Generally when you set up these devices you **register them** with the manufacturer on a cloud service. They can then be controlled via an App on a smart phone, Alexa etc but will require an Internet connection to function correctly. Although these devices are easy to setup and operate they are useless without an Internet connection. IMO the Internet should represent an alternative way of controlling devices, and not the only way.

In Lab Task: Implementation of Smart home using Cisco packet tracer

Writing space for the Problem: (For Student's use only)

Experiment #	<TO BE FILLED BY STUDENT>	**Student ID**	<TO BE FILLED BY STUDENT>
Date	<TO BE FILLED BY STUDENT>	**Student Name**	<TO BE FILLED BY STUDENT>

Experiment #	<TO BE FILLED BY STUDENT>	**Student ID**	<TO BE FILLED BY STUDENT>
Date	<TO BE FILLED BY STUDENT>	**Student Name**	<TO BE FILLED BY STUDENT>

VIVA-VOCE Questions (In-Lab):

1. What is a smart home, and how does it differ from a traditional home setup?
2. Explain the concept of the Internet of Things (IoT) and its role in smart home technology.
3. What communication protocols are commonly used in smart home devices, and how do they function?
4. What security considerations should be taken into account when configuring a smart home network in Packet Tracer?

Experiment #	<TO BE FILLED BY STUDENT>	**Student ID**	<TO BE FILLED BY STUDENT>
Date	<TO BE FILLED BY STUDENT>	**Student Name**	<TO BE FILLED BY STUDENT>

Experiment #	<TO BE FILLED BY STUDENT>	**Student ID**	<TO BE FILLED BY STUDENT>
Date	<TO BE FILLED BY STUDENT>	**Student Name**	<TO BE FILLED BY STUDENT>

Post Lab Task:

1. Describe the network topology you used for implementing the smart home in Cisco Packet Tracer. What devices were involved, and how were they interconnected?

2. Explain the concept of a smart home and its benefits.

3. Discuss the protocols or technologies you implemented to enable communication and control within the smart home environment.

Evaluator Remark (if Any):	**Marks Secured: _____out of 50**
	Signature of the Evaluator with Date

Experiment #	<TO BE FILLED BY STUDENT>	**Student ID**	<TO BE FILLED BY STUDENT>
Date	<TO BE FILLED BY STUDENT>	**Student Name**	<TO BE FILLED BY STUDENT>

Lab 7: Configuration of ARP and Static Routing using Cisco network switch and verify the connectivity

Date of the Session:___/___/____ **Session Time:____to_____**

Learning outcome:

- Understand the role of a router in a computer network and its importance in facilitating communication between different network segments.
- Gain familiarity with Huawei L3 network switches and their specific features and capabilities related to router functionality and static routing.

Pre-Lab Task:

1. Explain the purpose of a router in a network infrastructure. How does a router differ from other networking devices, such as switches and hubs?

2. Describe the key components and interfaces of a Huawei L3 network switch that enable routing functionality. What features or capabilities does the switch offer for routing?

3. What is static routing, and how does it differ from dynamic routing protocols? When would it be appropriate to use static routing in a network setup?

Experiment #	<TO BE FILLED BY STUDENT>	**Student ID**	<TO BE FILLED BY STUDENT>
Date	<TO BE FILLED BY STUDENT>	**Student Name**	<TO BE FILLED BY STUDENT>

In Lab Task:

Basic Router setup using Huawei L3 network switch and Static Routing.

Writing space for the Problem:(For Student's use only)

Device Configuration details

Device Name(Label)	Interface	IP Address	Subnet Mask	Default Gateway address

Experiment #	<TO BE FILLED BY STUDENT>	**Student ID**	<TO BE FILLED BY STUDENT>
Date	<TO BE FILLED BY STUDENT>	**Student Name**	<TO BE FILLED BY STUDENT>

Experiment #	<TO BE FILLED BY STUDENT>	**Student ID**	<TO BE FILLED BY STUDENT>
Date	<TO BE FILLED BY STUDENT>	**Student Name**	<TO BE FILLED BY STUDENT>

Post Lab Task:

1. Describe the topology you configured using the Huawei L3 network switch and the router. What devices were connected, and what was the purpose of each device in the network?

2. Explain the concept of static routing and its significance in network environments. How did you configure static routes on the Huawei L3 network switch to enable communication between different networks?

3. Describe the syntax and parameters used for configuring static routes on the Huawei L3 network switch. How did you specify the destination network and the next-hop router?

Evaluator Remark (if Any):	**Marks Secured: _____out of 50**
	Signature of the Evaluator with Date

Experiment #	<TO BE FILLED BY STUDENT>	**Student ID**	<TO BE FILLED BY STUDENT>
Date	<TO BE FILLED BY STUDENT>	**Student Name**	<TO BE FILLED BY STUDENT>

Lab 8: Configuration of RIP and OSPF using Cisco network switch and verify the connectivity

Date of the Session:_____/___/____ **Session Time:____to_____**

Learning outcome:

- Understanding OSPF Basics and its role in dynamic routing protocols.
- Demonstrate an understanding of basic Cisco switch configuration, including accessing the command-line interface (CLI) and configuring interfaces.
- Identify and specify the OSPF router ID and Choose the OSPF network type (point-to-point, broadcast, etc.) and configure it accordingly.
- Understand the concept of hierarchical OSPF and area design**.**

Pre-Lab Task:

4. Mention the purpose and benefits of dynamic routing protocols such as RIP (Routing Information Protocol) and OSPF (Open Shortest Path First) in a network environment?

5. Ensure you have access to the required Cisco network switch (real or simulated) and a terminal emulator tool like PuTTY or SecureCRT for accessing the switch's command-line interface?

6. Clearly define the objectives of your lab, specifying what OSPF configurations you intend to implement and what outcomes you expect to achieve.

Experiment #	<TO BE FILLED BY STUDENT>	Student ID	<TO BE FILLED BY STUDENT>
Date	<TO BE FILLED BY STUDENT>	Student Name	<TO BE FILLED BY STUDENT>

In Lab Task: Configuration of RIP and OSPF using Cisco network switch.

Configuring OSPF (Open Shortest Path First) on a Cisco network switch involves several steps. Here's a basic guide to help you configure OSPF and verify connectivity on a Cisco switch:

Note: OSPF is typically configured on routers rather than switches. If you are working with a Layer 3 switch, you can configure OSPF on the switch. If you are using a Layer 2 switch, you would configure OSPF on a connected router.

1. Access Switch CLI:

- Access the command-line interface (CLI) of your Cisco switch using a console cable, Telnet, or SSH.

2. Enter Global Configuration Mode:

- Enter global configuration mode by typing:

  switch> enable switch# configure terminal

3. Configure OSPF:

- Enter OSPF configuration mode and specify an OSPF process ID (e.g., 1):

  switch(config)# router ospf 1

4. Assign Router ID:

- Assign a router ID to the switch. This can be done manually or left to the system to choose. For manual assignment:

  switch(config-router)# router-id <router_id>

5. Enable OSPF on Interfaces:

- Enable OSPF on the interfaces participating in OSPF. For each interface, use:

switch(config-router)# network <network_address> <wildcard_mask> area <area_id>

6. Verify OSPF Configuration:

- Verify OSPF configuration using the following commands:

  switch# show ip ospf switch# show ip ospf interface

7. Exit Configuration Mode:

- Exit OSPF configuration mode and return to global configuration mode:

  switch(config-router)# exit

8. Save Configuration:

- Save the configuration to ensure it persists after a reboot:

  switch# write memory

9. Verify Connectivity:

- Verify OSPF connectivity by checking OSPF neighbor relationships and routing tables. Use commands such as:

  switch# show ip ospf neighbor switch# show ip route

10. Test Connectivity:

- Test connectivity between devices in different OSPF areas to ensure that OSPF is routing traffic correctly.

11. Troubleshoot if Necessary:

- If there are issues with OSPF adjacency or routing, use troubleshooting commands like:

  switch# show ip ospf interface switch# show ip ospf database

12. Monitor OSPF:

- Continuously monitor OSPF using commands such as:

  switch# debug ip ospf events switch# debug ip ospf adj

13. Disable Debugging:

- Once troubleshooting is complete, disable debugging:

  switch# undebug all

14. Save Final Configuration:

- Save the final configuration to ensure that it is persistent:

  switch# write memory

By following these steps, you can configure OSPF on a Cisco switch, verify the OSPF configuration, and ensure proper connectivity.

Writing space for the Problem: (For Student's use only)

Experiment #	<TO BE FILLED BY STUDENT>	**Student ID**	<TO BE FILLED BY STUDENT>
Date	<TO BE FILLED BY STUDENT>	**Student Name**	<TO BE FILLED BY STUDENT>

Device Configuration details

Device Name(Label)	Interface	IP Address	Subnet Mask	Default Gateway address

Experiment #	<TO BE FILLED BY STUDENT>	**Student ID**	<TO BE FILLED BY STUDENT>
Date	<TO BE FILLED BY STUDENT>	**Student Name**	<TO BE FILLED BY STUDENT>

Configuration for Routers	
Fast Ethernet Port Configuration & Serial Port Configuration	

Experiment #	<TO BE FILLED BY STUDENT>	**Student ID**	<TO BE FILLED BY STUDENT>
Date	<TO BE FILLED BY STUDENT>	**Student Name**	<TO BE FILLED BY STUDENT>

Configuration for Routers	
RIP Configuration	

Configuration for Routers	
OSPF Configuration	

Experiment #	<TO BE FILLED BY STUDENT>	**Student ID**	<TO BE FILLED BY STUDENT>
Date	<TO BE FILLED BY STUDENT>	**Student Name**	<TO BE FILLED BY STUDENT>

VIVA-VOCE Questions (In-Lab):

1. Explain what OSPF stands for and its primary purpose in networking.
2. How does OSPF differ from other routing protocols, such as RIP or EIGRP?
3. Describe the basic steps to configure OSPF on a Cisco network switch.
4. What is the OSPF router ID, and how is it determined?
5. What are OSPF areas, and why are they used in OSPF network design??

Experiment #	<TO BE FILLED BY STUDENT>	**Student ID**	<TO BE FILLED BY STUDENT>
Date	<TO BE FILLED BY STUDENT>	**Student Name**	<TO BE FILLED BY STUDENT>

Post Lab Task:

1. Verify the OSPF configurations to ensure that routing is functioning as expected. Use show commands to check OSPF neighbour relationships, routing tables, and routing information. Confirm that OSPF is redistributing routes correctly?

2. Differentiate the RIP and OSPF configuration by sending traffic between devices in the network to ensure that routing is working as expected?

3. Use show commands (e.g., **show ip route**) to verify that the switch's routing table includes RIP and OSPF-learned routes and that they are correct?

Experiment #	<TO BE FILLED BY STUDENT>	**Student ID**	<TO BE FILLED BY STUDENT>
Date	<TO BE FILLED BY STUDENT>	**Student Name**	<TO BE FILLED BY STUDENT>

Evaluator Remark (if Any):	**Marks Secured: _____out of 50**
	Signature of the Evaluator with Date

Course Title	**NETWORK PROTOCOLS & SECURITY**	**ACADEMIC YEAR: 2024-25**
Course Code(s)	**23EC2210R**	

Experiment #	<TO BE FILLED BY STUDENT>	**Student ID**	<TO BE FILLED BY STUDENT>
Date	<TO BE FILLED BY STUDENT>	**Student Name**	<TO BE FILLED BY STUDENT>

Lab 9: Configuration of Network address translation in Cisco packet tracer

Date of the Session:_____/___/____ **Session Time:____to_____**

Learning outcome:

- Learners will gain a solid understanding of Network Address Translation and its role in IP address translation between private and public networks.
- Learners will acquire hands-on experience in configuring different types of NAT in Cisco Packet Tracer.

Pre-Lab Task:

1. What is Network Address Translation (NAT), and what is its primary purpose in networking?

2. Explain the difference between static NAT and dynamic NAT. When would you use each of these NAT types?

3. What are the benefits and challenges of using NAT in a network environment?

Experiment #	<TO BE FILLED BY STUDENT>	**Student ID**	<TO BE FILLED BY STUDENT>
Date	<TO BE FILLED BY STUDENT>	**Student Name**	<TO BE FILLED BY STUDENT>

In Lab Task:

Configuration of Network address translation in Cisco packet tracer

Writing space for the Problem:(For Student's use only)

Experiment #	<TO BE FILLED BY STUDENT>	**Student ID**	<TO BE FILLED BY STUDENT>
Date	<TO BE FILLED BY STUDENT>	**Student Name**	<TO BE FILLED BY STUDENT>

Experiment #	<TO BE FILLED BY STUDENT>	**Student ID**	<TO BE FILLED BY STUDENT>
Date	<TO BE FILLED BY STUDENT>	**Student Name**	<TO BE FILLED BY STUDENT>

VIVA-VOCE Questions (In-Lab):

1. What is NAT, and what is its primary purpose in computer networks?
2. Explain the difference between private IP addresses and public IP addresses.
3. What is an Access Control List (ACL), and what is its primary purpose in a network?
4. How does an ACL help in controlling traffic flow in a router or a switch?
5. What are the different types of ACLs, and how do they differ in their functionality?

Experiment #	<TO BE FILLED BY STUDENT>	**Student ID**	<TO BE FILLED BY STUDENT>
Date	<TO BE FILLED BY STUDENT>	**Student Name**	<TO BE FILLED BY STUDENT>

Post Lab Task:

1. Describe the network topology you used for configuring Network Address Translation (NAT) in Cisco Packet Tracer. What devices were involved, and how were they interconnected?

2. Discuss the impact of NAT on network security and addressing.

3. Describe any specific translation rules or access control policies you implemented as part of the NAT configuration.

Evaluator Remark (if Any):	**Marks Secured: _____out of 50**
	Signature of the Evaluator with Date

Experiment #	<TO BE FILLED BY STUDENT>	**Student ID**	<TO BE FILLED BY STUDENT>
Date	<TO BE FILLED BY STUDENT>	**Student Name**	<TO BE FILLED BY STUDENT>

Lab 10: Configure the Standard and Extended Access Control List using cisco packet tracer and verify the configuration

Date of the Session:_____/___/____ **Session Time:____to_____**

Learning outcome:

- Learn how to access and navigate Cisco Packet Tracer and Cisco IOS for configuration tasks.
- Gain hands-on experience in creating Standard ACLs using source IP addresses.
- Acquire skills in creating Extended ACLs with criteria including source and destination IP addresses, protocols, and port numbers.
- Apply Standard and Extended ACLs to network interfaces in both inbound and outbound directions.
- Understand the implications of applying ACLs in different directions on network traffic.

Pre-Lab Task:

1 What is an Access Control List (ACL), and why is it important in network security?

2 Explain the difference between Standard and Extended ACLs.

3 Describe the implicit deny rule in ACLs.

Experiment #	<TO BE FILLED BY STUDENT>	**Student ID**	<TO BE FILLED BY STUDENT>
Date	<TO BE FILLED BY STUDENT>	**Student Name**	<TO BE FILLED BY STUDENT>

In Lab Task:

Configure the Standard and Extended Access Control List using cisco packet tracer

Writing space for the Problem:(For Student's use only)

Experiment #	<TO BE FILLED BY STUDENT>	**Student ID**	<TO BE FILLED BY STUDENT>
Date	<TO BE FILLED BY STUDENT>	**Student Name**	<TO BE FILLED BY STUDENT>

Experiment #	<TO BE FILLED BY STUDENT>	**Student ID**	<TO BE FILLED BY STUDENT>
Date	<TO BE FILLED BY STUDENT>	**Student Name**	<TO BE FILLED BY STUDENT>

VIVA-VOCE Questions (In-Lab):

1. What is an Access Control List (ACL), and what is its primary purpose in a network?
2. How does an ACL help in controlling traffic flow in a router or a switch?
3. What are the different types of ACLs, and how do they differ in their functionality?

Experiment #	<TO BE FILLED BY STUDENT>	**Student ID**	<TO BE FILLED BY STUDENT>
Date	<TO BE FILLED BY STUDENT>	**Student Name**	<TO BE FILLED BY STUDENT>

Post Lab Task:

1. What are the primary differences between Standard and Extended ACLs?

2. Describe the steps to create a Standard ACL that permits traffic from the IP range 192.168.10.0/24.

3. Outline the process of applying an Extended ACL to block all HTTP traffic from any source to a specific server with the IP address 10.0.0.5.

4. How would you modify an existing Standard ACL to permit an additional IP address (e.g., 192.168.1.50)?

Evaluator Remark (if Any):	**Marks Secured: _____out of 50**
	Signature of the Evaluator with Date

Experiment #	<TO BE FILLED BY STUDENT>	**Student ID**	<TO BE FILLED BY STUDENT>
Date	<TO BE FILLED BY STUDENT>	**Student Name**	<TO BE FILLED BY STUDENT>

Lab 11: Configuration of SMTP, FTP, DNS, HTTP and DHCP in Cisco packet tracer and verify the connection

Date of the Session:_____/___/____ **Session Time:____to_____**

Learning outcome:

- Learners will gain a solid understanding of SMTP, FTP, DNS, and HTTP
- Learners will acquire hands-on experience in configuring SMTP, FTP, DNS, and HTTP services using Cisco Packet Tracer.
- Understand the basic concepts of DHCP, including IP address allocation, lease duration, and the role of DHCP servers

Pre-Lab Task:

1. Give the purpose and function of SMTP (Simple Mail Transfer Protocol), DNS (Domain Name System), HTTP (Hypertext Transfer Protocol) and FTP (file Transfer Protocol) in a network environment.

2. Mention the importance of security considerations when configuring SMTP, FTP, DNS, and HTTP.

3. Discuss the interdependencies between SMTP, DNS, and HTTP in a network environment.

4. Define the scope of your DHCP implementation project. What are the specific objectives and goals you want to achieve with DHCP?

In Lab Task: Configuration of SMTP, FTP, DNS, HTTP and DHCP in Cisco packet tracer

Implementation of SMTP, FTP, DNS and HTTP in Cisco packet tracer

In Cisco Packet Tracer, you can simulate the implementation of various network protocols such as SMTP (Simple Mail Transfer Protocol), FTP (File Transfer Protocol), DNS (Domain Name System), and HTTP (Hypertext Transfer Protocol) to understand how these protocols work in a network environment. Here are the general steps for implementing these protocols:

SMTP (Simple Mail Transfer Protocol):

1. Topology Setup:
    - Create a network topology in Cisco Packet Tracer with devices such as routers, switches, and PCs.
2. Device Configuration:
    - Configure an email client on a PC (e.g., Outlook) and an email server (e.g., Mail Server) on another PC.
3. SMTP Configuration:
    - On the email client, configure the SMTP settings to point to the IP address or domain name of the email server.

4. Email Testing:
    - Send test emails from the client to the server to simulate the SMTP communication.

FTP (File Transfer Protocol):

1. Topology Setup:
    - Create a network topology with devices that support FTP, such as PCs or servers.
2. Device Configuration:
    - Set up an FTP server on one PC and configure an FTP client on another.
3. FTP Configuration:
    - Configure the FTP client with the server's IP address or domain.
4. File Transfer:
    - Initiate file transfers from the client to the server or vice versa to simulate FTP communication.

DNS (Domain Name System):

1. Topology Setup:
    - Create a network topology with DNS servers, client devices, and routers.
2. Device Configuration:
    - Set up a DNS server on a PC or a dedicated DNS server device. Configure client devices to use the DNS server.
3. DNS Configuration:
    - Populate the DNS server with domain names and corresponding IP addresses.
4. Name Resolution:
    - Test DNS name resolution by attempting to access websites using domain names from client devices.

HTTP (Hypertext Transfer Protocol):

1. Topology Setup:
    - Set up a network topology with web servers, client devices, and routers.
2. Device Configuration:
    - Configure a web server on a PC or a dedicated web server device. Set up web clients on other devices.
3. HTTP Configuration:
    - Populate the web server with web pages or applications.
4. Web Browsing:

- Access web pages hosted on the server from client devices to simulate HTTP communication.

General Tips:

- Router Configuration:
  - Ensure that routers are properly configured to route traffic between devices.
- Addressing:
  - Use proper IP addressing and subnetting to ensure devices can communicate within the network.
- Firewall Settings:
  - Adjust firewall settings on devices if necessary to allow traffic for the respective protocols.
- Packet Tracer Simulation:
  - Utilize Packet Tracer's simulation mode to observe the flow of packets and troubleshoot any issues.

By following these steps, you can simulate the implementation of SMTP, FTP, DNS, and HTTP in Cisco Packet Tracer, allowing you to understand how these protocols operate in a network environment.

Writing space for the Problem: (For Student's use only)

Device Configuration details

Device Name(Label)	Interface	IP Address	Subnet Mask	Default Gateway address

Experiment #	<TO BE FILLED BY STUDENT>	**Student ID**	<TO BE FILLED BY STUDENT>
Date	<TO BE FILLED BY STUDENT>	**Student Name**	<TO BE FILLED BY STUDENT>

Experiment #	<TO BE FILLED BY STUDENT>	Student ID	<TO BE FILLED BY STUDENT>
Date	<TO BE FILLED BY STUDENT>	Student Name	<TO BE FILLED BY STUDENT>

Implementation of DHCP in Cisco packet tracer

Dynamic Host Configuration Protocol (DHCP) is a network protocol that automatically assigns IP addresses and other network configuration information to devices on a network.
Here are the steps involved in the implementation of DHCP in Cisco Packet Tracer:

1. Build the Network Topology:

- Launch Cisco Packet Tracer and create a network topology by adding devices such as routers, switches, and PCs to the workspace.
-

2. Configure Router Interfaces:

- Access the command-line interface (CLI) of the router where you want to configure DHCP.
- Enter global configuration mode using the enable command and then configure terminal.
- Navigate to the interface configuration mode (e.g., interface FastEthernet0/0) for the interface connected to the local network.
- Use the ip address command to assign an IP address and subnet mask to the interface.

3. Enable DHCP on the Router:

- Enter the DHCP configuration mode by using the ip dhcp pool command, followed by a pool name.
- Define the network address and subnet mask for the DHCP pool.
- Specify the range of IP addresses to be dynamically assigned to devices in the network using the network and default-router commands.

Example:

```
Router(config)# ip dhcp pool MY_POOL
Router(dhcp-config)# network 192.168.1.0 255.255.255.0
Router(dhcp-config)# default-router 192.168.1.1
Router(dhcp-config)# exit
```

4. Configure DNS Servers (Optional):

- Optionally, configure DNS servers to be assigned to DHCP clients using the dns-server command in DHCP pool configuration mode.

Example:

```
Router(dhcp-config)# dns-server 8.8.8.8
```

5. Enable DHCP on the Router Interface:

- Enter the interface configuration mode for the interface connected to the local network.
- Use the ip dhcp server command to enable DHCP on the interface.

Experiment #	<TO BE FILLED BY STUDENT>	Student ID	<TO BE FILLED BY STUDENT>
Date	<TO BE FILLED BY STUDENT>	Student Name	<TO BE FILLED BY STUDENT>

Example:
Router(config)# interface FastEthernet0/0
Router(config-if)# ip dhcp server MY_POOL
Router(config-if)# exit

6. Verify DHCP Configuration:

- Use the show ip dhcp binding command on the router to view a list of devices that have obtained IP addresses from the DHCP server.

Example:
Router# show ip dhcp binding

7. Test DHCP Configuration:

- Power on the client devices (PCs) in the network and set their network interfaces to obtain IP addresses automatically (DHCP).

8. Observe DHCP Requests and Responses:

- Use Packet Tracer's simulation mode to observe DHCP request and response messages between clients and the DHCP server.

9. Document Your Configuration:

- Create documentation that includes the DHCP configuration settings, such as the pool name, network address, subnet mask, default gateway, and DNS server information.

10. Save Configuration: - Save your router's configuration to ensure that your DHCP settings are preserved even after a reboot. Use the write memory or copy running-config startup-config command.

By following these steps, you can successfully implement DHCP in Cisco Packet Tracer, providing dynamic IP address assignments to devices in your simulated network.

Device Configuration details

Device Name(Label)	Interface	IP Address	Subnet Mask	Default Gateway address

Experiment #	<TO BE FILLED BY STUDENT>	**Student ID**	<TO BE FILLED BY STUDENT>
Date	<TO BE FILLED BY STUDENT>	**Student Name**	<TO BE FILLED BY STUDENT>

Configuration of Router

Experiment #	<TO BE FILLED BY STUDENT>	**Student ID**	<TO BE FILLED BY STUDENT>
Date	<TO BE FILLED BY STUDENT>	**Student Name**	<TO BE FILLED BY STUDENT>

VIVA-VOCE Questions (In-Lab):

1. What is SMTP and FTP? Give the primary purpose?
2. How does SMTP facilitate the sending and receiving of emails?
3. What is DNS, and why is it essential for internet communication?
4. How does DHCP resolve assigning IP addresses by dynamically?
5. What is HTTP, and what role does it play in web communication?

Experiment #	<TO BE FILLED BY STUDENT>	**Student ID**	<TO BE FILLED BY STUDENT>
Date	<TO BE FILLED BY STUDENT>	**Student Name**	<TO BE FILLED BY STUDENT>

Post Lab Task:

1. Describe the network topology you used for configuring SMTP, FTP, DNS, and HTTP services in Cisco Packet Tracer. What devices were involved, and how were they interconnected?

2. Explain the purpose and significance of SMTP in the context of email communication.

3. Discuss the significance of HTTP in web communication.

4. Discuss the significance of DHCP.

Experiment #	<TO BE FILLED BY STUDENT>	**Student ID**	<TO BE FILLED BY STUDENT>
Date	<TO BE FILLED BY STUDENT>	**Student Name**	<TO BE FILLED BY STUDENT>

Evaluator Remark (if Any):	**Marks Secured: _____out of 50**
	Signature of the Evaluator with Date

Experiment #	<TO BE FILLED BY STUDENT>	**Student ID**	<TO BE FILLED BY STUDENT>
Date	<TO BE FILLED BY STUDENT>	**Student Name**	<TO BE FILLED BY STUDENT>

Lab 12: Write a python program for Transposition Technique using Rail fence Technique and columnar Technique.

Date of the Session:_____/___/____ **Session Time:____to_____**

Learning outcome:

- Understand the principles and operations of both the Rail Fence and Columnar ciphers. Be familiar with their historical context and modern applications.
- Learn how to encrypt and decrypt messages using both the Rail Fence and Columnar ciphers. Understand the algorithms and processes involved
- Understand how the Rail Fence cipher works, where letters are written diagonally in a "zigzag" pattern..
- Understand where they are suitable and how they've been historically employed.

Pre-Lab Task:

1. Learn how to set up the number of rails and perform encryption and decryption operations. Practice these methods on sample messages.

2. Explore potential cryptanalysis methods for breaking the Rail Fence cipher and learn how to recover plaintext from an encrypted message.

3. Practice selecting appropriate keys or keywords for different messages and varying the key lengths for encryption.

4. Identify specific use cases and scenarios where the Columnar cipher may be useful, such as secure messaging

In Lab Task: Write a python program for Transposition Technique using Rail fence Technique and columnar Technique

Rail fence Technique

Implementing the Rail Fence transposition technique is relatively straightforward. It involves arranging the characters of a plaintext message in a zigzag pattern along a set number of "rails" or rows, then reading the characters in a specific order to create the ciphertext.

Here are the steps for implementing the Rail Fence technique:

Step 1: Choose the Number of Rails (Rows)

- Decide on the number of rails or rows you want to use for the Rail Fence. This determines the depth of the zigzag pattern.

Step 2: Prepare the Plaintext

- Take your plaintext message, remove spaces, and special characters if necessary, and ensure it is in a suitable format.

Step 3: Create the Zigzag Pattern

- Start at the top-left corner of your rail (row 1).
- Write the first character of your plaintext in this position.
- Continue writing characters diagonally, moving down one rail after each character, until you reach the bottom rail.
- When you reach the bottom rail, start moving diagonally up toward the top rail, following the zigzag pattern. Repeat this process until you've used all characters from your plaintext.

Step 4: Reading the Ciphertext

- Read the characters along each rail from left to right, starting with the top rail and moving downward.
- Concatenate the characters from each rail to form the ciphertext.

Step 5: Encryption Example

- Let's say you have a plaintext message: "HELLO WORLD" and you want to use 3 rails.

Create the zigzag pattern as follows:

H……..…..…O……..…L

E……..L……..….W……..R……D

L….....O

Read the characters from left to right along each rail: "HORDELLWOL."

The ciphertext is "HORDELLWOL."

Step 6: Decryption (Optional)

- To decrypt a Rail Fence-encrypted message, you need to know the number of rails used.
- Create an empty zigzag pattern with the same number of rails.
- Fill in the ciphertext characters in the pattern following the same zigzag pattern.
- Read the characters in the pattern from left to right to reveal the original plaintext.

Step 7: Key Management

- For decryption, it's crucial to know the number of rails used. This information serves as the decryption key.

By following these steps, you can successfully implement the Rail Fence transposition technique to encrypt and decrypt messages. Keep in mind that the security of the Rail Fence cipher is relatively low, and it is primarily used for educational or illustrative purposes.

Experiment #	<TO BE FILLED BY STUDENT>	**Student ID**	<TO BE FILLED BY STUDENT>
Date	<TO BE FILLED BY STUDENT>	**Student Name**	<TO BE FILLED BY STUDENT>

Writing space for the Program: (For Student's use only)

Write a python program for Transposition Technique using Rail fence Technique

Experiment #	<TO BE FILLED BY STUDENT>	Student ID	<TO BE FILLED BY STUDENT>
Date	<TO BE FILLED BY STUDENT>	Student Name	<TO BE FILLED BY STUDENT>

Output

Columnar Transposition Technique

Implementing the Columnar Transposition Technique involves a series of steps to encrypt and decrypt messages. Below are the steps to implement the Columnar Transposition Technique:

Encryption using Columnar Transposition:

1. **Select a Keyword:** Choose a keyword or key phrase that will determine the order of columns for transposition. For example, let's use the keyword "CRYPTO" for this demonstration.
2. **Write the Message:** Write down your plaintext message in rows beneath the keyword, starting from left to right. The keyword dictates the order of the columns.
   Example:
   Keyword: CRYPTO
   Plaintext: THIS IS A SECRET MESSAGE
   Arranged in columns:
   CRYPTO
   THISIS
   ASECRET
   MESSAGE
3. **Order the Columns**: Rearrange the columns alphabetically based on the letters in your keyword. In this case, the keyword "CRYPTO" would be ordered as "COPRTY."

Example:
CRYPTO
THISIS
ASECRET
MESSAGE
Rearranged:
COPRTY
TSIHIS
AETSREC
GMEASSE

4. **Read the Ciphertext**: Read the message row by row, from left to right. This is your ciphertext.
   Example:
   Ciphertext: "CTT AIG EME HSAS RST SEO S"

Decryption using Columnar Transposition:

1. Select a Keyword: Choose the same keyword used for encryption, in this case, "CRYPTO."
2. Determine the Number of Columns: Count the number of columns, which is equal to the length of your keyword.
3. Calculate the Number of Rows: To find the number of rows, divide the length of the ciphertext by the number of columns. If there's a remainder, add one row.
   Example:
   - Ciphertext length: 23
   - Number of columns: 6 (based on the keyword)
   - Rows = 23 / 6 = 3 rows with a remainder of 5, so we add one more row for a total of 4 rows.
4. **Recreate the Grid**: Create a grid with the same number of columns as the keyword and the calculated number of rows. Fill in the grid with the ciphertext in a row-by-row manner, left to right.
   Example:
   Keyword: CRYPTO
   Ciphertext: CTT AIG EME HSAS RST SEO S
   Reconstructed grid:
   CTTAIG
   EMEHSA
   SRSTSE
   OS

5. Sort the Columns: Sort the columns based on the keyword (in alphabetical order). In this case, it would be sorted as "COPRTY."
   Example:
   Sorted grid:

COPRTY
TSIHIS
AETSREC
GMEASSE

6. Read the Plaintext: Read the message row by row, from left to right. This is your plaintext.
   Example:
   Plaintext: "THIS IS A SECRET MESSAGE"

By following these steps, you can encrypt and decrypt messages using the Columnar Transposition Technique.

Writing space for the Program: (For Student's use only)

Write a python program for Transposition Technique using columnar Technique

Experiment #	<TO BE FILLED BY STUDENT>	**Student ID**	<TO BE FILLED BY STUDENT>
Date	<TO BE FILLED BY STUDENT>	**Student Name**	<TO BE FILLED BY STUDENT>

Experiment #	<TO BE FILLED BY STUDENT>	**Student ID**	<TO BE FILLED BY STUDENT>
Date	<TO BE FILLED BY STUDENT>	**Student Name**	<TO BE FILLED BY STUDENT>

Output

VIVA-VOCE Questions (In-Lab):

1. Explain the basic concept of the Rail Fence cipher. How does it work?
2. What is the key factor in the Rail Fence cipher, and how does it determine the number of "rails"?
3. What is the key space in the Rail Fence cipher, and how does it impact the security of the cipher?
4. Explain the basic concept of the Columnar cipher. How does it differ from the Rail Fence cipher?
5. What is the role of the keyword or key phrase in the Columnar cipher? How is it used in encryption??

Experiment #	<TO BE FILLED BY STUDENT>	**Student ID**	<TO BE FILLED BY STUDENT>
Date	<TO BE FILLED BY STUDENT>	**Student Name**	<TO BE FILLED BY STUDENT>

Post Lab Task:

1. Were you able to decrypt the Rail Fence-encrypted message without knowing the number of rails used during encryption? If so, how did you achieve this?

2. Can you provide examples of real-world scenarios where the Rail Fence cipher might be used effectively for encryption?

3. Compare the security and operational characteristics of the Columnar cipher with the Rail Fence cipher.

4. How does the appearance of the encrypted text change when you use different keywords or key lengths in the Columnar cipher?

Experiment #	<TO BE FILLED BY STUDENT>	**Student ID**	<TO BE FILLED BY STUDENT>
Date	<TO BE FILLED BY STUDENT>	**Student Name**	<TO BE FILLED BY STUDENT>

Evaluator Remark (if Any):	**Marks Secured: _____out of 50**
	Signature of the Evaluator with Date

Course Title	**NETWORK PROTOCOLS & SECURITY**	**ACADEMIC YEAR: 2024-25**
Course Code(s)	**23EC2210R**	

Experiment #	<TO BE FILLED BY STUDENT>	**Student ID**	<TO BE FILLED BY STUDENT>
Date	<TO BE FILLED BY STUDENT>	**Student Name**	<TO BE FILLED BY STUDENT>

Lab 13: Write a python program to implement of RSA Algorithm

Date of the Session:_____/___/____ **Session Time:____to_____**

Learning outcome:

- Learners will gain a comprehensive understanding of public key cryptography and the principles behind it.
- To understand and implement the concept of RSA Algorithm.

Pre-Lab Task:

1. Mention the RSA algorithm in simple terms. What is its purpose and how does it work?

2. What are the key components of the RSA algorithm, and what roles do they play in the encryption and decryption processes?

3. Discuss the advantages and limitations of the RSA algorithm.

Experiment #	<TO BE FILLED BY STUDENT>	Student ID	<TO BE FILLED BY STUDENT>
Date	<TO BE FILLED BY STUDENT>	Student Name	<TO BE FILLED BY STUDENT>

In Lab Task: Write a python program to implement of RSA Algorithm

Implementing the RSA (Rivest-Shamir-Adleman) algorithm involves several steps for generating keys and performing encryption and decryption.

Here are the steps for implementing the RSA algorithm:

Key Generation:

Step 1: Select Two Large Prime Numbers (p and q):

Choose two distinct prime numbers, p and q. These should be large enough to provide security. The security of RSA relies on the difficulty of factoring the product of these two prime numbers (n = p * q).

Step 2: Calculate n and φ(n):

Calculate n = p * q, the modulus used for both the public and private keys.

Calculate φ(n) (Euler's totient function), which is the number of positive integers less than n that are coprime to n. φ(n) = (p - 1) * (q - 1).

Step 3: Select an Encryption Key (e):

Choose an encryption key (e) such that 1 < e < φ(n) and e is coprime to φ(n). Common choices include small prime numbers like 3 or 65537 (2^16 + 1). The value of e becomes part of the public key.

Step 4: Calculate the Decryption Key (d):

Calculate the modular multiplicative inverse of e modulo φ(n). In other words, find d such that (d * e) % φ(n) = 1. The value of d becomes part of the private key.

Encryption:

Step 5: Message Encoding:

Convert the plaintext message into an integer M. This can be done using various encoding schemes (e.g., ASCII, Unicode).

Step 6: Encryption:

Compute the ciphertext C by raising M to the power of e modulo n: C = (M^e) % n.

Decryption:

Step 7: Decryption:

Compute the plaintext message M by raising C to the power of d modulo n: M = (C^d) % n.

Step 8: Message Decoding:

Convert the integer M back to the original plaintext message using the same encoding scheme used for encryption.

Key Management:

Step 9: Key Storage and Protection:

Safeguard the private key, as it should be kept secret. The public key can be openly shared.

Cryptographic Strength and Security Considerations:

Step 10: Key Length Selection:

The security of RSA depends on the key length. Ensure that you use sufficiently long keys to resist attacks. For modern applications, key lengths of 2048 bits or higher are recommended.

Step 11: Periodic Key Renewal:

Consider periodically generating new key pairs and transitioning to them to enhance security.

Step 12: Protect Against Attacks:

Be aware of potential attacks on RSA, such as factoring attacks and timing attacks. Implement countermeasures and best practices to protect against these threats.

Step 13: Test and Validate:

Test the RSA implementation thoroughly to ensure that it functions correctly and securely.

Writing space for the Program: (For Student's use only)

Write a Python program to Implementation of RSA Algorithm

Experiment #	<TO BE FILLED BY STUDENT>	**Student ID**	<TO BE FILLED BY STUDENT>
Date	<TO BE FILLED BY STUDENT>	**Student Name**	<TO BE FILLED BY STUDENT>

Experiment #	<TO BE FILLED BY STUDENT>	**Student ID**	<TO BE FILLED BY STUDENT>
Date	<TO BE FILLED BY STUDENT>	**Student Name**	<TO BE FILLED BY STUDENT>

Output

VIVA-VOCE Questions (In-Lab):

1. What is the RSA algorithm, and what is its primary purpose in cryptography?
2. Who are the creators of the RSA algorithm, and when was it introduced?
3. Explain the basic principles behind the RSA algorithm's encryption and decryption processes.
4. What is the key size in RSA, and why is it important for security?
5. What are the advantages of using the RSA algorithm for secure data transmission and encryption?

Experiment #	<TO BE FILLED BY STUDENT>	**Student ID**	<TO BE FILLED BY STUDENT>
Date	<TO BE FILLED BY STUDENT>	**Student Name**	<TO BE FILLED BY STUDENT>

Experiment #	<TO BE FILLED BY STUDENT>	**Student ID**	<TO BE FILLED BY STUDENT>
Date	<TO BE FILLED BY STUDENT>	**Student Name**	<TO BE FILLED BY STUDENT>

Post Lab Task:

1. Explain the purpose and significance of the RSA algorithm in cryptography.

2. What advantages does it offer in terms of secure communication and data encryption?

3. Discuss the importance of prime number generation and selection in the RSA algorithm.

Evaluator Remark (if Any):	**Marks Secured: _____out of 50**
	Signature of the Evaluator with Date

Experiment #	<TO BE FILLED BY STUDENT>	**Student ID**	<TO BE FILLED BY STUDENT>
Date	<TO BE FILLED BY STUDENT>	**Student Name**	<TO BE FILLED BY STUDENT>

Lab 14: Write a python program to Implement S-DES algorithm

Date of the Session:_____/___/____ **Session Time:____to_____**

Learning outcome:

- Understand the fundamental concepts of encryption, including plaintext, cipher text, keys, and the goals of encryption (confidentiality and security).
- Learn the principles of block ciphers, where data is encrypted in fixed-size blocks.
- Gain a comprehensive understanding of the S-DES algorithm, including its structure, rounds, and key generation process.
- Understand the security strengths and weaknesses of the S-DES algorithm. Explore potential vulnerabilities and attacks.

Pre-Lab Task:

1. Give the purpose of the S-DES algorithm in the field of cryptography?

2. Discuss about the key length of the S-DES algorithm, and what implications does it have for security?

3. Describe the basic principles and techniques used in the S-DES algorithm for encryption and decryption.

Experiment #	<TO BE FILLED BY STUDENT>	Student ID	<TO BE FILLED BY STUDENT>
Date	<TO BE FILLED BY STUDENT>	Student Name	<TO BE FILLED BY STUDENT>

In Lab Task: Implementation of S-DES algorithm

The Simplified Data Encryption Standard (S-DES) algorithm is a simplified version of the Data Encryption Standard (DES) and is used for educational purposes. It provides a great way to understand the fundamentals of encryption.

Below are the steps to implement the S-DES algorithm:

Key Generation:

Initial Key (10 bits): Start with a 10-bit binary key (e.g., 1010000010). This key will be used to generate two 8-bit subkeys, K1 and K2.

Permutation 10 (P10): Perform an initial permutation of the key using the P10 permutation table. This shuffles the bits of the key.

Split into Two 5-bit Halves: Split the 10-bit result into two 5-bit halves.

Circular Left Shifts: Perform a circular left shift (LS-1) on both 5-bit halves. This means that the leftmost bit is moved to the rightmost position.

Permutation 8 (P8): Combine the two 5-bit halves and perform a permutation using the P8 table to generate the first subkey, K1.

Apply Another Circular Left Shift: Perform another circular left shift (LS-2) on the original two 5-bit halves.

Permutation 8 (P8): Combine the two 5-bit halves and perform a permutation using the P8 table again to generate the second subkey, K2.

Data Encryption:

Initial Permutation (IP): Perform the initial permutation (IP) on the 8-bit plaintext to rearrange its bits.

Split into Two 4-bit Halves: Split the 8-bit result into two 4-bit halves, referred to as L0 and R0.

Round 1 (Feistel Network):

Expansion (E/P): Expand the R0 half to 8 bits using the E/P table.

XOR with K1: XOR the result with the first subkey, K1.

Substitution Boxes (S-Boxes): Split the 8 bits into two 4-bit halves. Each 4-bit half goes through a specific S-box substitution.

Permutation 4 (P4): Combine the outputs of the S-boxes and permute the bits using the P4 table.

XOR with L0: XOR the result with the original L0 half.

Swap Halves: Swap the two halves, so L1 becomes R0, and R1 becomes L0.

Round 2 (Feistel Network):

Repeat the steps of Round 1, but use the second subkey, K2.

Inverse Initial Permutation (IP^-1): Perform the inverse of the initial permutation on the combined result of L2 and R2.

Data Decryption:

The decryption process follows the same steps as encryption, but the subkeys are used in reverse order (K2 is used first, then K1).

The final output is the original plaintext.

These steps outline the basic implementation of the S-DES algorithm for encrypting and decrypting data. It's a simplified version of the DES algorithm, offering insight into the principles of Feistel networks, permutations, and S-box substitutions..

Writing space for the Program: (For Student's use only)

Experiment #	<TO BE FILLED BY STUDENT>	**Student ID**	<TO BE FILLED BY STUDENT>
Date	<TO BE FILLED BY STUDENT>	**Student Name**	<TO BE FILLED BY STUDENT>

Experiment #	<TO BE FILLED BY STUDENT>	**Student ID**	<TO BE FILLED BY STUDENT>
Date	<TO BE FILLED BY STUDENT>	**Student Name**	<TO BE FILLED BY STUDENT>

VIVA-VOCE Questions (In-Lab):

1. What is the S-DES algorithm, and what is its primary purpose in cryptography?
2. Who developed the S-DES algorithm, and when was it introduced?
3. Explain the basic principles behind the S-DES algorithm's encryption and decryption processes.
4. What is the block size and key size used in S-DES, and why were these specific values chosen?
5. What is the role of the Initial Permutation (IP) and Final Permutation (FP) in S-DES?

Experiment #	<TO BE FILLED BY STUDENT>	**Student ID**	<TO BE FILLED BY STUDENT>
Date	<TO BE FILLED BY STUDENT>	**Student Name**	<TO BE FILLED BY STUDENT>

Post Lab Task:

1. Explain the purpose and significance of the S-DES algorithm in cryptography.

2. What advantages does S-DES algorithm offer in terms of data confidentiality and encryption?

3. Discuss the security considerations and vulnerabilities associated with the S-DES algorithm.

Evaluator Remark (if Any):	**Marks Secured: _____out of 50**
	Signature of the Evaluator with Date