



**S.I.E.S College of Arts, Science and Commerce,**  
**Sion(W), Mumbai – 400 022.**

**CERTIFICATE**

This is to certify that Mr. **Parth Dedhia** Roll No. **TCS2324010** has successfully completed the necessary course of experiments in the subject of **Information And Network security** during the academic year **2023–2024** complying with the requirements of **University of Mumbai**, for the course of **T.Y.BSc. Computer Science [Semester-V]**

Head of the Department  
(Computer Science)

**-Dr. Manoj Singh**

Prof. In-Charge

**Mr. Abuzar Ansari**

Date: 1<sup>th</sup> September 2023

College Seal

# INDEX

Practical No	Topics	Page no.	Date	Signature
1	Write a program to implement substitution Caesar Cipher		26/07/23	
2	Write a program to implement substitution Monoalphabetic Cipher		26/07/23	
3	Write a program to implement Rail Fence Cipher		02/08/23	
4	Write a program to implement RSA algorithm to Perform Encryption & Decryption of input string		09/08/23	
5	Write A program to implement Diffiehellman key Agreement algorithm to generate symmetric key		16/08/23	
6	Write a program to		23/08/23	

	implement MD5 algorithm compute the message digest.			
7	Write a program to calculate HMACSHA256 Signature		23/08/23	
8	Configure windows Firewall to block: 1. Website 2. Port		30/08/23	
9	Configure the windows vpn to bypass the Firewall		30/08/23	

## **Practical No. 1**

***Aim:*** Write A program to implement Substitution Caesar Cipher

***Code:***

```
import java.util.*;
class CaesarCipher
{
public static void main(String args[])
{
Scanner sc=new Scanner(System.in);
int shift,i,n;
String str;
String str1="";
String str2="";
System.out.println("Enter the plaintext");
str=sc.nextLine();
```

```

str=str.toLowerCase();
n=str.length();
char ch1[]=str.toCharArray();
char ch3,ch4;
System.out.println("Enter the value by which each letter of the
string is to be shifted");
shift=sc.nextInt();
System.out.println();
System.out.println("Encrypted text is");
for(i=0;i<n;i++)
{
if(Character.isLetter(ch1[i]))
{
ch3=(char)((((int)ch1[i]+shift-97)%26+97);
//System.out.println(ch1[i]+" = "+ch3);
str1=str1+ch3;
}
else if(ch1[i]==' ')
{

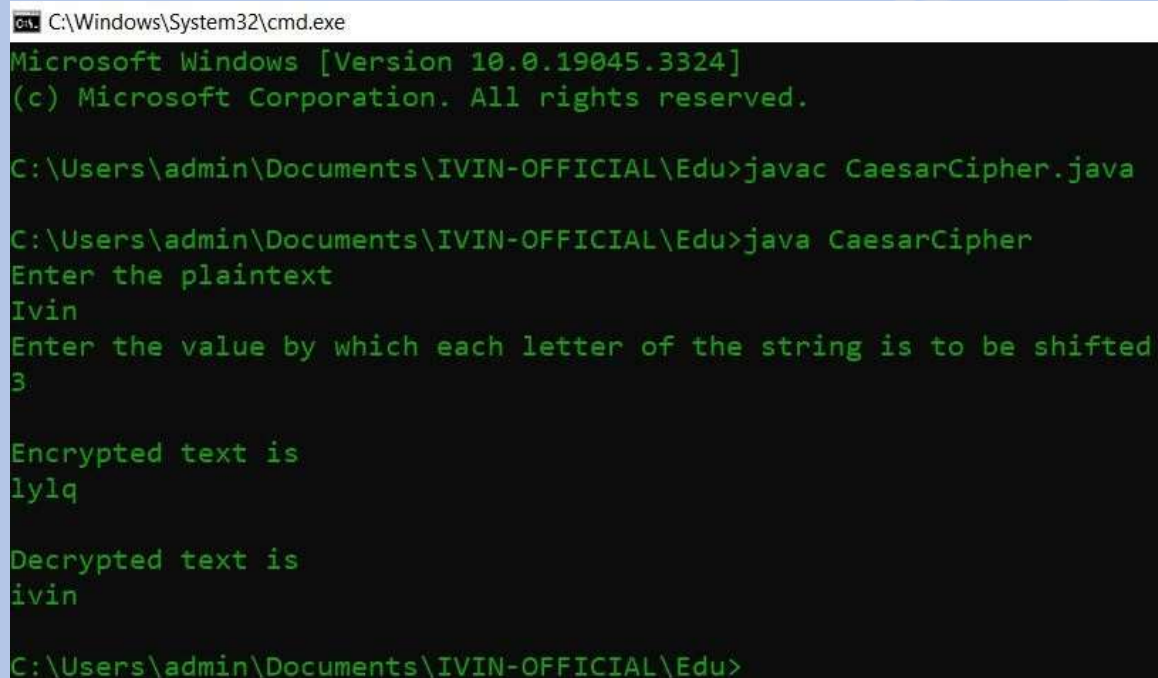
str1=str1+ch1[i];
}
}
System.out.println(str1);
System.out.println();
System.out.println("Decrypted text is");
char ch2[]=str1.toCharArray();
for(i=0;i<str1.length();i++)
{
if(Character.isLetter(ch2[i]))
{
if((((int)ch2[i]-shift)<97)
{
ch4=(char)((((int)ch2[i]-shift-97+26)%26+97);
}
else
{

ch4=(char)((((int)ch2[i]-shift-97)%26+97);

```

```
}  
str2=str2+ch4;  
}  
else if(ch2[i]==' ')  
{  
str2=str2+ch2[i];  
}  
}  
System.out.println(str2);  
}  
}
```

### ***Output:***



```
C:\Windows\System32\cmd.exe  
Microsoft Windows [Version 10.0.19045.3324]  
(c) Microsoft Corporation. All rights reserved.  
  
C:\Users\admin\Documents\IVIN-OFFICIAL\Edu>javac CaesarCipher.java  
  
C:\Users\admin\Documents\IVIN-OFFICIAL\Edu>java CaesarCipher  
Enter the plaintext  
Ivin  
Enter the value by which each letter of the string is to be shifted  
3  
  
Encrypted text is  
lylq  
  
Decrypted text is  
ivin  
  
C:\Users\admin\Documents\IVIN-OFFICIAL\Edu>
```

---

## **Practical No. 2**

***Aim:*** Write A program to implement Substitution Monoalphabetic Cipher

***Code:***

**GUI.java**

```
import javax.swing.*;
import java.awt.*;
import java.awt.event.*;

public class GUI {
    private static void createAndShowGUI() {
        //Create and set up the window.
        JFrame frame = new JFrame("HelloWorldSwing");

        frame.setDefaultCloseOperation(JFrame.EXIT_ON_CLOSE);

        JPanel body = new JPanel();
        final JTextField label = new
            JTextField("                ");
        body.add(label);
        final JTextField key = new JTextField("1");
        body.add(key);
        final JTextField result = new
            JTextField("                ");
        JButton activationButton = new JButton("Encrypt");
        activationButton.addActionListener(new
        ActionListener()
        {
            @Override
```

```

        public void actionPerformed(ActionEvent ae)
        {
            String plainText = label.getText();
            String keyval = key.getText();

            result.setText(MonoalphabeticCipher.caesarCipher(plainText, Integer.parseInt(keyval)));
        }
    });
    body.add(activationButton);
    body.add(result);
    frame.add(body);
    //Display the window.
    frame.pack();
    frame.setVisible(true);
}
public static void main(String[] args) {
    javax.swing.SwingUtilities.invokeLater(new
Runnable() {
        public void run() {
            createAndShowGUI();
        }
    });
}
}

```

### **Monoalphabetic.java**

```

public class MonoalphabeticCipher {
    static final String alphabet =
"abcdefghijklmnopqrstuvwxyz";
    public static char shift(char ch, int amount) {
        return alphabet.charAt((alphabet.indexOf(ch) +
amount) %
alphabet.length());
    }
}

```

```

    }
    public static String caesarCipher(String text, int
amount) {
        String result = "";
        for (char ch : text.toCharArray()) {
            if (alphabet.indexOf(ch) >= 0) {
                result += shift(ch, amount);
            }
        }
        return result;
    }
    public static void main(String[] args) {
        assert shift('a', 1) == 'b';
        assert shift('z', 2) == 'b';
        assert caesarCipher("abc", 2).equals("cde");
    }
}

```

### ***Output:***




---

## **Practical No. 3**

***Aim:*** Write A program to implement Rail fence Cipher

***Code:***



```

import java.util.*;
public class RailFenceCipher {

    int depth;
    String Encryption(String plainText,int depth)throws Exception
    {
        int r=depth,len=plainText.length();
        int c=len/depth;
        char mat[][]=new char[r][c];
        int k=0;

        String cipherText="";

        for(int i=0;i< c;i++)
        {
            for(int j=0;j< r;j++)
            {
                if(k!=len)
                    mat[j][i]=plainText.charAt(k++);
                else
                    mat[j][i]='X';
            }
        }
        for(int i=0;i< r;i++)
        {
            for(int j=0;j< c;j++)
            {
                cipherText+=mat[i][j];
            }
        }
        return cipherText;
    }
    String Decryption(String cipherText,int depth)throws
Exception
    {
        int r=depth,len=cipherText.length();
        int c=len/depth;
        char mat[][]=new char[r][c];
        int k=0;
    }
}

```

```

String plainText="";

for(int i=0;i< r;i++)
{
    for(int j=0;j< c;j++)
    {
        mat[i][j]=cipherText.charAt(k++);
    }
}
for(int i=0;i< c;i++)
{
    for(int j=0;j< r;j++)
    {
        plainText+=mat[j][i];
    }
}
return plainText;
}
}

class RailFence{
    public static void main(String args[])throws Exception
    {
        RailFenceCipher rf=new RailFenceCipher();
        Scanner scn=new Scanner(System.in);
        int depth;
        String plainText,cipherText,decryptedText;
        System.out.println("Enter plain text:");
        plainText=scn.nextLine();
        System.out.println("Enter depth for Encryption:");
        depth=scn.nextInt();
        cipherText=rf.Encryption(plainText,depth);
        System.out.println("Encrypted text is:\n"+cipherText);
        decryptedText=rf.Decryption(cipherText, depth);
        System.out.println("Decrypted text is:\n"+decryptedText);
    }
}

```

***Output:***

```

C:\Users\admin\Documents\IVIN-OFFICIAL\Edu>java RailFence
Enter plain text:
I am Ivin Santhosh
Enter depth for Encryption:
3
Encrypted text is:
Imv no iStsaInahh
Decrypted text is:
I am Ivin Santhosh

C:\Users\admin\Documents\IVIN-OFFICIAL\Edu>

```

---

## Practical No. 4

***Aim:*** Write a Program to Implement RSA algorithm to Perform Encryption & Decryption of input string

***Code:***

```

import java.math.BigInteger;
import java.util.Random;
import java.io.*;
public class RSA {

    private BigInteger p;
    private BigInteger q;
    private BigInteger N;
    private BigInteger phi;
    private BigInteger e;
    private BigInteger d;
    private int bitlength = 1024;
    private int blocksize = 256;
    //blocksize in byte
    private Random r;
    public RSA() {
        r = new Random();
        System.out.println("r");
        System.out.println(r);
    }
}

```

```

    p = BigInteger.probablePrime(bitlength, r);
    System.out.println("p");
    System.out.println(p);
    q = BigInteger.probablePrime(bitlength, r);
    System.out.println("q");
    System.out.println(q);
    N = p.multiply(q);
    System.out.println("N");
    System.out.println(N);
    phi =
p.subtract(BigInteger.ONE).multiply(q.subtract(BigInteger.ONE));
    System.out.println("phi");
    System.out.println(phi);
    e = BigInteger.probablePrime(bitlength/2, r);
    System.out.println("e");
    System.out.println(e);
    while (phi.gcd(e).compareTo(BigInteger.ONE) > 0 &&
e.compareTo(phi) < 0 ) {
        e.add(BigInteger.ONE);
    }
    d = e.modInverse(phi);
    System.out.println("d");
    System.out.println(d);
}
public RSA(BigInteger e, BigInteger d, BigInteger N) {
    this.e = e;
    this.d = d;
    this.N = N;
}
public static void main (String[] args) throws IOException {
    RSA rsa = new RSA();
    DataInputStream in=new DataInputStream(System.in);
    String teststring ;
    System.out.println("Enter the plain text:");
    teststring=in.readLine();
    System.out.println("Encrypting String: " + teststring);
    System.out.println("String in Bytes: " +
    bytesToString(teststring.getBytes()));
    // encrypt

```

```

        byte[] encrypted = rsa.encrypt(teststring.getBytes());
        System.out.println("Encrypted String in Bytes: " +
bytesToString(encrypted));
        // decrypt
        byte[] decrypted = rsa.decrypt(encrypted);
        System.out.println("Decrypted String in Bytes: " +
bytesToString(decrypted));
        System.out.println("Decrypted String: " + new
String(decrypted));
    }
    private static String bytesToString(byte[] encrypted) {
        String test = "";
        for (byte b : encrypted) {
            test += Byte.toString(b);
        }
        return test;
    }
    //Encrypt message
    public byte[] encrypt(byte[] message) {
        return (new BigInteger(message)).modPow(e,N).toByteArray();
    }
    // Decrypt message
    public byte[] decrypt(byte[] message) {
        return (new BigInteger(message)).modPow(d,N).toByteArray();
    }
}

```

***Output:***

```

TUN1
z
java.util.Random@6d06d69c
P
17550717494815924558270345139586729806599713073112513082498317171437393903607042597745549314063435029588973080311768747842034223863
q
1682728210853983949175903203189364129667739555689370095284942874857347666471128918701563627000527157713293180550779682666888833146
R
3953308744398010416553846002127329612155824012116949834252953588930564535718995618113544255587479635965322102265469325372326813430
phi
2953308744398010416553846002127329612155824012116949834252953588930564535718995618113544255587479635965322102265469325372326813430
e
7822409136672396869523454217139242156772817111758940584621291931094466097750402585585549706530490409128998785492328375888547962326
d
1083315823062997704231439958897308511204598980431267059613163852576489056647304312222184962152432531767362042989656604775240431585
Enter the plain text:
I am Kartik Kunder
Encrypting String: I am Kartik Kunder
String in Bytes: 7332971093275971141161051073275117110100101114
Encrypted String in Bytes: 97-1092-128302073-5-7090556867104276479-1181848266670-9193114-59-704660114-38121-73-518253-6311113-751-
Decrypted String in Bytes: 7332971093275971141161051073275117110100101114
Decrypted String: I am Kartik Kunder
BUILD SUCCESSFUL (total time: 18 seconds)

```

## Practical No. 5

**Aim:** Write A program to implement Diffie\_hellman key Agreement algorithm to generate symmetric key

**Code:**

```
import java.util.*;
public class Diffie_hellman {
    public static void main(String args[])
    {
        Scanner sc=new Scanner(System.in);
        System.out.println("Enter modulo(p)");
        int p=sc.nextInt();
        System.out.println("Enter primitive root of "+p);
        int g=sc.nextInt();
        System.out.println("Choose 1st secret no(Alice)");
        int a=sc.nextInt();
        System.out.println("Choose 2nd secret no(BOB)");
        int b=sc.nextInt();
        int A = (int)Math.pow(g,a)%p;
        int B = (int)Math.pow(g,b)%p;
        int S_A = (int)Math.pow(B,a)%p;
        int S_B =(int)Math.pow(A,b)%p;
        if(S_A==S_B)
        {
            System.out.println("ALice and Bob can communicate with
each other!!!");
            System.out.println("They share a secret no = "+S_A);
        }
        else
        {
            System.out.println("ALice and Bob cannot communicate
with each other!!!");
        }
    }
}
```

## ***Output:***

```
C:\Windows\System32\cmd.exe

C:\Users\admin\Documents\IVIN-OFFICIAL\Edu>javac Diffie_hellman.java

C:\Users\admin\Documents\IVIN-OFFICIAL\Edu>java Diffie_hellman
Enter modulo(p)
7
Enter primitive root of 7
8
Choose 1st secret no(Alice)
7
Choose 2nd secret no(BOB)
2
Alice and Bob can communicate with each other!!!
They share a secret no = 1

C:\Users\admin\Documents\IVIN-OFFICIAL\Edu>
```

---



---

## **Practical No. 6**

***Aim:*** Write a program to implement MD5 algorithm compute the message digest

***Code:***

```
import java.math.BigInteger;
import java.security.MessageDigest;
import java.security.NoSuchAlgorithmException;
public class MD5Hash {
    public static void main(String[] args) {
        System.out.println("For null " + generateHash(""));
        System.out.println("For simple text "+ generateHash("Kartik
Kunder"));
        System.out.println("For simple numbers " +
generateHash("67890"));
    }
    public static String generateHash(String input) {
        String md5 = null;
        if(null == input)
            return null;
        try {
            //Create MessageDigest object for MD5 or pass SHA-1
```

```
        MessageDigest digest =  
MessageDigest.getInstance("MD5");  
        //Update input string in message digest  
        digest.update(input.getBytes(), 0, input.length());  
        //Converts message digest value in base 16 (hex)  
        md5 = new BigInteger(1, digest.digest()).toString(16);  
    }  
    catch (NoSuchAlgorithmException e) {  
        e.printStackTrace();  
    }  
    return md5;  
}  
}
```

### ***Output:***

```
C:\Users\admin\Documents\IVIN-OFFICIAL\Edu>javac MD5Hash.java  
  
C:\Users\admin\Documents\IVIN-OFFICIAL\Edu>java MD5Hash  
For null d41d8cd98f00b204e9800998ecf8427e  
For simple text 8d7659aa75f51e7c9a44e5e990fe3534  
For simple numbers 1e01ba3e07ac48cbdab2d3284d1dd0fa  
  
C:\Users\admin\Documents\IVIN-OFFICIAL\Edu>
```

---

## **Practical No. 7**

***Aim:*** Write a program to calculate HMAC\_SHA256 Signature

***Code:***

```
import java.security.MessageDigest;
import java.security.NoSuchAlgorithmException;
public class PasswordSha256 {
    public static void main(String[] args) throws
    NoSuchAlgorithmException {
        String password = "123457";
        MessageDigest md =
        MessageDigest.getInstance("SHA-256");
        byte[] hashInBytes = md.digest(password.getBytes());
        // bytes to hex
        StringBuilder sb = new StringBuilder();
        for (byte b : hashInBytes) {
            sb.append(String.format("%02x", b));
        }
        System.out.println(sb.toString());
    }
}
```

***Output:***

```
C:\Users\admin\Documents\IVIN-OFFICIAL\Edu>javac PasswordSha256.java
C:\Users\admin\Documents\IVIN-OFFICIAL\Edu>java PasswordSha256
54b688a517f7654563a6c64d945a3670880a4c602ec67a065bbebbcd2b22edd5
C:\Users\admin\Documents\IVIN-OFFICIAL\Edu>
```

## Practical No. 8

**Aim:** Configure windows Firewall to block: 1. Website 2. Port

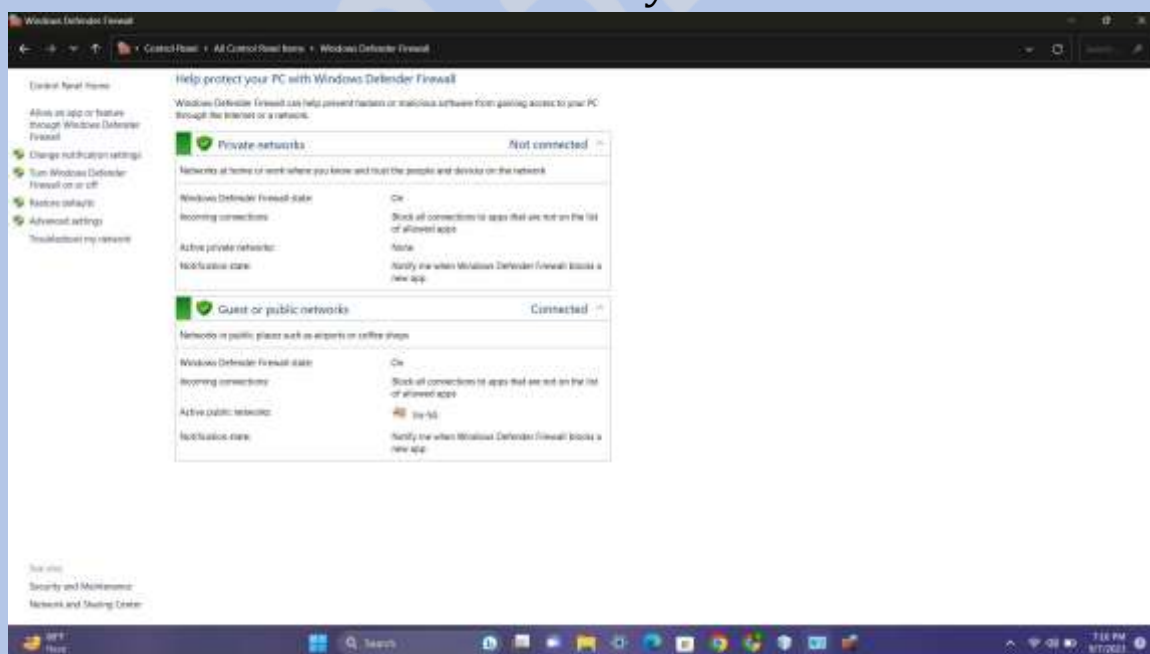
**Code:**

**Steps :**

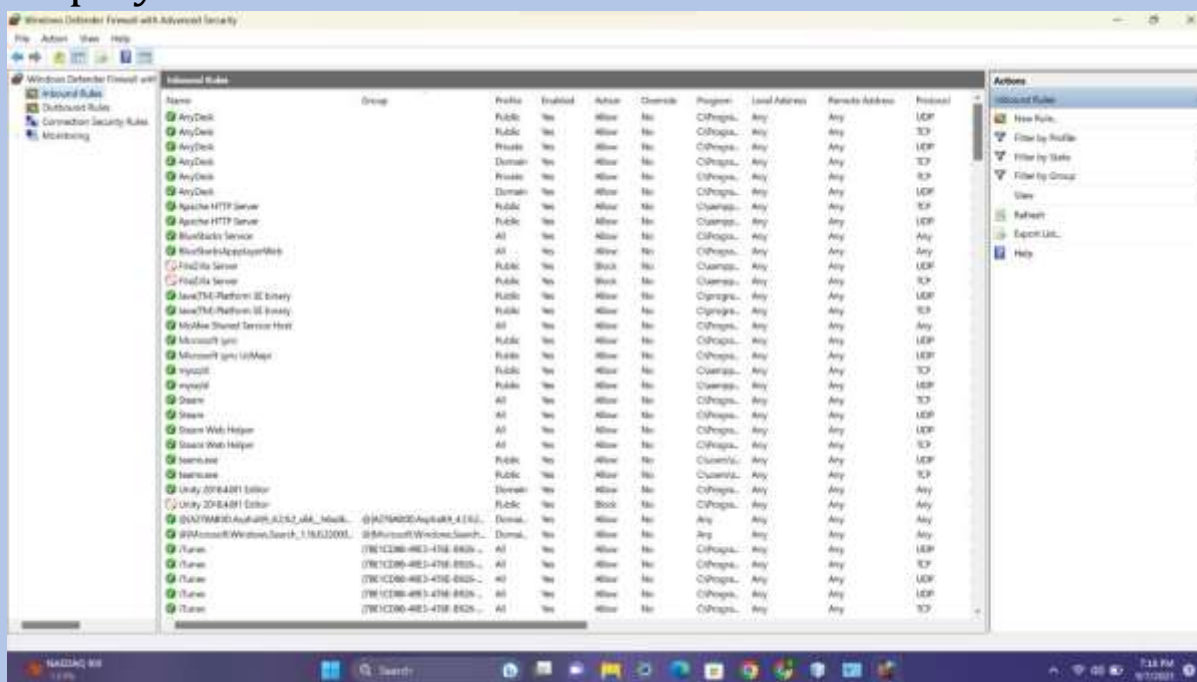
### **Block port in Windows Firewall**

Windows + R -> type Control

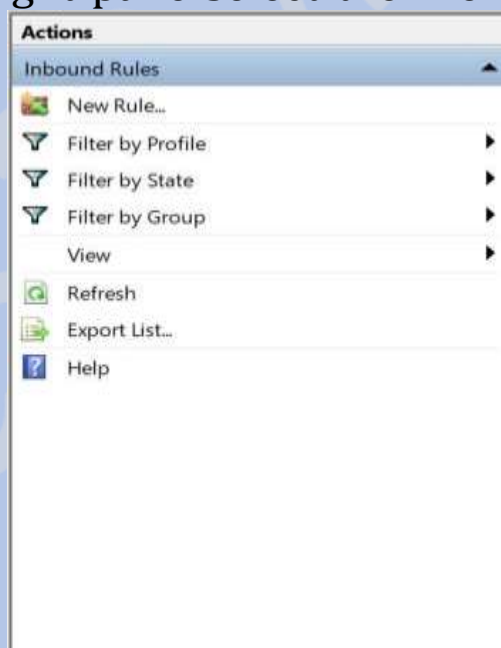
When in the 'Advanced Settings' of Windows 8 firewall, click the Advanced settings link in the left-hand pane of the main firewall dialog. This will bring up the Windows Firewall with Advanced Security window.



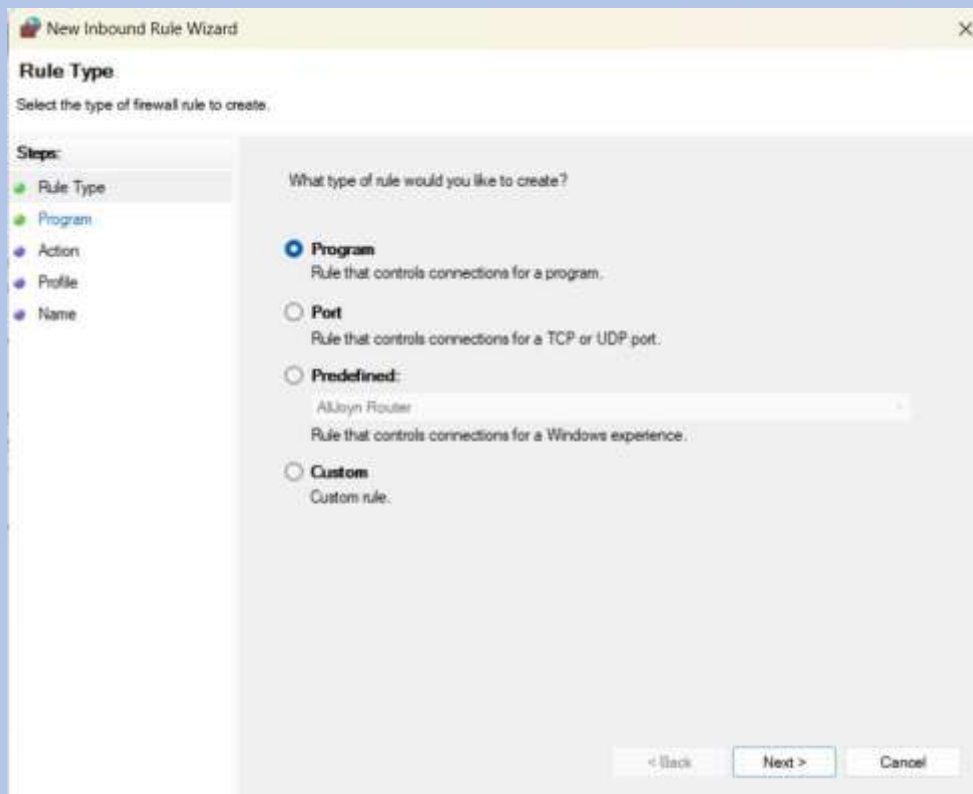
Now, if you see the firewall window shows a list of rules on the left side. From the list, select Inbound Rules to display the inbound rules section.



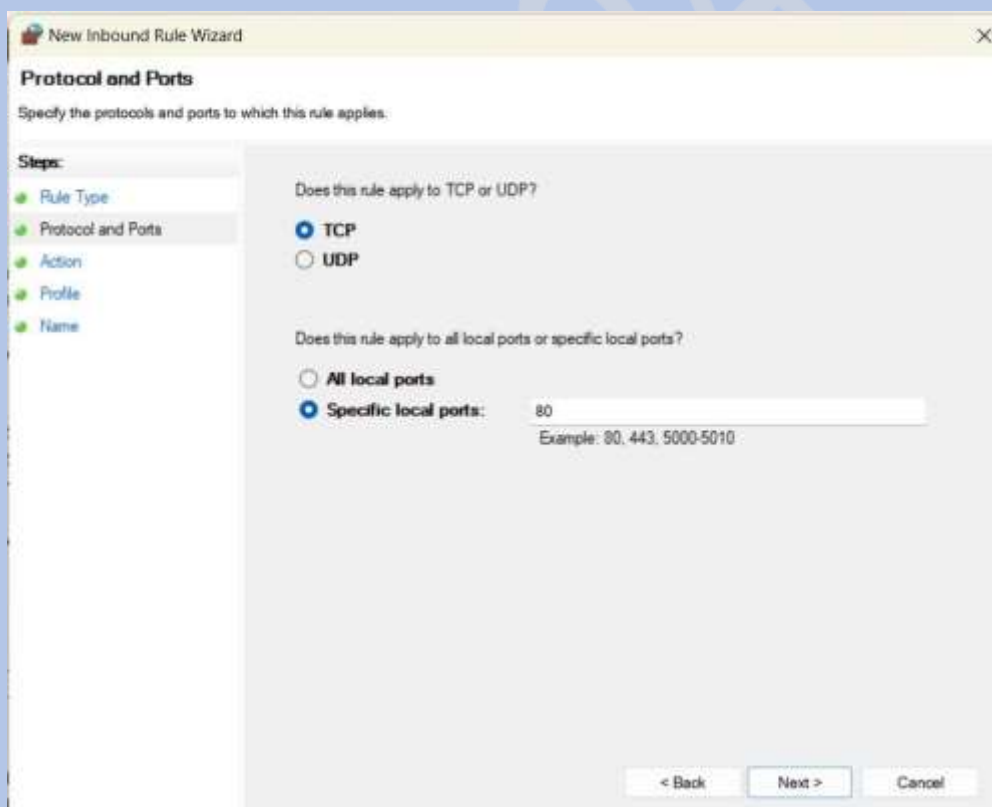
Then, from the right pane select the 'New Rule' option.



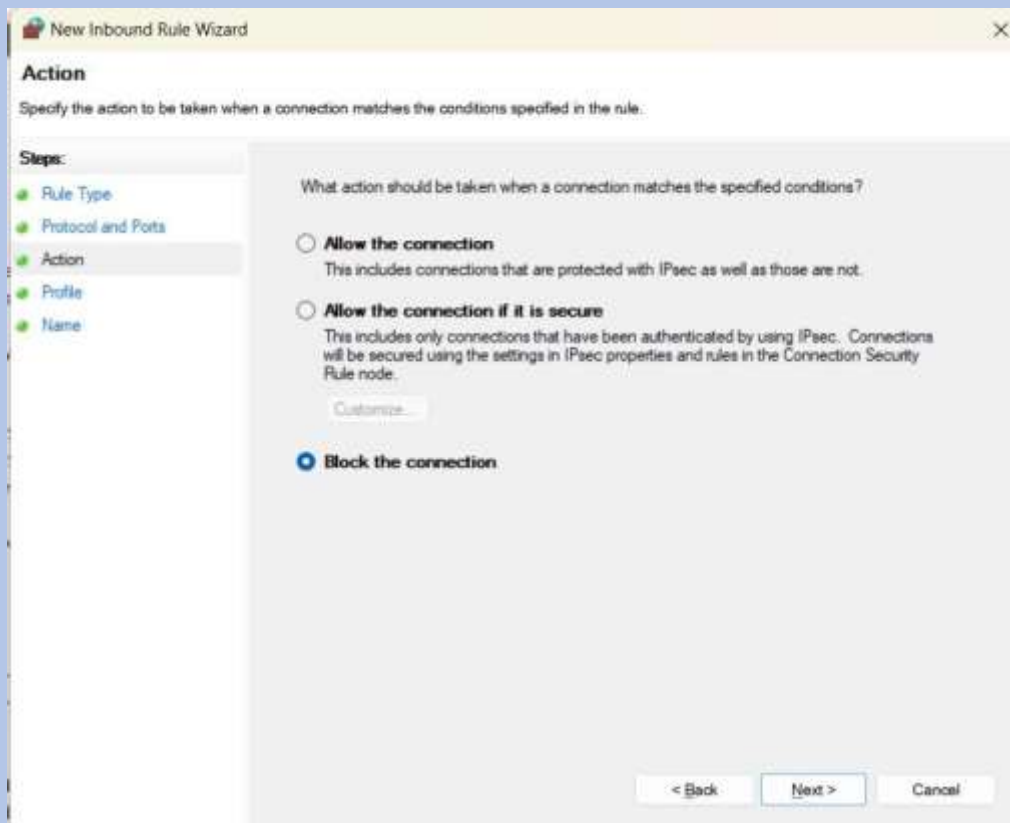
Doing so will open the 'New Inbound Rule Wizard' window. From it, select 'Port' as the new Rule Type and click Next. For safety purposes, I tried blocking TCP port. Click on Specific local ports. Then choose one port like 80 as shown in the screenshot below.



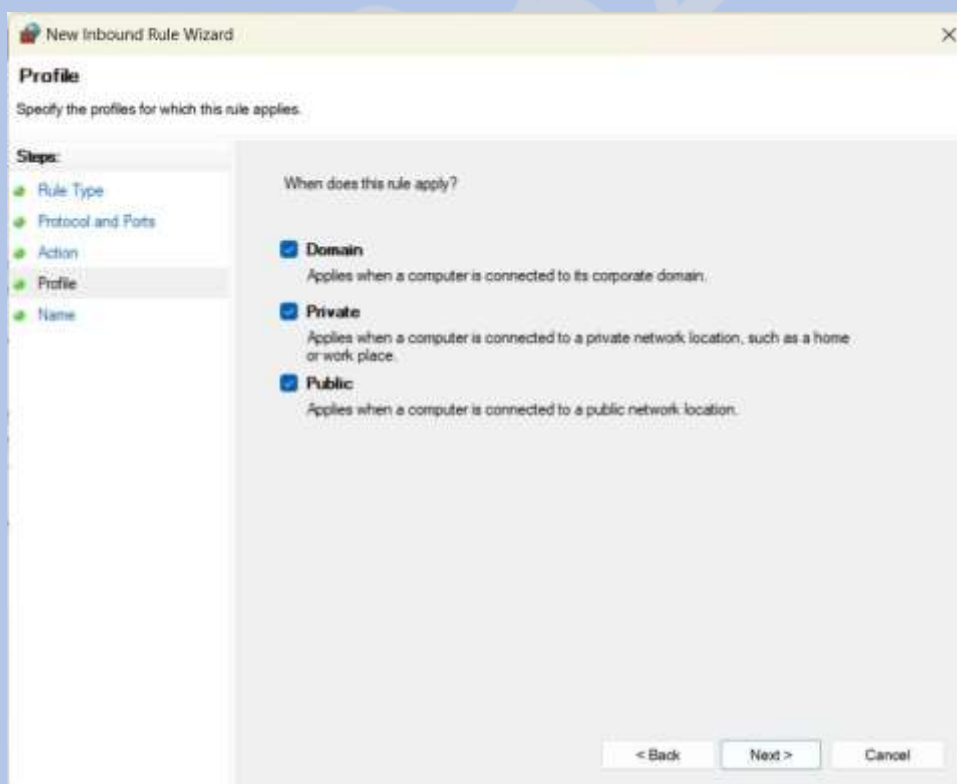
Click Next to continue.



Next, select 'Block the connection' as the Action and click Next.

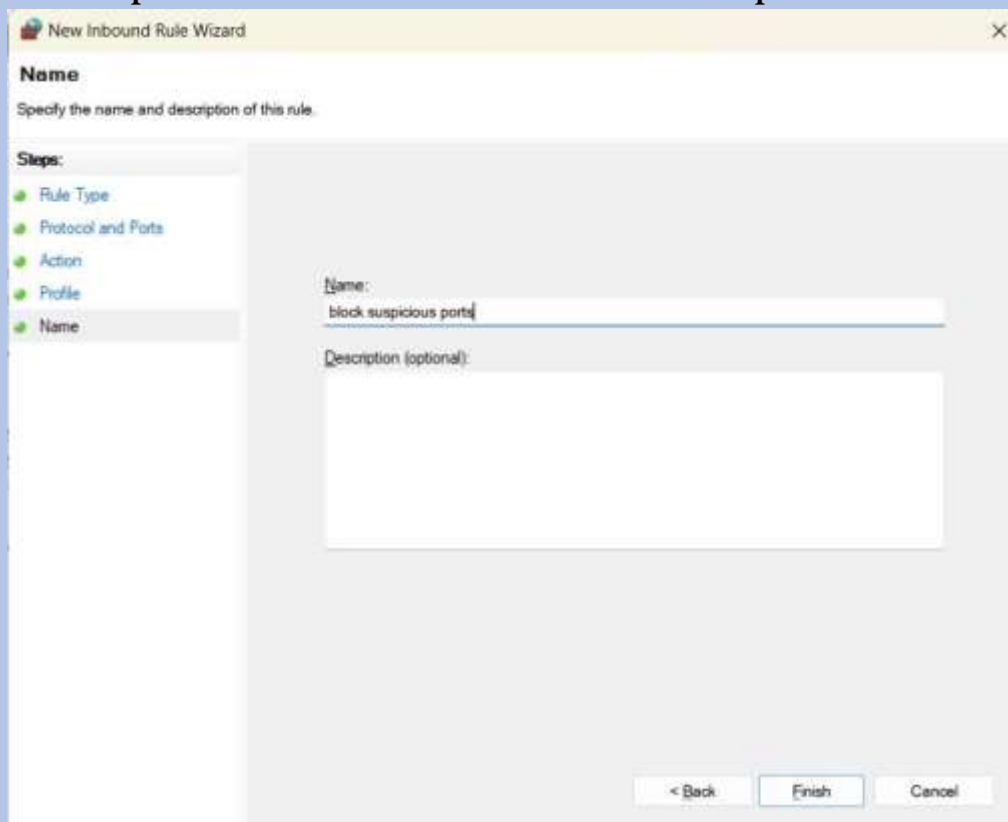


Later, select all the profiles available for different type of connections (Domain, Private and Public) and Click Next to continue.





Give a name of your choice to the new rule. I used 'block suspicious ports'. If you want, you can add the description to the new rule. This step is however optional.



Finally, click the Finish button to configure the settings.

## Open port in Windows Firewall

At times, you may feel the need of opening a port in the Windows firewall to let a specific IP communicate with your computer. For example, while playing games. The procedure to open a port remains more or less the same. All you need to do is follow the instructions in the **New Inbound Rule wizard**, specify the **Port** and select **Allow the connection**.

### 1. Open Start



2. Click the Windows logo in the bottom-left corner of the screen.

3. **Open Firewall.** Type in Windows Defender Firewall, then click Windows Defender Firewall at the top of the Start window. 4. Click Advanced settings. It's a link in the upper-left corner of the Windows Firewall window.

5. **Click Outbound Rules.** This tab is on the left side of the window.

6. **Click New Rule....** It's in the upper-right corner of the window. Doing so opens a new window in which you'll create your Firewall rule.

7. **Check the "Program" box.** You'll find this option at the top of the page.

8. **Click Next.** It's at the bottom of the window.

9. **Select a program.** Before you can block a program, you'll need to select the program to find its path:

- Check the "This program path" box and click Browse...
- Click This PC on the left side of the window.
- Scroll down and double-click your hard drive's name (e.g., OS (C:)).
- Double-click the Program Files folder.
- If the program you want to block is elsewhere, go to the program's folder instead.
- Find the folder for your program, then double-click the folder.
- Select the program file by clicking it once.

10. **Copy the program's path.** Click the address bar at the top of the window to select the path there, then press Ctrl+C to copy the path.

- This is necessary because Windows will restructure the path to the file once you open the file in Firewall, thus breaking your outbound rule. You can bypass

this problem by manually pasting in the path to the file.

11. **Click Open.** It's in the bottom-right corner of the window.

12. **Replace the path before the app's name with your copied one.** Highlight the path in the "This program path" text box up to the last backslash before the app's name, then press Ctrl+V to paste in your copied path.

- For example, if you wanted to block Chrome in the path "C:\Program 61 Files\Google\Application\chrome.exe", you would select all but the "\chrome.exe" section and replace it with your copied text.
- Leaving the app's name and extension at the end of the path is crucial, as failing to do so will leave you with a rule that doesn't block anything.

13. **Click Next three times.** This button is in the lower right side of the window on each page. Doing so takes you to the final page.

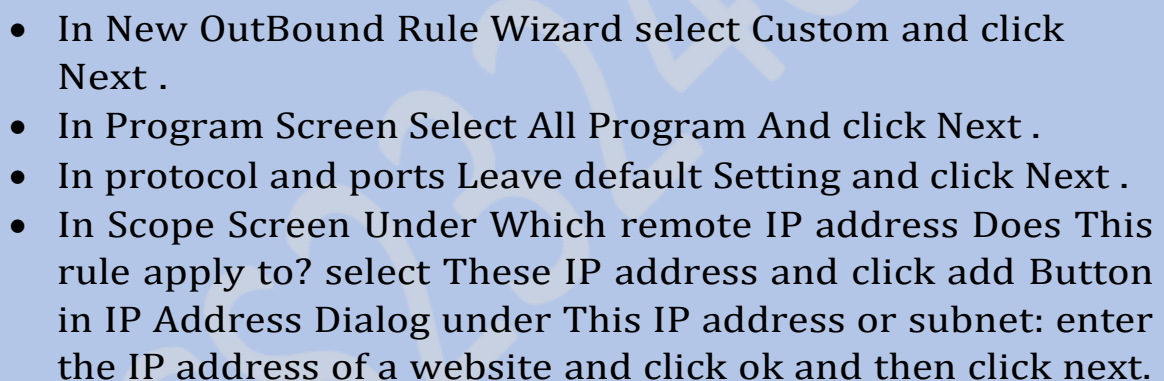
14. **Enter a name for your rule.** Type whatever you want to name your rule into the top textbox on the page.

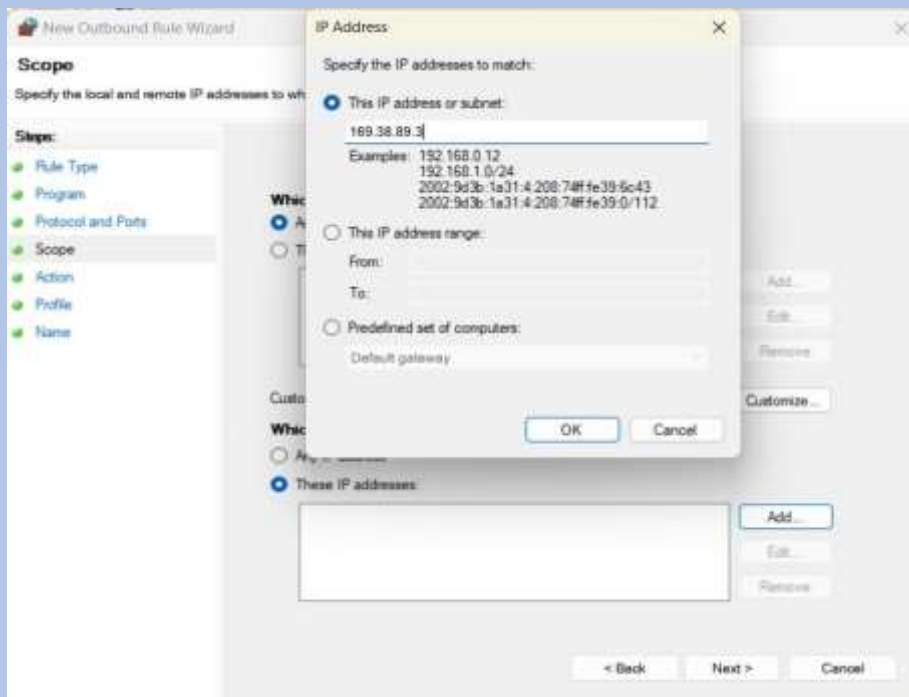
- For example, if you're blocking Google Chrome on your computer, you might name your rule "Chrome Block" here.

15. **Click Finish.** It's at the bottom of the window. Doing so saves and applies your rule; from now until you delete or disable the rule, your program will not be able to access the Internet

## Website

Go to **Control Panel > windows Firewall >** in the left side click **Advanced Setting.**





- In Action screen select Block the connection and click next .
- In Profile, screen leave all 3 check box selected and click next.
- In Name Screen choose a name for the rule and click finish[Text Wrapping Break]test whatyou do by entering URL in any browser that you want.

---

## **Practical No. 9**

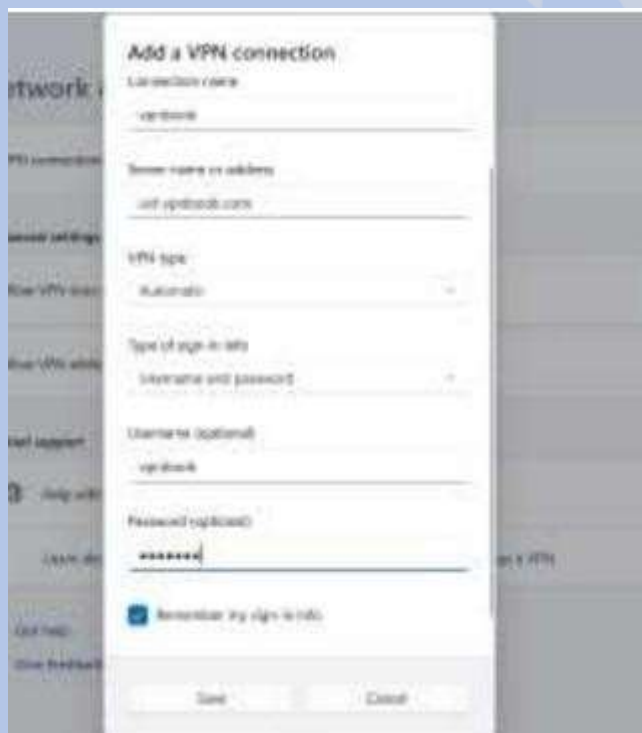
***Aim:*** Configure the windows vpn to bypass the Firewall

***Code:***

Free PPTP VPN Account (Easy to setup, no need to download any software, works with all Windows, Mobile and PS3 Devices)


- **Poland VPN Server:** PL226.vpnbook.com
- **Germany VPN Server:** de4.vpnbook.com
- Following servers are optimized for fast web surfing; no p2p downloading
- **US VPN Server:** us1.vpnbook.com
- **US VPN Server:** us2.vpnbook.com
- **France VPN Server:** fr1.vpnbook.com
- **France VPN Server:** fr8.vpnbook.com
- **Canada VPN Server:** ca222.vpnbook.com
- **Canada VPN Server:** ca198.vpnbook.com
- Username: vpnbook
- Password: 2k7k5vc
- **More servers coming...**

## ***Output:***





Network & internet > VPN

VPN connections Add VPN

 vpnbook Connected Disconnect

My IP Address is:

IPv4:  **198.7.62.204**

IPv6:  **Not detected**

My IP Information:

ISP:	LeaseWeb USA Inc.
Services:	<a href="#">Network Sharing</a> <a href="#">Details</a>
City:	Washington
Region:	District of Columbia
Country:	United States

◀ THE END ▶