Index

Practical 1

```
#Columnar Transposition
#Author Inbasagar
import math
def encrypt(message, key):
   columns = len(key)
   rows = math.ceil(len(message)/columns)
   cipherMatrix = []
   for i in range(rows):
      row = list(" " * columns)
      for j in range(columns):
         if(i * columns + j < len(message)):
            row[key[j]] = message [i * columns + j]
      cipherMatrix.append(row)
   cipher = ""
   for i in range(columns):
      for j in range(rows):
         cipher += cipherMatrix[j][i]
   return cipher

def decrypt(cipher, key):
   rows = len(cipher)//len(key)
   message = ""
   for i in range(rows):
      for j in range(len(key)):
         message += cipher[key[j] * rows + i]
   return message

message = input("Enter Message\n")
cols = int(input("Enter number of columns\n"))
key = []
for i in range(cols):
   key.append(int(input("key"+str(i)+": ")))
cipher = encrypt(message, key)
print("encrypt('" + message + "',", key, "): " + cipher)
print("decrypt('" + cipher +  "',", key, "): " + decrypt(cipher,key))
```

```
Enter message
Inbasagar
Enter number of columns
4
Enter key
3
2
1
0
Encrypted:aa bg na Isr
Decrypted:Inbasagar
BUILD SUCCESSFUL (total time: 9 seconds)
```

Practical 2

```
#Rail Fence Cipher
#Author Inbasagar
def encrypt(message, depth):
    array = []
    for i in range(depth):
        array.append("")
    mod = 2*(depth-1)
    for i in range(len(message)):
        array[min(i%mod, mod-i%mod)] += message[i]
    return "".join(array)

def decrypt(cipher, depth):
    array = []
    for i in range(depth):
        array.append([])
    mod = 2*(depth-1)
    index = 0
    for i in range(depth+1):
        for j in range(0,len(cipher)):
            if(min(j%mod, mod-j%mod) == i):
                array[i].append(cipher[index])
                index += 1
    message = ""
    for i in range(len(cipher)):
        message += array[min(i%mod,mod-i%mod)].pop(0)
    return message

message = input("Enter Message\n")
depth = int(input("Enter Depth\n"))
cipher = encrypt(message,depth)
print("encrypt('" + message + "',", depth, "): " + cipher)
print("decrypt('" + cipher + "',", depth, "): " + decrypt(cipher,depth))
```

```
Enter message
Inbasagar Nadar
Enter depth
3
Encrypted:Isrdnaaa aabgNr
Decrypted:Inbasagar Nadar
BUILD SUCCESSFUL (total time: 7 seconds)
```

Practical 3

```
Enter message
inbasagar
Enter key
2
Encrypted:kpdcucict
Decrypted:inbasagar
BUILD SUCCESSFUL (total time: 8 seconds)
```

Practical 4

```
Enter the value of Xa & Xb
2
3
Enter a Prime no. p
7
Enter Primitive Root a, with condition that a<p
6
Transmission successful
BUILD SUCCESSFUL (total time: 10 seconds)
```

Practical 5

```
hello : 5d41402abc4b2a76b9719d911017c592
sies  : bd7cf24638f2c8c785bd32190e7f2108
BUILD SUCCESSFUL (total time: 0 seconds)
```

Practical 6

```
Enter text of which SHA value has to be generated
Inbasagar
getSHA('Inbasagar'):2cbb702988ecbe05405a2a2aae9b682daba7487580eb57a4d5956db10dd047df
BUILD SUCCESSFUL (total time: 4 seconds)
```

Practical 7

```
Enter the plain text:
Inbasagar
String in Bytes: 7311098971159710397114
Encrypted String in Bytes: 232948-51-8310862-46-3721-575316-381-856179-25-55-41-1843-9610547-21-672534·
Decrypted String in Bytes: 7311098971159710397114
Decrypted String: Inbasagar
BUILD SUCCESSFUL (total time: 4 seconds)
```

Practical 8

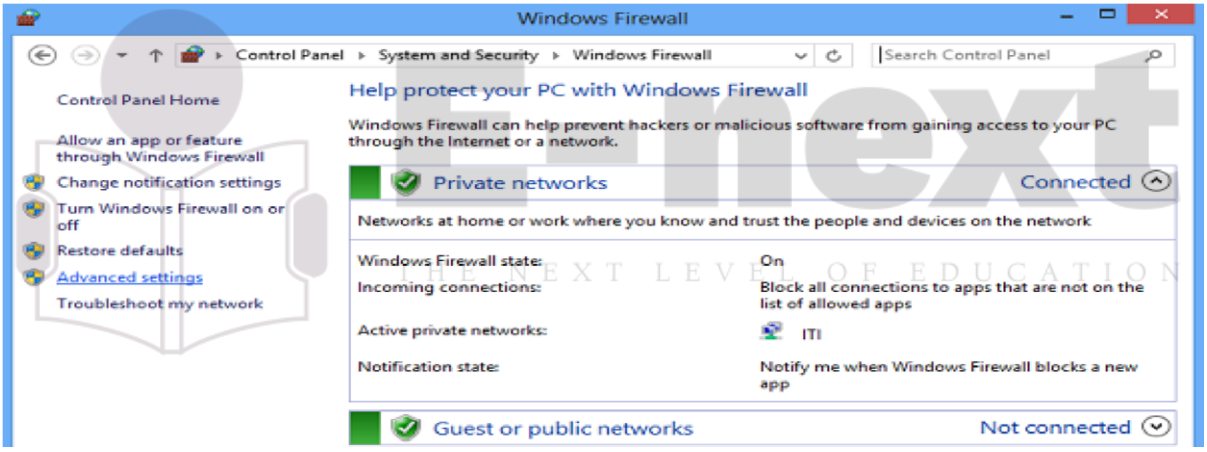
Aim:

To configure Windows Firewall to block:

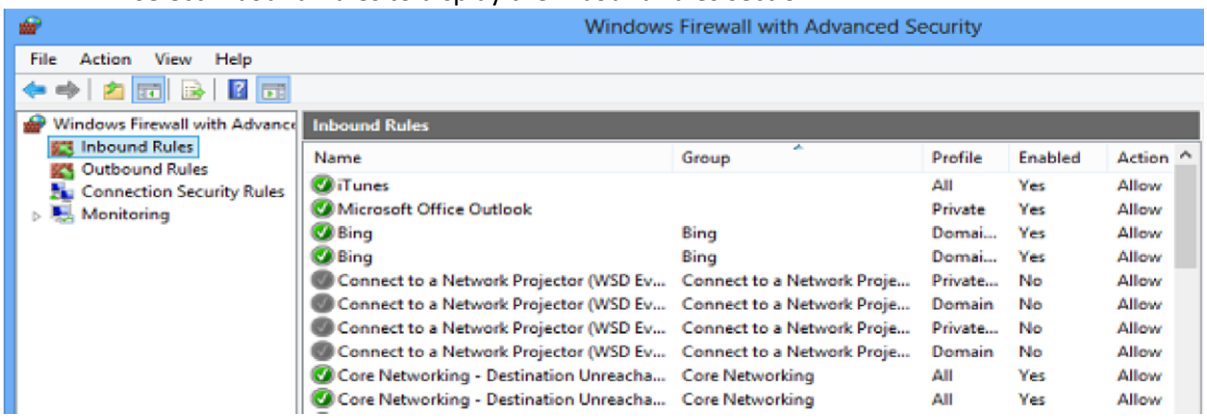
- A port,
- A Program &
- A website.

To block a port in Windows Firewall:

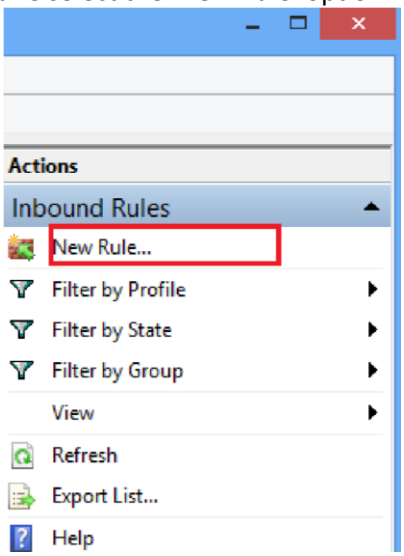
- Windows + R -> type Control
- When in the 'Advanced Settings' of Windows 8 firewall, click the Advanced settings link in the left-hand pane of the main firewall dialog. This will bring up the Windows Firewall with Advanced Security window.



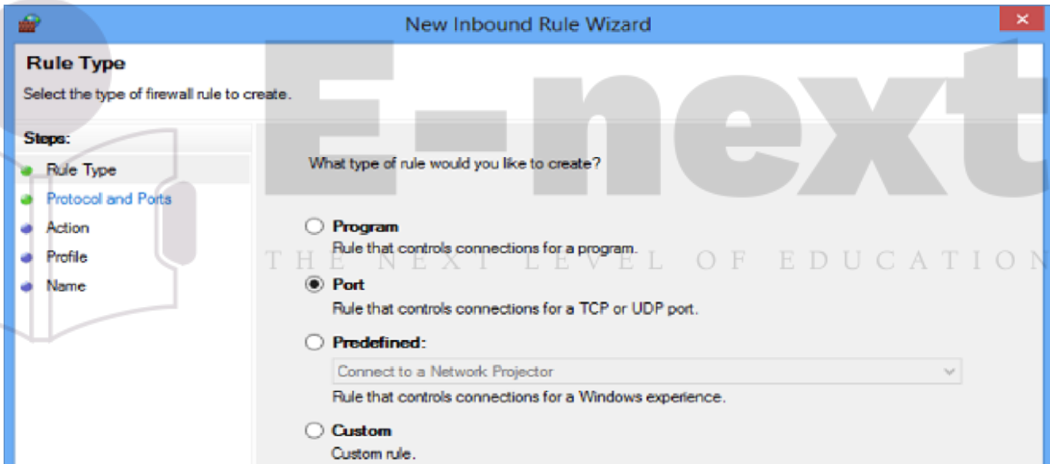
- Now, if you see the firewall window shows a list of rules on the left side. From the list, select Inbound Rules to display the inbound rules section.

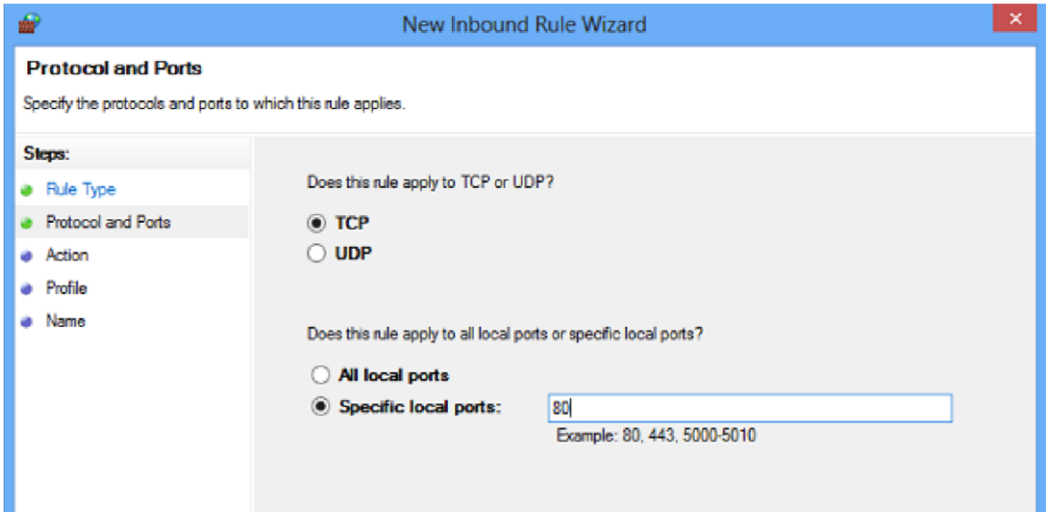


- Then, from the right pane select the ‘New Rule’ option.



- 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.





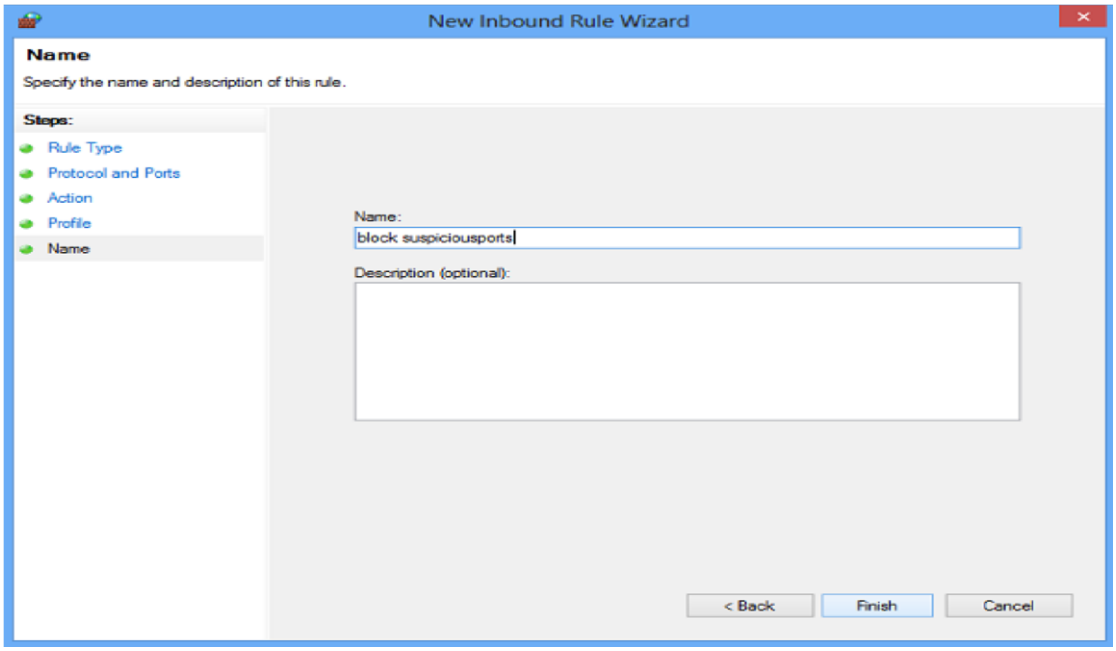
- Click Next to continue.

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

2.Open Firewall. Type in Windows Defender Firewall, then click **Windows Defender Firewall** at the top of the Start window.

3.Click **Advanced settings.** It's a link in the upper-left corner of the Windows Firewall window.

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

5.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.

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

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

8. Select a program. Before you can block a program, you'll need to select the program in order 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.

9.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.

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

11.Replace the path before the app's name with your copied one. Highlight the path in the "This program path" text box all the way 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 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.

12.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.

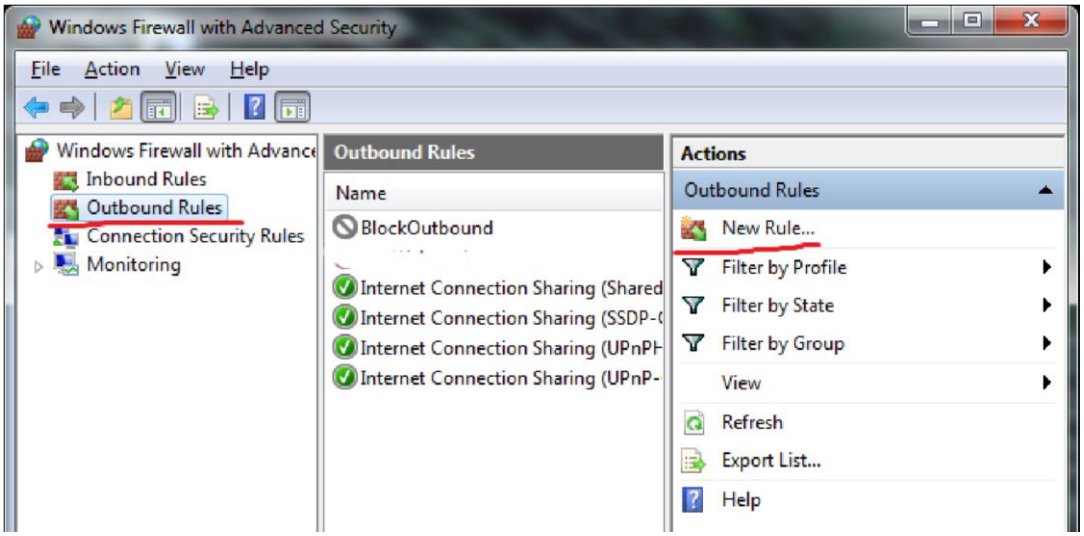
13.Enter a name for your rule. Type whatever you want to name your rule into the top text box on the page.

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

14.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

For a Website:-

1. Go to **Control Panel** > **Windows FireWall** > in the left side click **Advanced Setting**
2. go to **Outbound Rule** and in right side Click **New Rule**



3. in **New OutBound Rule Wizard** select **Custom** and click **Next**
4. in **Program** Screen Select **All Program** And click **Next**
5. in **protocol and ports** Leave default Setting and click **Next**
6. in **Scope** Screen Under **Which remote IP address Does This rule apply to?** select **These IP address** and click **add** Button
7. in **IP Address** Dialog under **This IP address or subnet:**enter IP address of website and click ok and then click next.
8. in **Action** screen select **Block the connection** and click next
9. in **Profile** screen leave all 3 check box selected and click next
10. in **Name** Screen choose name for rule and click finish test what you do by enter URL in any browser that you want