Practical No.1 Substitution Cipher Techniques-1

Aim:- Write a program to implement the following substitution cipher technique.

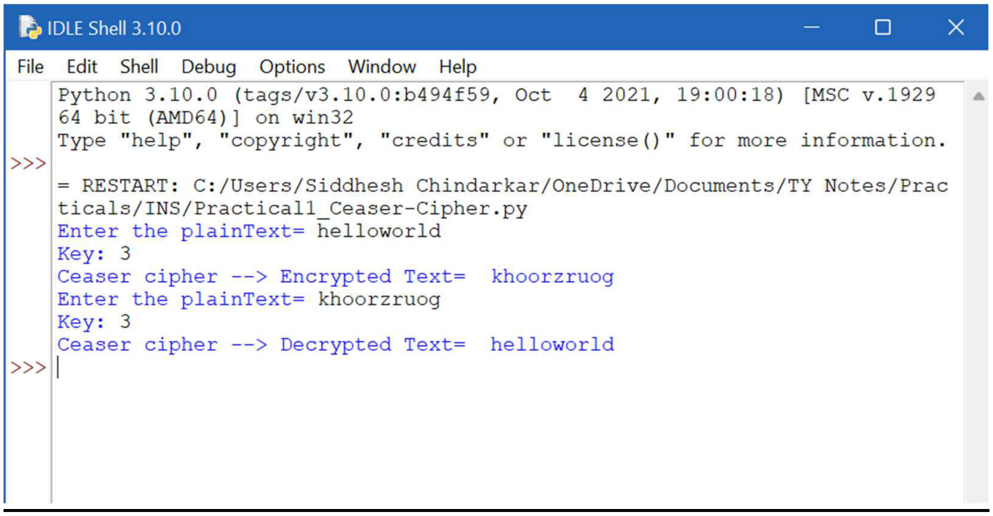
i) Ceaser cipher

Code:-

```
def encryption(pt, key):
   list1="abcdefghijklmnopqrstuvwxyz"
   en=''
   for i in pt.lower():
      k=(list1.index(i)+key)%26
      en+=list1[k]
   print("Ceaser cipher --> Encrypted Text= ", en)
def decryption(pt, key):
   list1="abcdefghijklmnopqrstuvwxyz"
   en=''
   for i in pt.lower():
      k=(list1.index(i)-key)%26
      en+=list1[k]
   print("Ceaser cipher --> Decrypted Text= ", en)
pt=input("Enter the plainText= ")
key=int(input("Key: "))
encryption(pt,key)
pt=input("Enter the plainText= ")
key=int(input("Key: "))
```

```
decryption(pt,key)
```

Output:-



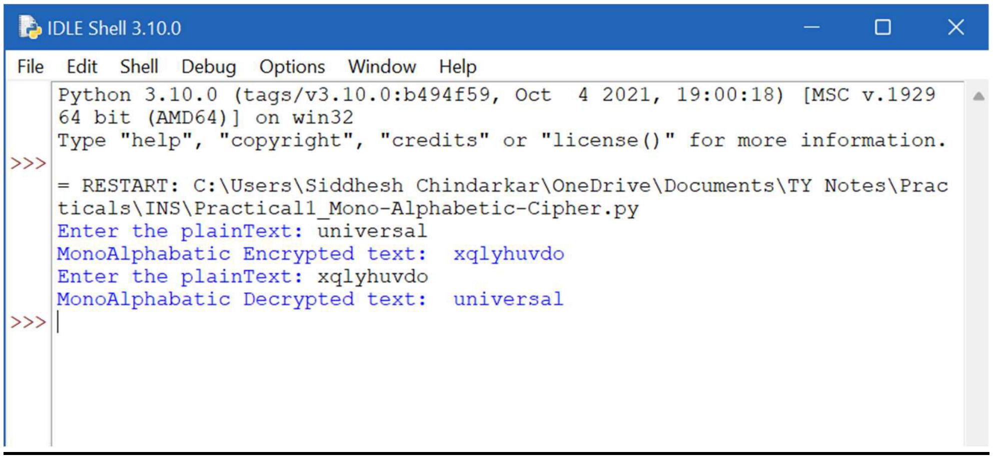
```
Python 3.10.0 (tags/v3.10.0:b494f59, Oct  4 2021, 19:00:18) [MSC v.1929
64 bit (AMD64)] on win32
Type "help", "copyright", "credits" or "license()" for more information.
>>>
= RESTART: C:/Users/Siddhesh Chindarkar/OneDrive/Documents/TY Notes/Prac
ticals/INS/Practical1_Ceaser-Cipher.py
Enter the plainText= helloworld
Key: 3
Ceaser cipher --> Encrypted Text=  khoorzruog
Enter the plainText= khoorzruog
Key: 3
Ceaser cipher --> Decrypted Text=  helloworld
>>>
```

ii) Monoalphabetic cipher

Code:-

```
def mono_encrypt(pt):
   a1="abcdefghijklmnopqrstuvwxyz"
   key="defghijklmnopqrstuvwxyzabc"
   en=''

   for j in pt.lower():
      for i in a1:
         if i==j:
            en+=key[a1.index(i)]
   print("MonoAlphabatic Encrypted text: ",en)

def mono_decrypt(pt):
   a1="abcdefghijklmnopqrstuvwxyz"
   key="defghijklmnopqrstuvwxyzabc"
   de=''
   for j in pt.lower():
    for i in a1:
        if i==j:
            de+=a1[key.index(i)]
  print("MonoAlphabatic Decrypted text: ",de)


pt=input("Enter the plainText: ")
mono_encrypt(pt)
pt=input("Enter the plainText: ")
mono_decrypt(pt)
```

Output:-



```
Python 3.10.0 (tags/v3.10.0:b494f59, Oct  4 2021, 19:00:18) [MSC v.1929
64 bit (AMD64)] on win32
Type "help", "copyright", "credits" or "license()" for more information.
>>>
= RESTART: C:\Users\Siddhesh Chindarkar\OneDrive\Documents\TY Notes\Prac
ticals\INS\Practical1_Mono-Alphabetic-Cipher.py
Enter the plainText: universal
MonoAlphabatic Encrypted text:  xqlyhuvdo
Enter the plainText: xqlyhuvdo
MonoAlphabatic Decrypted text:  universal
>>>
```

Practical No.2 Substitution Cipher Techiques-2

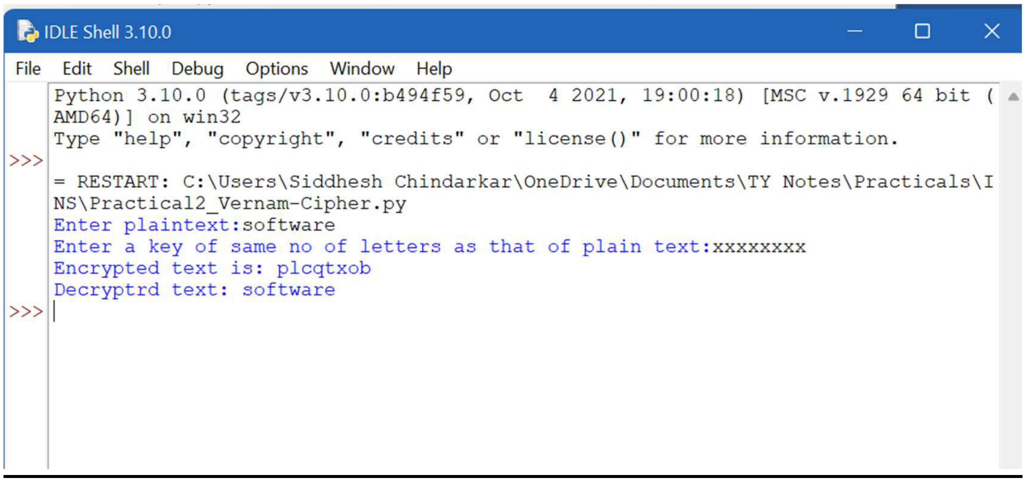
Aim:- Write a program to implement the following substitution cipher technique.

i)Vernam Cipher

Code:-

```
def ver(pt,key):
    pt=pt.replace("","")
    al='abcdefghijklmnopqrstuvwxyz'
    en=''
    de=''
    i=0
    j=0
    n=0
    a=[]
    b=[]
    for x in range(0,len(pt)):
        a.append(0)
        b.append(0)
    for l1 in pt.lower():
        a[i]=al.index(l1)
        i+=1
    for l2 in key.lower():
        b[j]=al.index(l2)
        j+=1
    for k in range(0,len(pt)):
        s1=(a[k]+b[k])%26
        en+=al[s1]
    print("Encrypted text is:",en)
    for k in range(0,len(pt)):
        n=n+1
        s2=al.index(en[k])-al.index(key[n-1])
        de=de+al[s2%26]
    print("Decryptrd text:",de)
pt=input("Enter plaintext:")
key=input("Enter a key of same no of letters as that of plain text:")
ver(pt,key)
```

Output:-



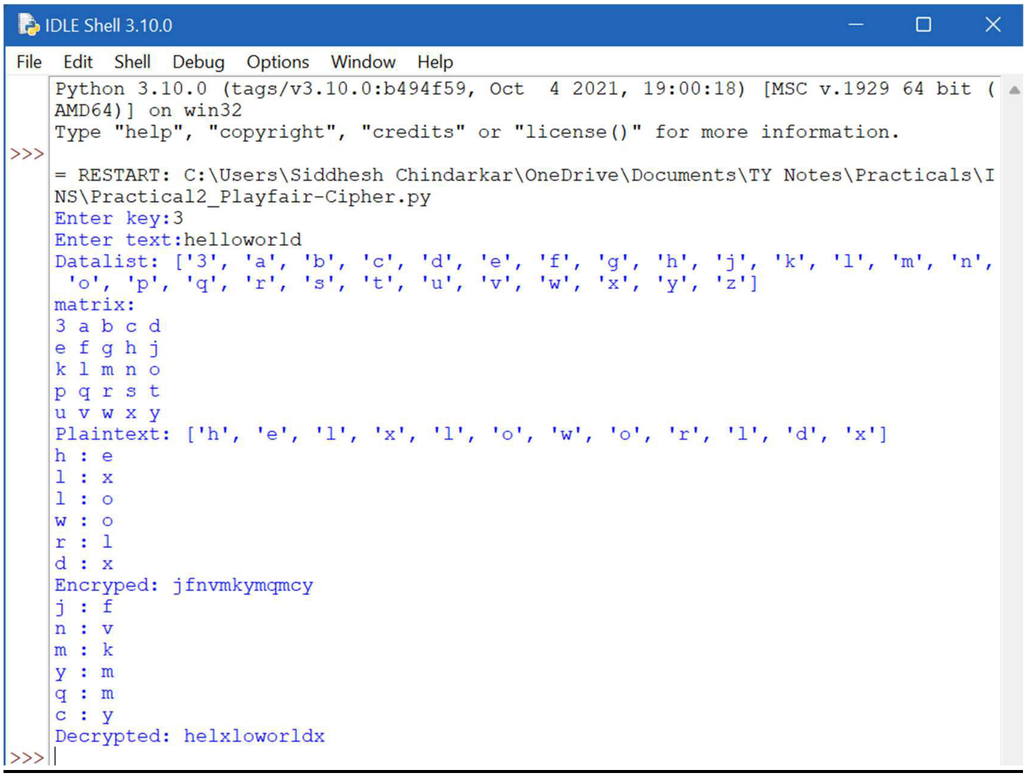
```
Python 3.10.0 (tags/v3.10.0:b494f59, Oct  4 2021, 19:00:18) [MSC v.1929 64 bit (
AMD64)] on win32
Type "help", "copyright", "credits" or "license()" for more information.
>>>
= RESTART: C:\Users\Siddhesh Chindarkar\OneDrive\Documents\TY Notes\Practicals\I
NS\Practical2_Vernam-Cipher.py
Enter plaintext:software
Enter a key of same no of letters as that of plain text:xxxxxxxx
Encrypted text is: plcqtxob
Decryptrd text: software
>>>
```

ii) Playfair Cipher

Code:-

```
from itertools import product
from re import findall
array= ['a','b','c','d','e','f','g','h','i','j','k','l','m','n','o','p','q','r','s','t','u','v','w','x','y','z']
def datalist_normal(key):
    key=key.replace(" ","")
    key=key.lower()
    list1=list()
    for i in range(len(key)):
        char=key[i]
        if char not in list1:
            if char=='i':
                list1.append('j')
            else:
                list1.append(char)
    for i in range(len(array)):
        char=array[i]
        if char not in list1:
            if char=='i':
                list1.append('j')
            else:
                list1.append(char)
    return list1
def matrix(list1):
    m=[]
    index=0
    for i in range(5):
        a=[]
        for j in range(5):
            a.append(list1[index])
            index=index+1
        m.append(a)
    print("matrix:")
    for i in range(5):
        for j in range(5):
            print(m[i][j],end=" ")
        print()
    return m
def plain(text):
    text=text.replace(" ","")
    p=list()
    for i in range(len(text)):
        char=text[i]
        if char=='i':
            p.append('j')
        else:
            p.append(char)
    for i in range(0,len(p),2):
        if i<len(p)-1:
            if p[i]==p[i+1]:
                p.insert(i+1,"x")
        if len(p)%2!=0:
            p.append("x")
    return p
def enc(p, m):
    encr=""
    for i in range(0,len(p),2):
        print(p[i],":",p[i+1])
        for j in range(5):
            for k in range(5):
                if p[i] == m[j][k]:
                    a=j
                    b=k
        for j in range(5):
            for k in range(5):
                if p[i+1] == m[j][k]:
                    c=j
                    d=k
        if a==c and b!=d:
            encr+=(m[a][(b+1)%5])
            encr+=(m[c][(d+1)%5])
        elif b==d and a!=c:
            encr+=(m[(a+1)%5][b])
            encr+=(m[(c+1)%5][d])
        else:
            encr+=(m[a][d])
            encr+=(m[c][b])
    return encr
def dec(p, m):
    decr=""
    for i in range(0,len(p),2):
        print(p[i],":",p[i+1])
        for j in range(5):
            for k in range(5):
                if p[i] == m[j][k]:
                    a=j
                    b=k
        for j in range(5):
            for k in range(5):
                if p[i+1] == m[j][k]:
                    c=j
                    d=k
        if a==c and b!=d:
            decr+=(m[a][(b-1)%5])
            decr+=(m[c][(d-1)%5])
        elif b==d and a!=c :
            decr+=(m[(a-1)%5][b])
            decr+=(m[(c-1)%5][d])
        else:
            decr+=(m[a][d])
            decr+=(m[c][b])
    return decr
key=input("Enter key:")
text=input("Enter text:")
#creating datalist
list1=datalist_normal(key)
print("Datalist:",list1)
#creating matrix
matrix1=matrix(list1)
#creating plaintext list and adding dummy letters
plaintext=plain(text)
print("Plaintext:",plaintext)
#Creating pairs
#pair(plaintext)
#encrption
encrypt=enc(plaintext, matrix1)
print("Encryped:",encrypt)
#decryption
decrypt=dec(encrypt, matrix1)
print("Decrypted:",decrypt)
```

Output:-



```
Python 3.10.0 (tags/v3.10.0:b494f59, Oct  4 2021, 19:00:18) [MSC v.1929 64 bit (
AMD64)] on win32
Type "help", "copyright", "credits" or "license()" for more information.
>>>
= RESTART: C:\Users\Siddhesh Chindarkar\OneDrive\Documents\TY Notes\Practicals\I
NS\Practical2_Playfair-Cipher.py
Enter key:3
Enter text:helloworld
Datalist: ['3', 'a', 'b', 'c', 'd', 'e', 'f', 'g', 'h', 'j', 'k', 'l', 'm', 'n',
 'o', 'p', 'q', 'r', 's', 't', 'u', 'v', 'w', 'x', 'y', 'z']
matrix:
3 a b c d
e f g h j
k l m n o
p q r s t
u v w x y
Plaintext: ['h', 'e', 'l', 'x', 'l', 'o', 'w', 'o', 'r', 'l', 'd', 'x']
h : e
l : x
l : o
w : o
r : l
d : x
Encryped: jfnvmkymqmcy
j : f
n : v
m : k
y : m
q : m
c : y
Decrypted: helxloworldx
>>>
```

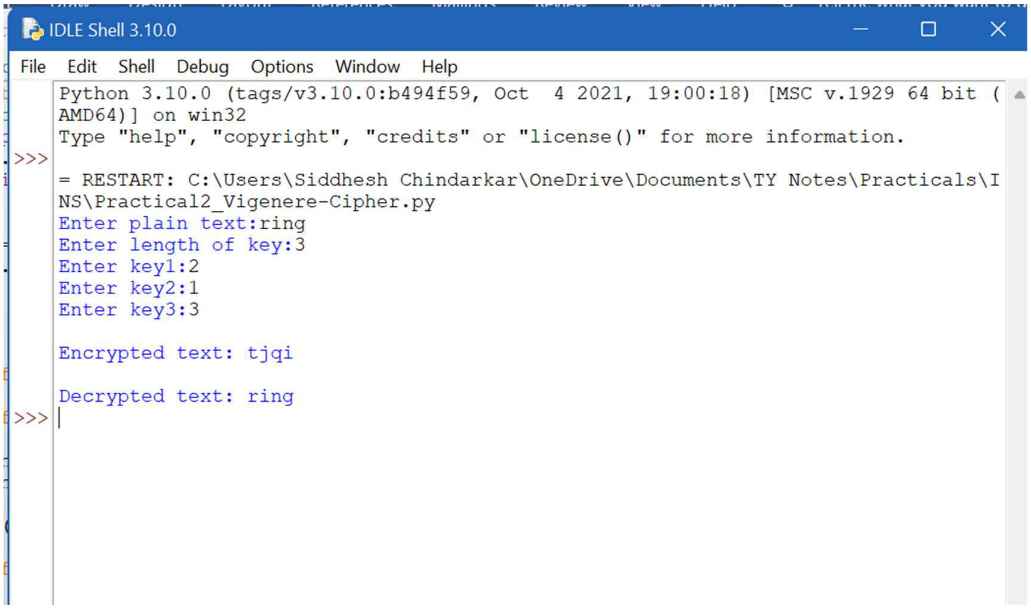
ii)Vigenere Cipher

Code:-

```
import math

l="abcdefghijklmnopqrstuvwxyz"

pt=input("Enter plain text:")

pt=pt.replace("","")

lenk=int(input("Enter length of key:"))

k=[]

for i in range(0,lenk):

   v=int(input("Enter key"+str(i+1)+":"))

   k.append(v)

en=""

de=""

n=0
```

```
for i in range(0,len(pt)):
   if(n<len(k)):
      n=n+1
   if(n>=len(k)):
      n=0
   ind=l.index(pt[i])+k[n-1]
   en=en+l[ind%26]
n=0
print("\nEncrypted text:",en)
for i in range(0,len(pt)):
   if(n<len(k)):
      n=n+1
   if(n>=len(k)):
      n=0
   ind=l.index(en[i])-k[n-1]
   de=de+l[ind%26]
print("\nDecrypted text:",de)
```

Output:-



```
Python 3.10.0 (tags/v3.10.0:b494f59, Oct  4 2021, 19:00:18) [MSC v.1929 64 bit (
AMD64)] on win32
Type "help", "copyright", "credits" or "license()" for more information.
>>>
= RESTART: C:\Users\Siddhesh Chindarkar\OneDrive\Documents\TY Notes\Practicals\I
NS\Practical2_Vigenere-Cipher.py
Enter plain text:ring
Enter length of key:3
Enter key1:2
Enter key2:1
Enter key3:3

Encrypted text: tjqi

Decrypted text: ring
>>>
```

Practical No.3 Transposition Cipher Techniques

Aim:- Write Programs to implement the following transposition cipher techniques:-

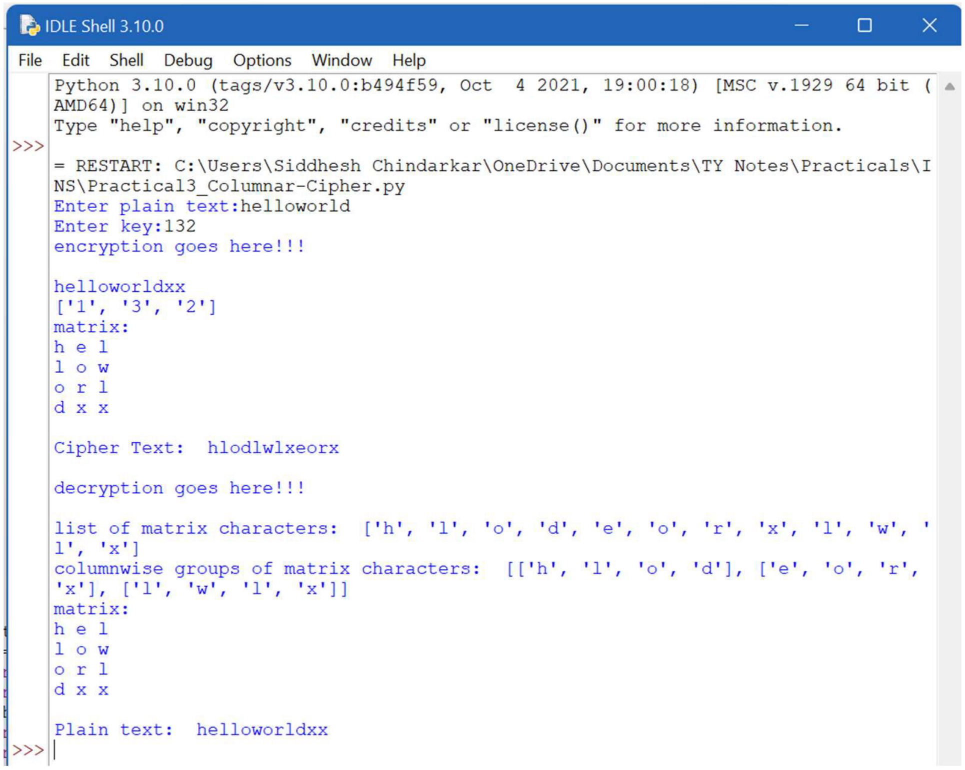
i)Simple Columnar Technique

Code:-

```
def plainText(text,key):
    text=text.lower()
    text=text.replace(" ","")
    for i in range(len(text)):
        if len(text)%len(key)!=0:
            text+="x"
    return text
def keyList(key):
    list1=list()
    for i in range(len(key)):
        list1.append(key[i])
    return list1
#Encryption Starts here!!!!
def matrix_encrypt(text,list1):
    m=[]
    index=0
    for i in range(len(text)//len(list1)):
        a=[]
        for j in range(len(list1)):
            if index<len(text):
                a.append(text[index])
                index=index+1
        m.append(a)
    print("matrix:")

    for i in range(len(text)//len(list1)):

        for j in range(len(list1)):

            print(m[i][j],end=" ")

        print()

    return m

def encrypt(m, list1,list2, text):

    en=""

    row=(len(text)//len(list1))

    for k in range(len(list1)):

        num=list1.index(min(list2))

        list2.remove(min(list2))

        for i in range(row):

            for j in range(len(list1)):

                #print(m[i])

                #print(num)

                en+=m[i][num]

                break

    print(" ")

    print("Cipher Text: ",en)

    return en

def encryptionAlgo(text, key):

    plain_text=plainText(text,key)

    key_list1=keyList(key)

    key_list2=keyList(key)

    print(plain_text)

    print(key_list1)

    m_plain=matrix_encrypt(plain_text,key_list1)

    cipher=encrypt(m_plain,key_list1, key_list2, plain_text)
    return cipher
#Decryption Starts here!!!!
def keyList(key):
    list1=list()
    for i in range(len(key)):
        list1.append(key[i])
    return list1
def matrix_list(cipher, list1):
    a=[]
    matrix_list=list()
    var=len(cipher)//len(list1)
    index=0
    for i in range(len(list1)):
        if index<len(list1):
            letter=list1[i]
            letter=int(letter)
            num=(letter*var)-var
            for j in range(num,num+var):
                a.append(cipher[j])
        else:
            break
    print("list of matrix characters: ",a)
    return a
def matrix_decrypt(mat_list,list1):
    m=[]
    index=0
    for i in range(len(list1)):
        a=[]
        for j in range(len(mat_list)//len(list1)):
            if index<len(mat_list):
                a.append(mat_list[index])
                index=index+1
        m.append(a)
    print("columnwise groups of matrix characters: ",m)
    print("matrix:")
    for i in range(len(mat_list)//len(list1)):#
        for j in range(len(list1)):#
            print(m[j][i],end=" ")
        print()
    return m
def decryption(m,mat_list,list1):
    de=""
    for i in range(len(mat_list)//len(list1)):#
        for j in range(len(list1)):#
            de+=m[j][i]
    print(" ")
    print("Plain text: ",de)
    return de
def decryptionAlgo(cipher, key):
    list1=keyList(key)
    mat_list=matrix_list(cipher, list1)
    m=matrix_decrypt(mat_list,list1)
    plain=decryption(m,mat_list,list1)
    return plain
text=input("Enter plain text:")
key=input("Enter key:")
print("encryption goes here!!!")
print(" ")
```

```
cipher=encryptionAlgo(text, key)

print(" ")

print("decryption goes here!!!")

print(" ")

plain=decryptionAlgo(cipher, key)
```

Output:-



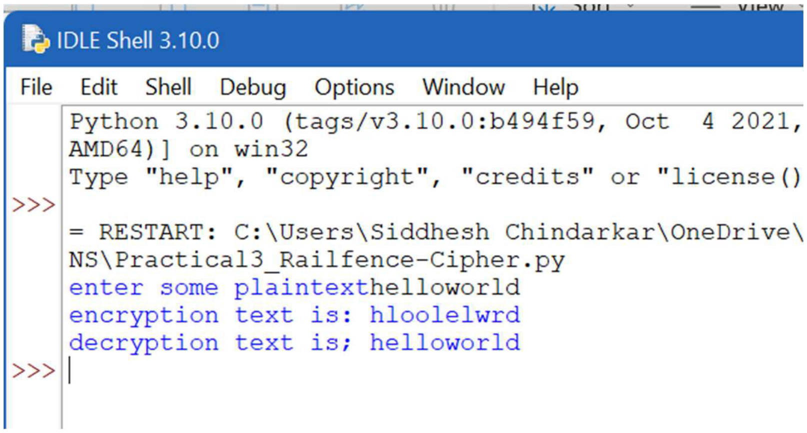
```
Python 3.10.0 (tags/v3.10.0:b494f59, Oct  4 2021, 19:00:18) [MSC v.1929 64 bit (
AMD64)] on win32
Type "help", "copyright", "credits" or "license()" for more information.
>>>
= RESTART: C:\Users\Siddhesh Chindarkar\OneDrive\Documents\TY Notes\Practicals\I
NS\Practical3_Columnar-Cipher.py
Enter plain text:helloworld
Enter key:132
encryption goes here!!!

helloworldxx
['1', '3', '2']
matrix:
h e l
l o w
o r l
d x x

Cipher Text:  hlodlwlxeorx

decryption goes here!!!

list of matrix characters:  ['h', 'l', 'o', 'd', 'e', 'o', 'r', 'x', 'l', 'w', '
l', 'x']
columnwise groups of matrix characters:  [['h', 'l', 'o', 'd'], ['e', 'o', 'r',
'x'], ['l', 'w', 'l', 'x']]
matrix:
h e l
l o w
o r l
d x x

Plain text:  helloworldxx
>>> |
```

ii)Railfence Technique

Code:-

```
def rf(pt):

    pt=pt.replace("","")

    u=""

    l=""

    en=""

    de=""

    j=len(pt)//2
    for i in range(0,len(pt)):
        if(i%2==0):
            u+=pt[i]
        else:
            l+=pt[i]
    en=u+l
    print("encryption text is:",en)
    if(len(pt)%2==0):
        for i in range(0,j):
            de+=u[i]
            de+=l[i]
        print("decryption text is;",de)
    else:
        for i in range(0,j):
            de+=u[i]
            de+=l[i]
        de+=u[-l]
        print("decryption text is:",de)
pt=input("enter some plaintext")
rf(pt)
```

Output:-



```
Python 3.10.0 (tags/v3.10.0:b494f59, Oct  4 2021,
AMD64)] on win32
Type "help", "copyright", "credits" or "license()
>>>
= RESTART: C:\Users\Siddhesh Chindarkar\OneDrive\
NS\Practical3_Railfence-Cipher.py
enter some plaintexthelloworld
encryption text is: hloolelwrd
decryption text is; helloworld
>>> |
```

Practical No.4

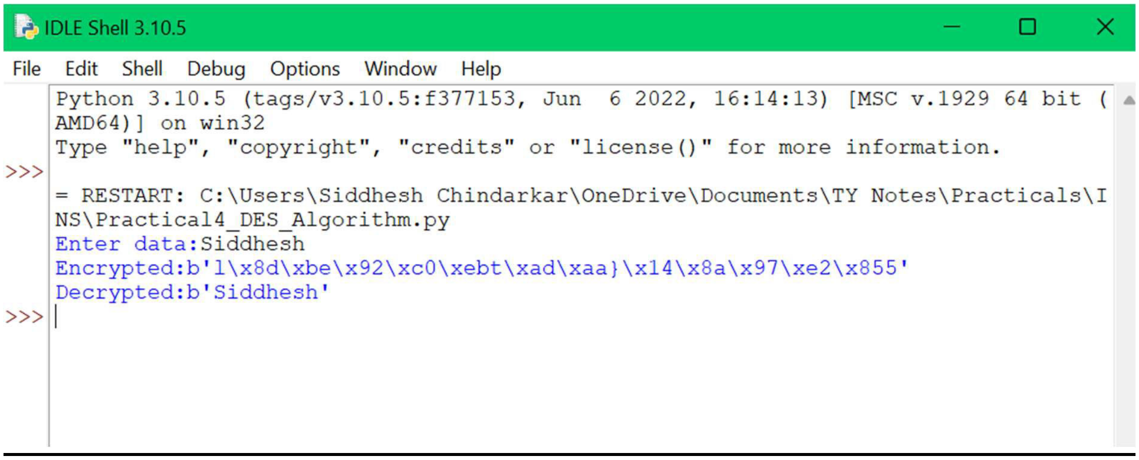
Aim:- Write program to encrypt and decrypt strings using - DES Algorithm.

i) DES Algorithm

Code:-

```
#DES

from pyDes import*

data=input("Enter data:")

k=des("Descrypt",CBC,"\0\0\0\0\0\0\0\0",pad=None,padmode=PAD_PKCS5)

d=k.encrypt(data)

print("Encrypted:%r"%d)

print("Decrypted:%r"%k.decrypt(d))
```

Output:-



```
Python 3.10.5 (tags/v3.10.5:f377153, Jun  6 2022, 16:14:13) [MSC v.1929 64 bit (
AMD64)] on win32
Type "help", "copyright", "credits" or "license()" for more information.
>>>
= RESTART: C:\Users\Siddhesh Chindarkar\OneDrive\Documents\TY Notes\Practicals\I
NS\Practical4_DES_Algorithm.py
Enter data:Siddhesh
Encrypted:b'l\x8d\xbe\x92\xc0\xebt\xad\xaa}\x14\x8a\x97\xe2\x855'
Decrypted:b'Siddhesh'
>>> |
```

ii) AES Algorithm

Code:-

```
#AES

import pyaes

aes=pyaes.AESModeOfOperationCTR(b'DESCRYPTDESCRYPT')
```

plaintext=input("enter text:")

ct=aes.encrypt(plaintext)

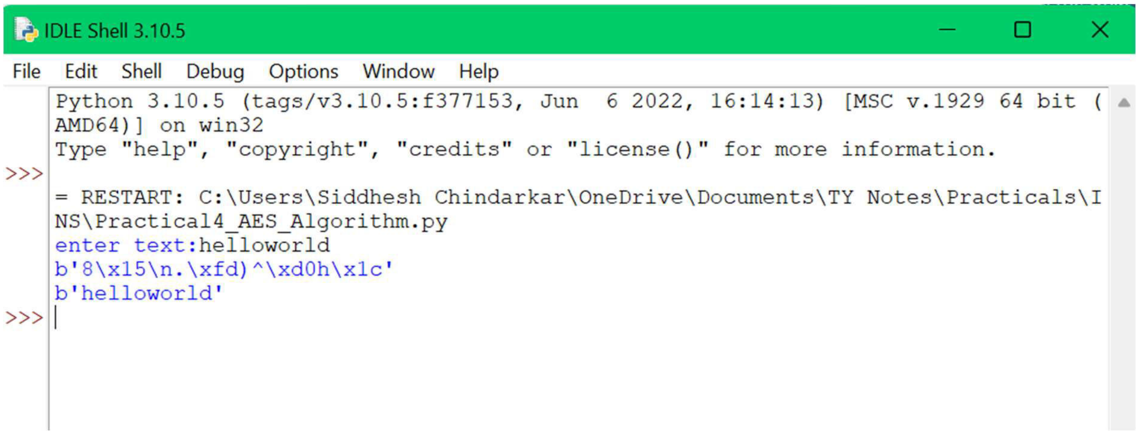
print(ct)

aes=pyaes.AESModeOfOperationCTR(b'DESCRYPTDESCRYPT')

plaintext=aes.decrypt(ct)

print(plaintext)

Output:-



```
Python 3.10.5 (tags/v3.10.5:f377153, Jun  6 2022, 16:14:13) [MSC v.1929 64 bit (
AMD64)] on win32
Type "help", "copyright", "credits" or "license()" for more information.
>>> 
= RESTART: C:\Users\Siddhesh Chindarkar\OneDrive\Documents\TY Notes\Practicals\I
NS\Practical4_AES_Algorithm.py
enter text:helloworld
b'8\x15\n.\xfd)^\xd0h\x1c'
b'helloworld'
>>> 
```

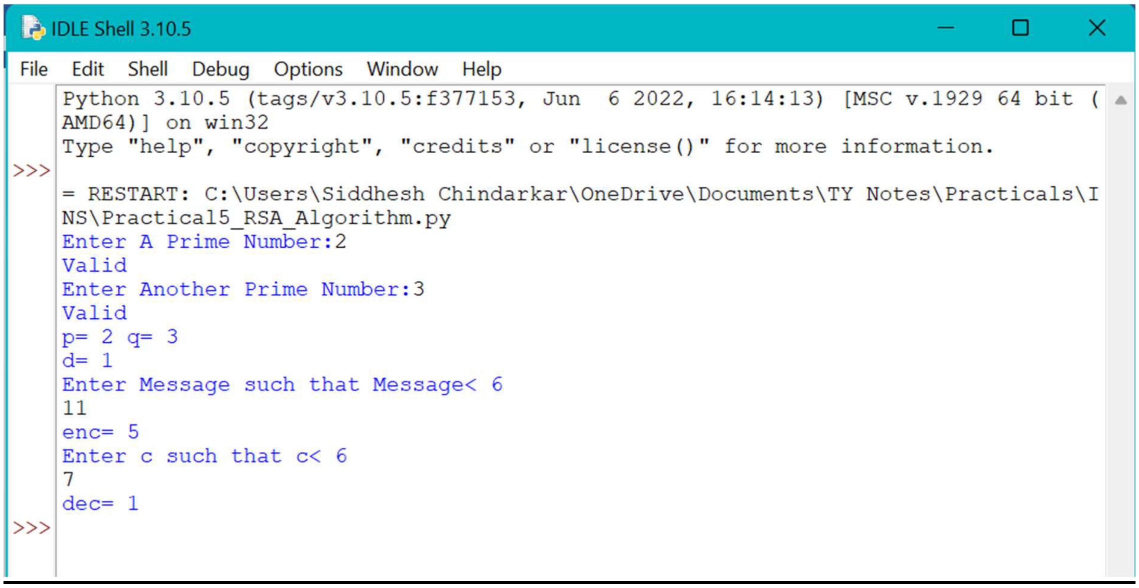
Practical No.5

Aim:- Write a program to implement RSA algorithm to perform encryption / decryption of a given string.

Code:-

```
def gcd(m,n):
    if m<n:
        (m,n)=(n,m)
    if(m%n)==0:
        return n
    else:
        return(gcd(n,m%n))#Recursion taking place
def rsaAlgo(p,q):
    print("p=",p,"q=",q)
    n=p*q
    fin=(p-1)*(q-1)
    for i in range(1,fin):
        if gcd(i,fin)==1:
            e=i
            d=i
    print("d=",d)
    #Encryption
    print("Enter Message such that Message<",n)
    message=int(input(""))
    enc=message**e%n
    print("enc=",enc)


    #Decryption
    print("Enter c such that c<",n)
    cipher=int(input(""))
    dec=cipher**d%n
    print("dec=",dec)
def primeNum(n):
    if n>1:
        for i in range(2,n):
            if n%i==0:
                print("Invalid")
                n=int(input("Enter a Prime Number"))
        else:
            print("Valid")
    else:
        print()
    return n
p=int(input("Enter A Prime Number:"))
p1=primeNum(p)
q=int(input("Enter Another Prime Number:"))
q1=primeNum(q)
rsaAlgo(p1,q1)
```

Output:-



```
Python 3.10.5 (tags/v3.10.5:f377153, Jun  6 2022, 16:14:13) [MSC v.1929 64 bit (
AMD64)] on win32
Type "help", "copyright", "credits" or "license()" for more information.
>>>
= RESTART: C:\Users\Siddhesh Chindarkar\OneDrive\Documents\TY Notes\Practicals\I
NS\Practical5_RSA_Algorithm.py
Enter A Prime Number:2
Valid
Enter Another Prime Number:3
Valid
p= 2 q= 3
d= 1
Enter Message such that Message< 6
11
enc= 5
Enter c such that c< 6
7
dec= 1
>>>
```

Practical No.6 Diffie-Hellman Key Exchange

Aim:- Write a program to implement the Diffie-Hellman Key Agreement algorithm to generate symmetric keys.

Code:-

```
#Diffie Hellman Key Exchange

from math import sqrt

# Returns True if n is prime

def isPrime( n):

    # Corner cases

    if (n <= 1):

        return False

    if (n<= 3):

        return True

    if (n % 2 == 0 or n % 3 == 0):

        return False

    i = 5

    while(i * i <= n):

        if (n % i== 0 or n % (i + 2) == 0) :

            return False

        i= i + 6

    return True


def power(x,y,p):

    res = 1 # Initialize result
```

```
 x = x % p # Update x if it is more

 # than or equal to p

 while (y > 0):

 # If y is odd, multiply x with result

    if (y & 1):

       res = (res * x) % p

       y = y>>1

       x = (x * x) % p

 return res


# Utility function to store prime # factors of a number

def findPrimefactors(s, n) :

 while(n%2==0):

    # Print the number of 2s that divide n while (n % 2 == 0) :

    s.add(2)

    n = n // 2

    # n must be odd at this po. So we can # skip one element (Note i = i +2)

 for i in range(3, int(sqrt(n)), 2):

    # While i divides n, print i and divide n

    while (n % i == 0) :

       s.add(i)

       n = n // i

 if (n > 2) :

    s.add(n)
```

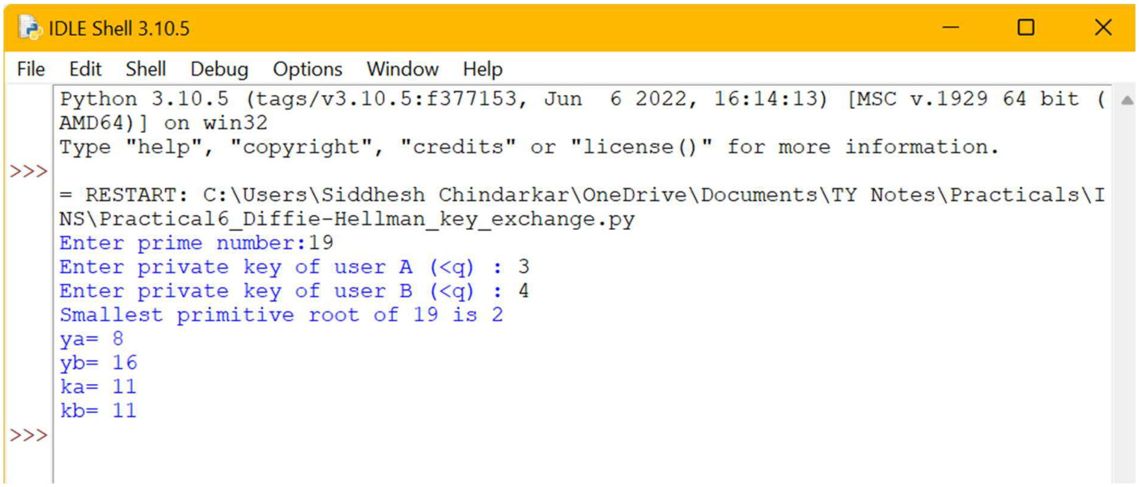
```
# Function to find smallest primitive # root of n
def findPrimitive( n) :
    s= set()
    # Check if n is prime or not
    if (isPrime(n) == False):
        return -1
    # Find value of Euler Totient function
    # of n. Since n is a prime number, the # value of Euler Totient function is n-1 # as there are n-1 relatively prime numbers.
    phi = n - 1
    # Find prime factors of phi and store in a set
    findPrimefactors(s, phi)
    # Check for every number from 2 to phi
    for r in range(2, phi + 1):
        # Iterate through all prime factors of phi. # and check if we found a power with value 1
        flag = False
        for it in s:
            if (pow(r, phi // it,n) == 1):
                flag = True
                break
            # If there was no power with value 1.
        if (flag == False):
            return r
            # If no primitive root found
    return r
#generating public key of user A,B
def pua(xa,a,q):
    if xa<q:
        ya=(a**xa)%q
        return ya
    else:
        print("xa should be < ", q)
        #key generation
def keyGen(x,y,q):
    k=(y**x)%q
    return k

q = int(input("Enter prime number:"))
a=findPrimitive(q)
xa=int(input("Enter private key of user A (<q) : "))
xb=int(input("Enter private key of user B (<q) : "))
ya=pua(xa,a,q)
yb=pua(xb,a,q)
ka=keyGen(xa,yb,q)
kb=keyGen(xb,ya,q)
print("Smallest primitive root of", q, "is", a)
print("ya=",ya)
```

print("yb=",yb)

print("ka=",ka)

print("kb=",kb)

Output:-



```
Python 3.10.5 (tags/v3.10.5:f377153, Jun  6 2022, 16:14:13) [MSC v.1929 64 bit (
AMD64)] on win32
Type "help", "copyright", "credits" or "license()" for more information.
>>> 
= RESTART: C:\Users\Siddhesh Chindarkar\OneDrive\Documents\TY Notes\Practicals\I
NS\Practical6_Diffie-Hellman_key_exchange.py
Enter prime number:19
Enter private key of user A (<q) : 3
Enter private key of user B (<q) : 4
Smallest primitive root of 19 is 2
ya= 8
yb= 16
ka= 11
kb= 11
>>> 
```

Practical No.7

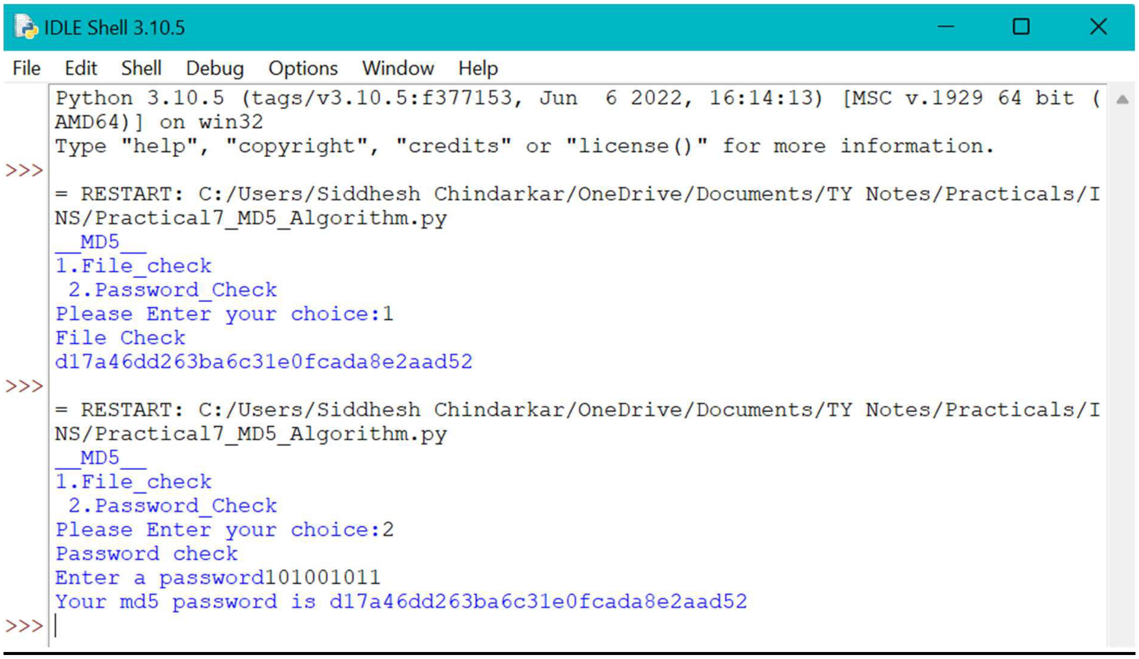
Aim:- Write a program to implement the MD5 algorithm compute the message digest.

Code:-

```
#MD5


import hashlib
def file_check(filename):
   hash1=hashlib.md5()
   with open(filename,'rb')as open_file:
      content=open_file.read()
      hash1.update(content)
   print(hash1.hexdigest())


def pass_check(pw):
   hash1=hashlib.md5(pw.encode('utf-8'))
   print ("Your md5 password is",hash1.hexdigest())


print("__MD5__")
print("1.File_check \n 2.Password_Check")
choice=int(input("Please Enter your choice:"))
if (choice ==1):
   print("File Check")
   fn='hello.txt'
   file_check(fn)
elif(choice==2):
   print("Password check")
   pw=input("Enter a password")
```

```
    pass_check(pw)
else:
    print("Wrong choice")
```

Output:-



```
Python 3.10.5 (tags/v3.10.5:f377153, Jun  6 2022, 16:14:13) [MSC v.1929 64 bit (
AMD64)] on win32
Type "help", "copyright", "credits" or "license()" for more information.
>>>
= RESTART: C:/Users/Siddhesh Chindarkar/OneDrive/Documents/TY Notes/Practicals/I
NS/Practical7_MD5_Algorithm.py
__MD5__
1.File_check
 2.Password_Check
Please Enter your choice:1
File Check
d17a46dd263ba6c31e0fcada8e2aad52
>>>
= RESTART: C:/Users/Siddhesh Chindarkar/OneDrive/Documents/TY Notes/Practicals/I
NS/Practical7_MD5_Algorithm.py
__MD5__
1.File_check
 2.Password_Check
Please Enter your choice:2
Password check
Enter a password101001011
Your md5 password is d17a46dd263ba6c31e0fcada8e2aad52
>>>
```

Practical No.8

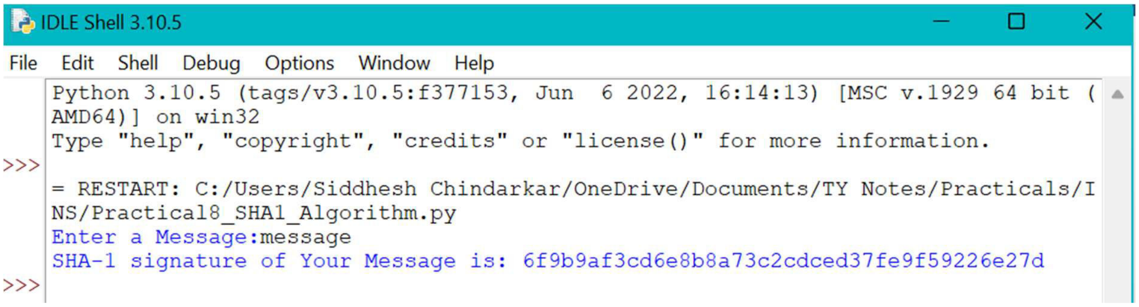
Aim:- Write a program to calculate HMAC-SHA1 Signature & HMAC-SHA512 Signature.

i) HMAC-SHA1 Signature

Code:-

```
import hashlib

def sha(m):

    m=m.encode("utf8")

    hash1=hashlib.sha1(m)

    print("SHA-1 signature of Your Message is:",hash1.hexdigest())

pt=input("Enter a Message:")

sha(pt)
```

Output:-



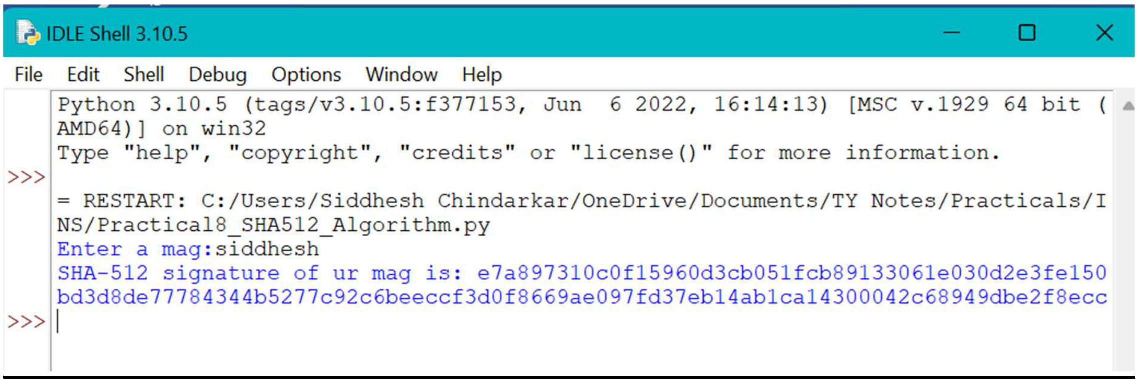
```
Python 3.10.5 (tags/v3.10.5:f377153, Jun  6 2022, 16:14:13) [MSC v.1929 64 bit (
AMD64)] on win32
Type "help", "copyright", "credits" or "license()" for more information.
>>>
= RESTART: C:/Users/Siddhesh Chindarkar/OneDrive/Documents/TY Notes/Practicals/I
NS/Practical8_SHA1_Algorithm.py
Enter a Message:message
SHA-1 signature of Your Message is: 6f9b9af3cd6e8b8a73c2cdced37fe9f59226e27d
>>>
```

ii) HMAC-SHA512 Signature

Code:-

```
import hashlib

def sha(m):

    m=m.encode("utf-8")

    hash512=hashlib.sha512(m)

    print("SHA-512 signature of ur mag is:",hash512.hexdigest())

pt=input("Enter a mag:")

sha(pt)
```

Output:-



```
Python 3.10.5 (tags/v3.10.5:f377153, Jun  6 2022, 16:14:13) [MSC v.1929 64 bit (
AMD64)] on win32
Type "help", "copyright", "credits" or "license()" for more information.
>>> 
= RESTART: C:/Users/Siddhesh Chindarkar/OneDrive/Documents/TY Notes/Practicals/I
NS/Practical8_SHA512_Algorithm.py
Enter a mag:siddhesh
SHA-512 signature of ur mag is: e7a897310c0f15960d3cb051fcb89133061e030d2e3fe150
bd3d8de77784344b5277c92c6beeccf3d0f8669ae097fd37eb14ab1ca14300042c68949dbe2f8ecc
>>> |
```

Practical No.9

Aim:- Configure Windows Firewall to block:-

i) A port

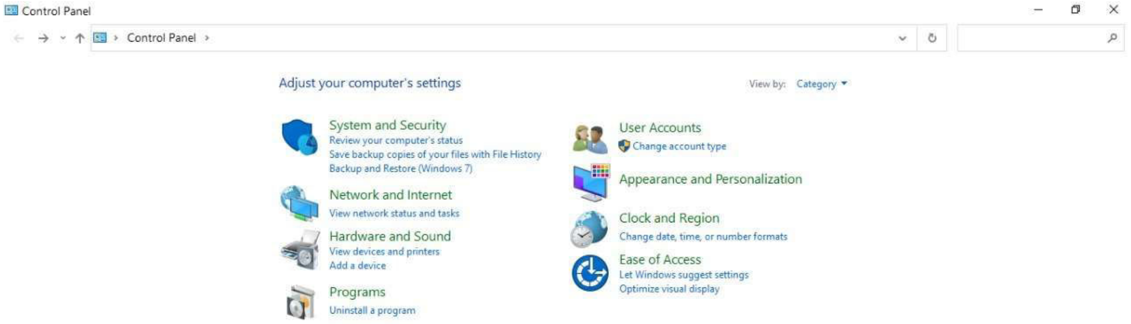
ii) An Program

iii) A website

i) A port

Steps:-

1. Open control panel.



Control Panel

Control Panel >

Adjust your computer's settings

View by: Category

System and Security
Review your computer's status
Save backup copies of your files with File History
Backup and Restore (Windows 7)

Network and Internet
View network status and tasks

Hardware and Sound
View devices and printers
Add a device

Programs
Uninstall a program

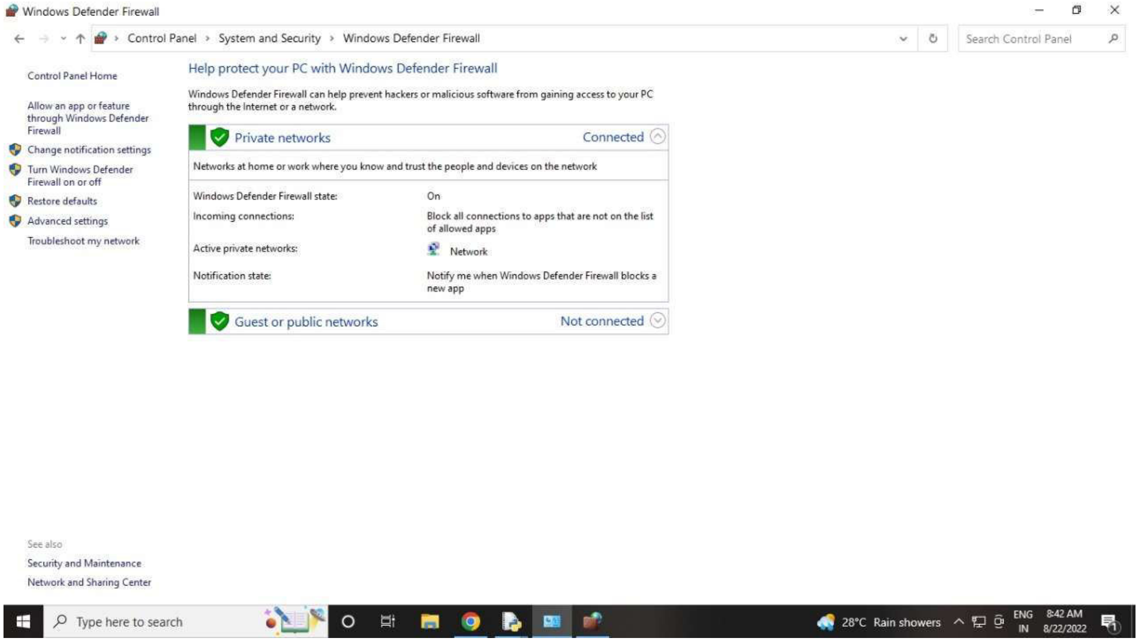
User Accounts
Change account type

Appearance and Personalization

Clock and Region
Change date, time, or number formats

Ease of Access
Let Windows suggest settings
Optimize visual display

2.Go to firewall in search box.



Windows Defender Firewall

Control Panel > System and Security > Windows Defender Firewall

Search Control Panel

Control Panel Home
Allow an app or feature through Windows Defender Firewall
Change notification settings
Turn Windows Defender Firewall on or off
Restore defaults
Advanced settings
Troubleshoot my network

Help protect your PC with Windows Defender Firewall

Windows Defender Firewall can help prevent hackers or malicious software from gaining access to your PC through the Internet or a network.

Private networks — Connected

Networks at home or work where you know and trust the people and devices on the network

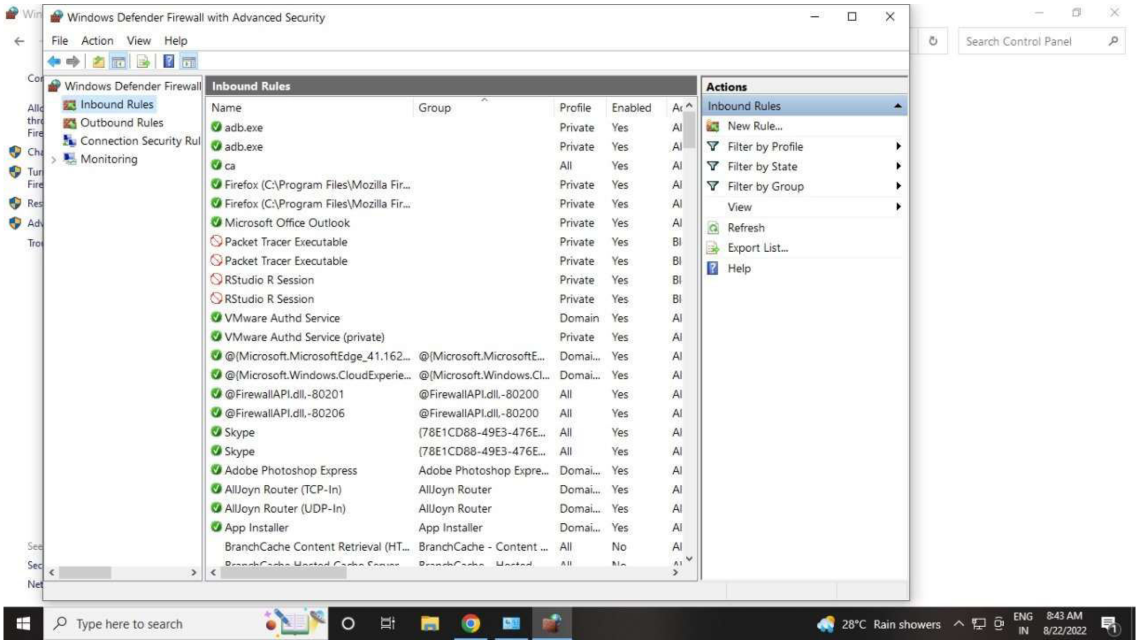
Windows Defender Firewall state:	On
Incoming connections:	Block all connections to apps that are not on the list of allowed apps
Active private networks:	Network
Notification state:	Notify me when Windows Defender Firewall blocks a new app

Guest or public networks — Not connected

See also
Security and Maintenance
Network and Sharing Center

Type here to search
28°C Rain showers ENG IN 8:42 AM 8/22/2022

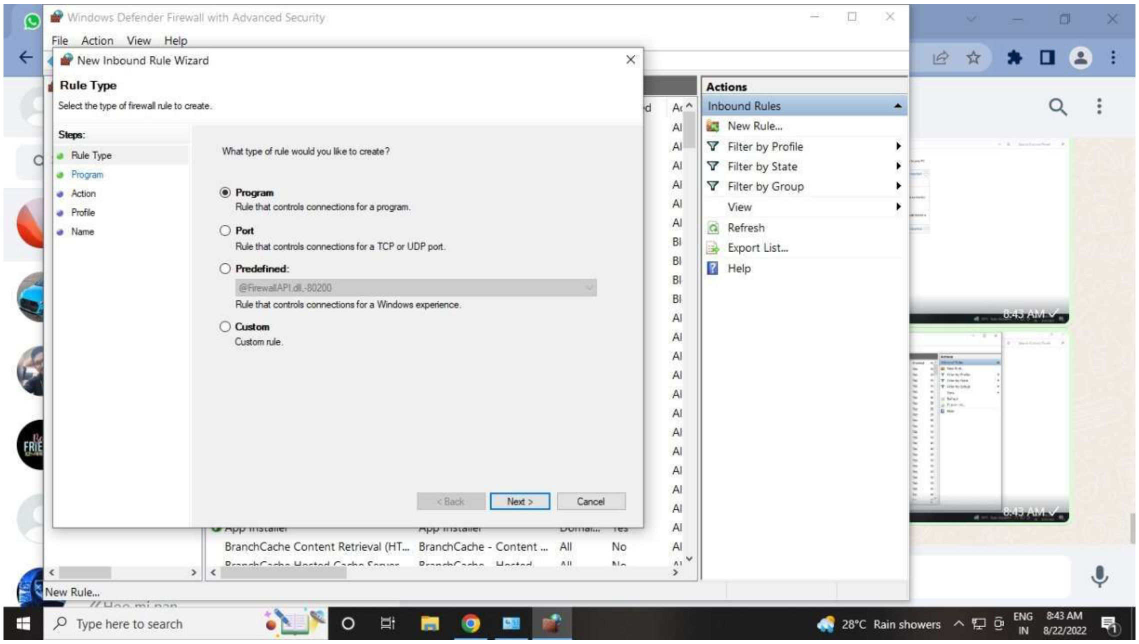
3.In the windows firewall, Click on advanced setting and then click on Inbound Rule.



Inbound Rules

Name	Group	Profile	Enabled	Ac
adb.exe		Private	Yes	Al
adb.exe		Private	Yes	Al
ca		All	Yes	Al
Firefox (C:\Program Files\Mozilla Fir...		Private	Yes	Al
Firefox (C:\Program Files\Mozilla Fir...		Private	Yes	Al
Microsoft Office Outlook		Private	Yes	Al
Packet Tracer Executable		Private	Yes	Bl
Packet Tracer Executable		Private	Yes	Bl
RStudio R Session		Private	Yes	Bl
RStudio R Session		Private	Yes	Bl
VMware Authd Service		Domain	Yes	Al
VMware Authd Service (private)		Private	Yes	Al
@{Microsoft.MicrosoftEdge_41.162...	@{Microsoft.MicrosoftE...	Domai...	Yes	Al
@{Microsoft.Windows.CloudExperie...	@{Microsoft.Windows.Cl...	Domai...	Yes	Al
@FirewallAPI.dll,-80201	@FirewallAPI.dll,-80200	All	Yes	Al
@FirewallAPI.dll,-80206	@FirewallAPI.dll,-80200	All	Yes	Al
Skype	{78E1CD88-49E3-476E...	All	Yes	Al
Skype	{78E1CD88-49E3-476E...	All	Yes	Al
Adobe Photoshop Express	Adobe Photoshop Expre...	Domai...	Yes	Al
AllJoyn Router (TCP-In)	AllJoyn Router	Domai...	Yes	Al
AllJoyn Router (UDP-In)	AllJoyn Router	Domai...	Yes	Al
App Installer	App Installer	Domai...	Yes	Al
BranchCache Content Retrieval (HT...	BranchCache - Content ...	All	No	Al

4.Go to new Rule in RHS.



New Inbound Rule Wizard

Rule Type

Select the type of firewall rule to create.

Steps:

- Rule Type
- Program
- Action
- Profile
- Name

What type of rule would you like to create?

● **Program**
Rule that controls connections for a program.

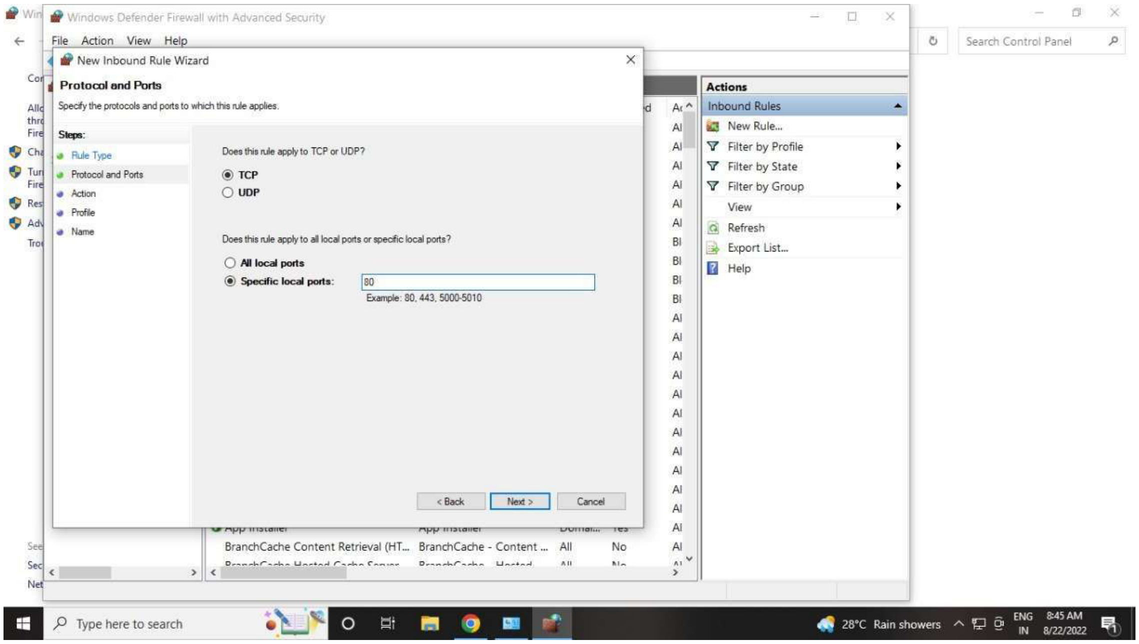
○ **Port**
Rule that controls connections for a TCP or UDP port.

○ **Predefined:**
@FirewallAPI.dll,-80200
Rule that controls connections for a Windows experience.

○ **Custom**
Custom rule.

< Back | Next > | Cancel

5.Go to the port and then set TCP and set Specific local ports which you want to block Eg.80.



New Inbound Rule Wizard

Protocol and Ports

Specify the protocols and ports to which this rule applies.

Steps:
- Rule Type
- Protocol and Ports
- Action
- Profile
- Name

Does this rule apply to TCP or UDP?

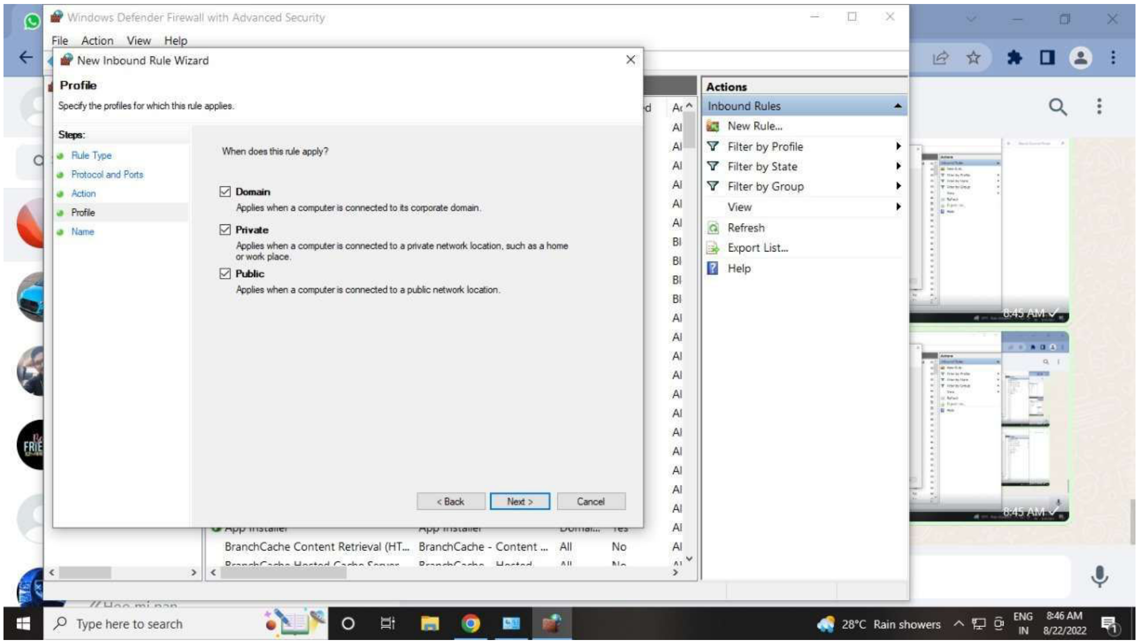
● TCP
○ UDP

Does this rule apply to all local ports or specific local ports?

○ All local ports
● Specific local ports: 80

Example: 80, 443, 5000-5010

6.Click next till the last dialog box appears.



New Inbound Rule Wizard

Profile

Specify the profiles for which this rule applies.

Steps:
- Rule Type
- Protocol and Ports
- Action
- Profile
- Name

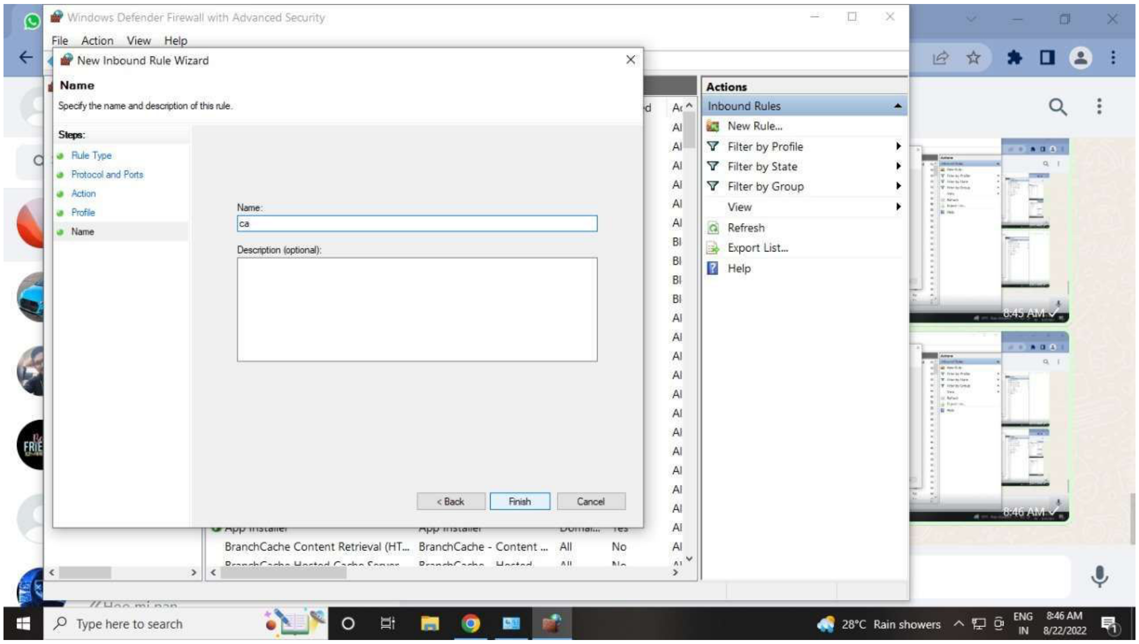
When does this rule apply?

☑ Domain
Applies when a computer is connected to its corporate domain.

☑ Private
Applies when a computer is connected to a private network location, such as a home or work place.

☑ Public
Applies when a computer is connected to a public network location.

7.Click Finish.



Name

Specify the name and description of this rule.

Steps:
- Rule Type
- Protocol and Ports
- Action
- Profile
- Name

Name: ca

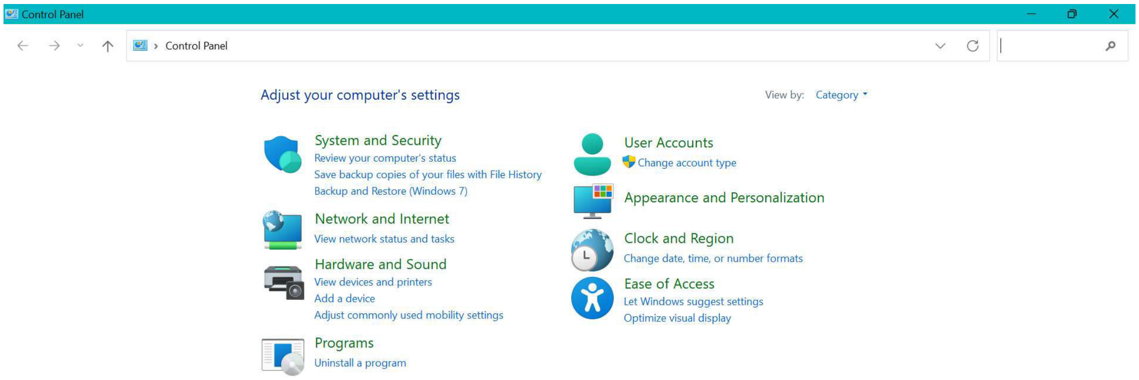
Description (optional):

< Back Finish Cancel

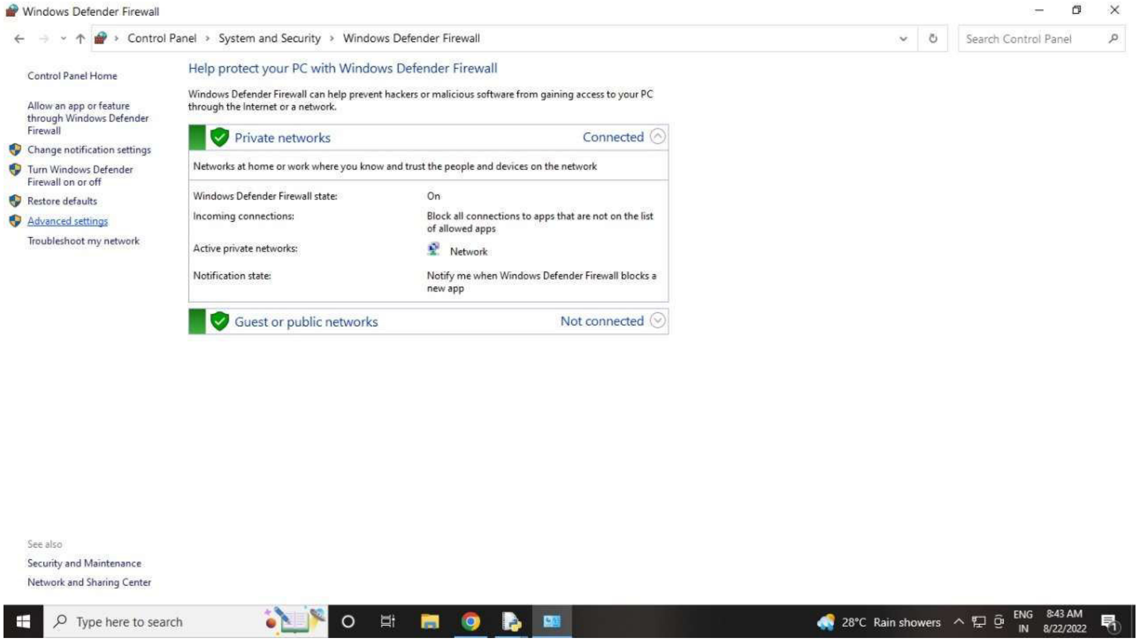
ii) An Program

<u>Steps:-</u>

1. Open control panel.


Control Panel
Control Panel
Adjust your computer's settings
View by: Category
System and Security
Review your computer's status
Save backup copies of your files with File History
Backup and Restore (Windows 7)
Network and Internet
View network status and tasks
Hardware and Sound
View devices and printers
Add a device
Adjust commonly used mobility settings
Programs
Uninstall a program
User Accounts
Change account type
Appearance and Personalization
Clock and Region
Change date, time, or number formats
Ease of Access
Let Windows suggest settings
Optimize visual display

2.Go to firewall in search box.


Windows Defender Firewall
Control Panel › System and Security › Windows Defender Firewall
Search Control Panel
Control Panel Home
Allow an app or feature through Windows Defender Firewall
Change notification settings
Turn Windows Defender Firewall on or off
Restore defaults
Advanced settings
Troubleshoot my network
See also
Security and Maintenance
Network and Sharing Center
Type here to search
28°C Rain showers
ENG IN
8:43 AM
8/22/2022

Help protect your PC with Windows Defender Firewall

Windows Defender Firewall can help prevent hackers or malicious software from gaining access to your PC through the Internet or a network.

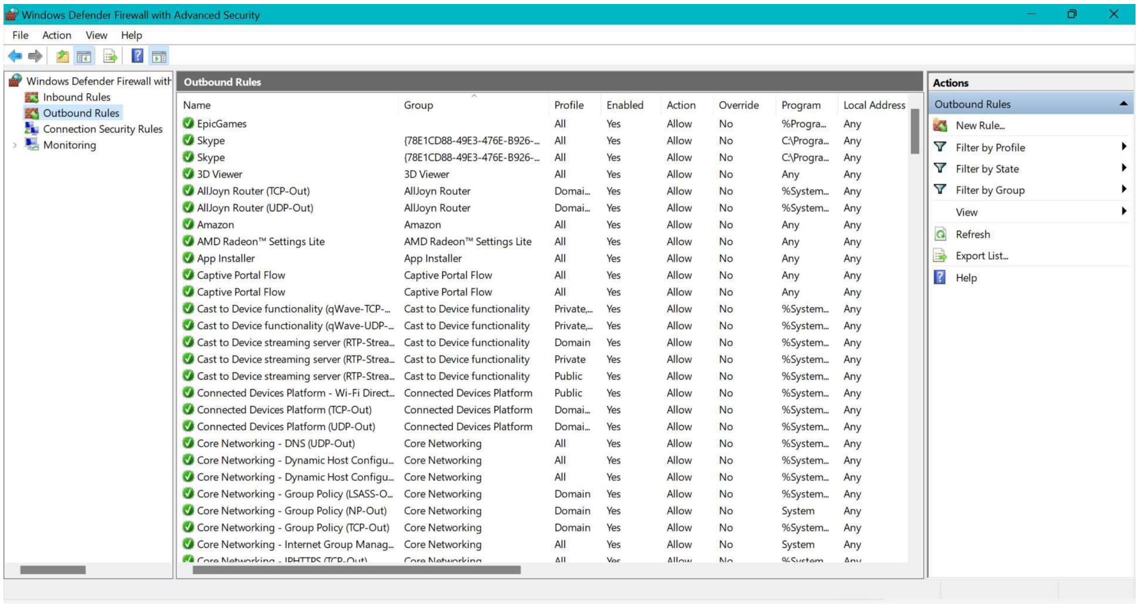
Private networks — Connected

Networks at home or work where you know and trust the people and devices on the network

Windows Defender Firewall state:	On
Incoming connections:	Block all connections to apps that are not on the list of allowed apps
Active private networks:	Network
Notification state:	Notify me when Windows Defender Firewall blocks a new app

Guest or public networks — Not connected

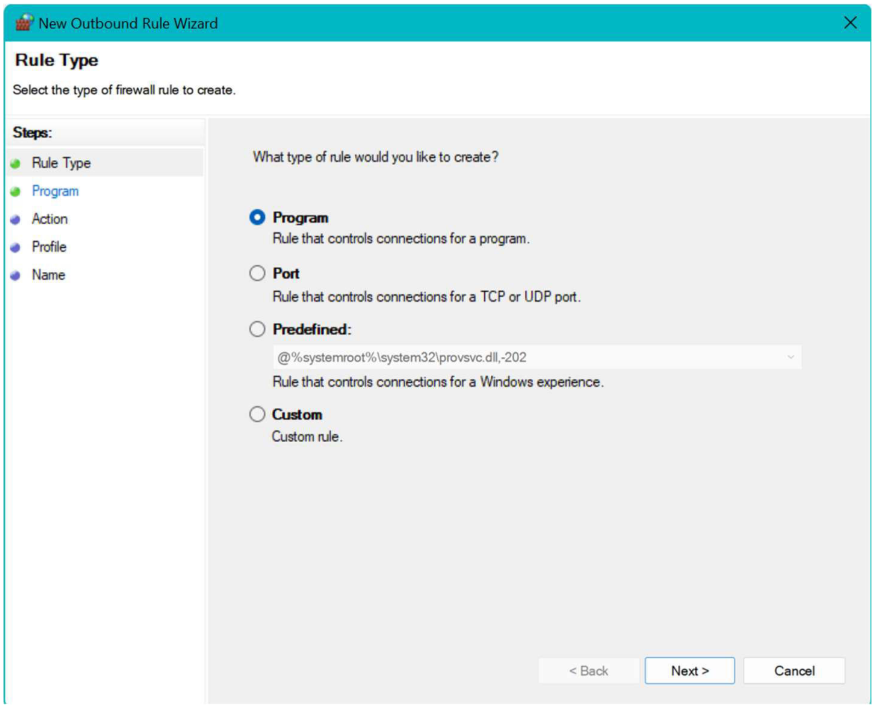
3.In the windows firewall, Click on advanced setting and then click on Outbound Rule.



Outbound Rules

Name	Group	Profile	Enabled	Action	Override	Program	Local Address
EpicGames		All	Yes	Allow	No	%Progra...	Any
Skype	{78E1CD88-49E3-476E-B926-...	All	Yes	Allow	No	C:\Progra...	Any
Skype	{78E1CD88-49E3-476E-B926-...	All	Yes	Allow	No	C:\Progra...	Any
3D Viewer	3D Viewer	All	Yes	Allow	No	Any	Any
AllJoyn Router (TCP-Out)	AllJoyn Router	Domai...	Yes	Allow	No	%System...	Any
AllJoyn Router (UDP-Out)	AllJoyn Router	Domai...	Yes	Allow	No	%System...	Any
Amazon	Amazon	All	Yes	Allow	No	Any	Any
AMD Radeon™ Settings Lite	AMD Radeon™ Settings Lite	All	Yes	Allow	No	Any	Any
App Installer	App Installer	All	Yes	Allow	No	Any	Any
Captive Portal Flow	Captive Portal Flow	All	Yes	Allow	No	Any	Any
Captive Portal Flow	Captive Portal Flow	All	Yes	Allow	No	Any	Any
Cast to Device functionality (qWave-TCP-...	Cast to Device functionality	Private,...	Yes	Allow	No	%System...	Any
Cast to Device functionality (qWave-UDP-...	Cast to Device functionality	Private,...	Yes	Allow	No	%System...	Any
Cast to Device streaming server (RTP-Strea...	Cast to Device functionality	Domain	Yes	Allow	No	%System...	Any
Cast to Device streaming server (RTP-Strea...	Cast to Device functionality	Private	Yes	Allow	No	%System...	Any
Cast to Device streaming server (RTP-Strea...	Cast to Device functionality	Public	Yes	Allow	No	%System...	Any
Connected Devices Platform - Wi-Fi Direct...	Connected Devices Platform	Public	Yes	Allow	No	%System...	Any
Connected Devices Platform (TCP-Out)	Connected Devices Platform	Domai...	Yes	Allow	No	%System...	Any
Connected Devices Platform (UDP-Out)	Connected Devices Platform	Domai...	Yes	Allow	No	%System...	Any
Core Networking - DNS (UDP-Out)	Core Networking	All	Yes	Allow	No	%System...	Any
Core Networking - Dynamic Host Configu...	Core Networking	All	Yes	Allow	No	%System...	Any
Core Networking - Dynamic Host Configu...	Core Networking	All	Yes	Allow	No	%System...	Any
Core Networking - Group Policy (LSASS-O...	Core Networking	Domain	Yes	Allow	No	%System...	Any
Core Networking - Group Policy (NP-Out)	Core Networking	Domain	Yes	Allow	No	System	Any
Core Networking - Group Policy (TCP-Out)	Core Networking	Domain	Yes	Allow	No	%System...	Any
Core Networking - Internet Group Manag...	Core Networking	All	Yes	Allow	No	System	Any
Core Networking - IPHTTPS (TCP-Out)	Core Networking	All	Yes	Allow	No	%System	Any

4.Go to new Rule in RHS.



New Outbound Rule Wizard

Rule Type

Select the type of firewall rule to create.

What type of rule would you like to create?

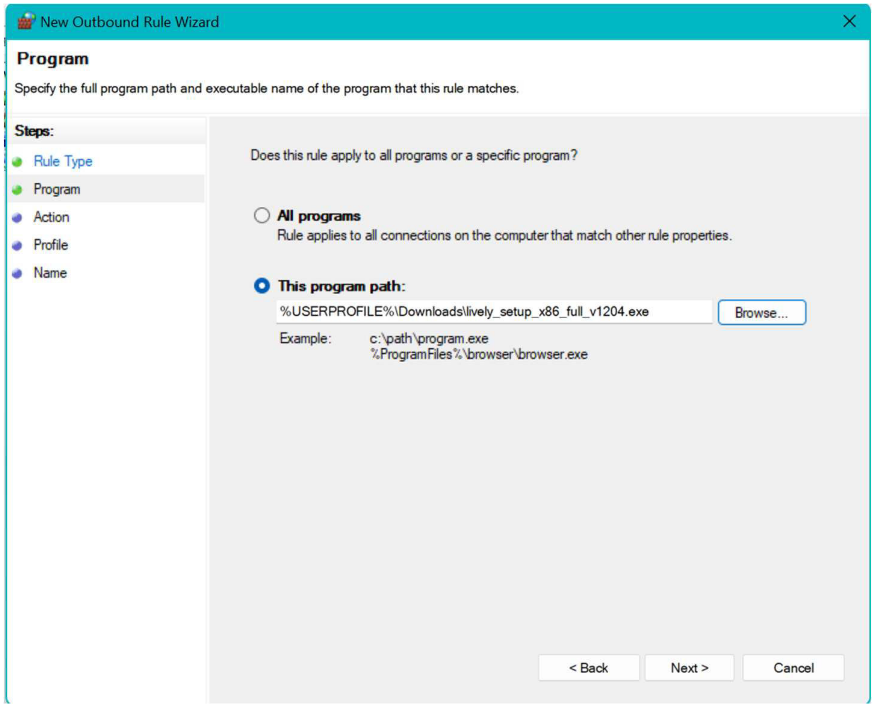
● **Program**
Rule that controls connections for a program.

○ **Port**
Rule that controls connections for a TCP or UDP port.

○ **Predefined:**
@%systemroot%\system32\provsvc.dll,-202
Rule that controls connections for a Windows experience.

○ **Custom**
Custom rule.

5.Go to programs then browse the files which you want to block.



New Outbound Rule Wizard

Program

Specify the full program path and executable name of the program that this rule matches.

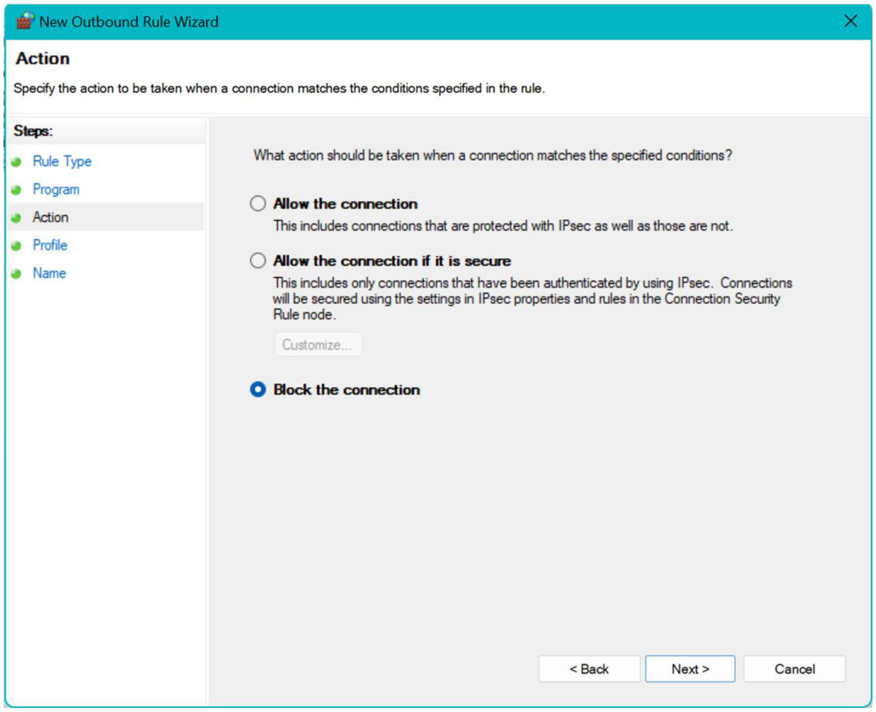
Does this rule apply to all programs or a specific program?

○ **All programs**
Rule applies to all connections on the computer that match other rule properties.

● **This program path:**
%USERPROFILE%\Downloads\lively_setup_x86_full_v1204.exe

Example: c:\path\program.exe
%ProgramFiles%\browser\browser.exe

6.Click on Next.



New Outbound Rule Wizard

Action

Specify the action to be taken when a connection matches the conditions specified in the rule.

Steps:
- Rule Type
- Program
- Action
- Profile
- Name

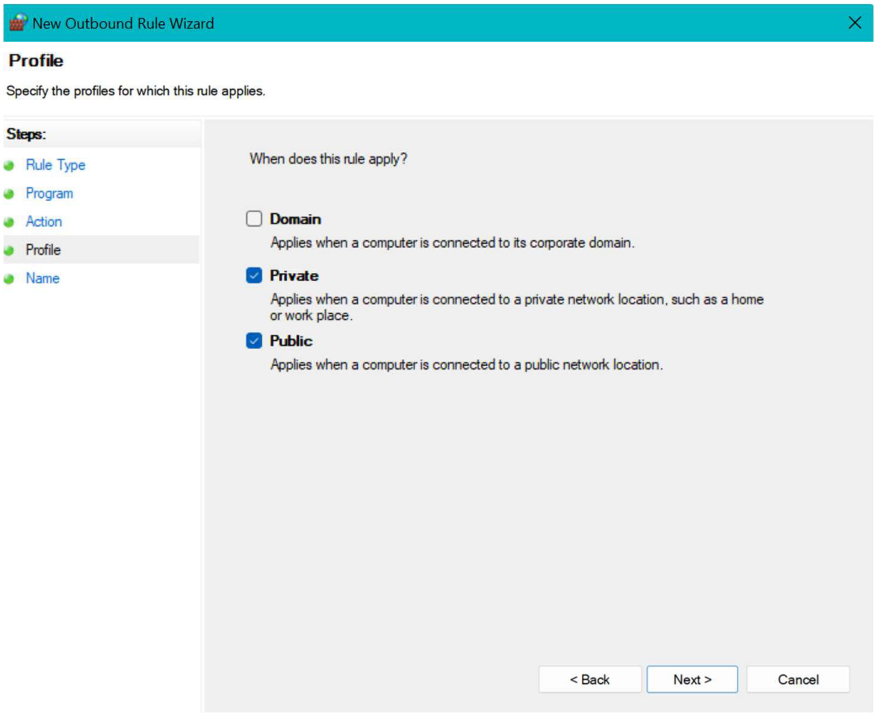
What action should be taken when a connection matches the specified conditions?

○ **Allow the connection**
This includes connections that are protected with IPsec as well as those are not.

○ **Allow the connection if it is secure**
This includes only connections that have been authenticated by using IPsec. Connections will be secured using the settings in IPsec properties and rules in the Connection Security Rule node.

● **Block the connection**

7.Click on Next.



New Outbound Rule Wizard

Profile

Specify the profiles for which this rule applies.

Steps:
- Rule Type
- Program
- Action
- Profile
- Name

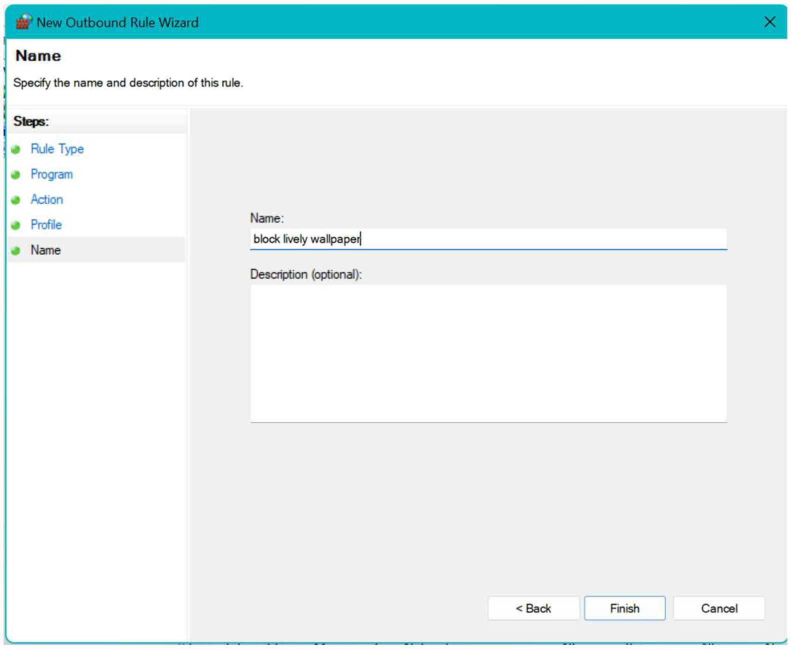
When does this rule apply?

□ **Domain**
Applies when a computer is connected to its corporate domain.

☑ **Private**
Applies when a computer is connected to a private network location, such as a home or work place.

☑ **Public**
Applies when a computer is connected to a public network location.

8.Click on Finish.



New Outbound Rule Wizard

Name

Specify the name and description of this rule.

Steps:
- Rule Type
- Program
- Action
- Profile
- Name

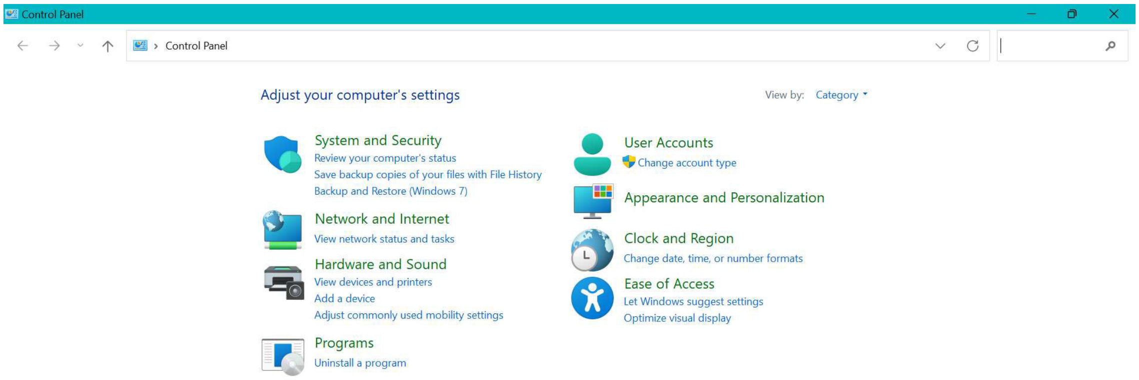
Name:
block lively wallpaper

Description (optional):

iii) A website

Steps:-

1.Open control panel.



Adjust your computer's settings

View by: Category

System and Security
Review your computer's status
Save backup copies of your files with File History
Backup and Restore (Windows 7)

Network and Internet
View network status and tasks

Hardware and Sound
View devices and printers
Add a device
Adjust commonly used mobility settings

Programs
Uninstall a program

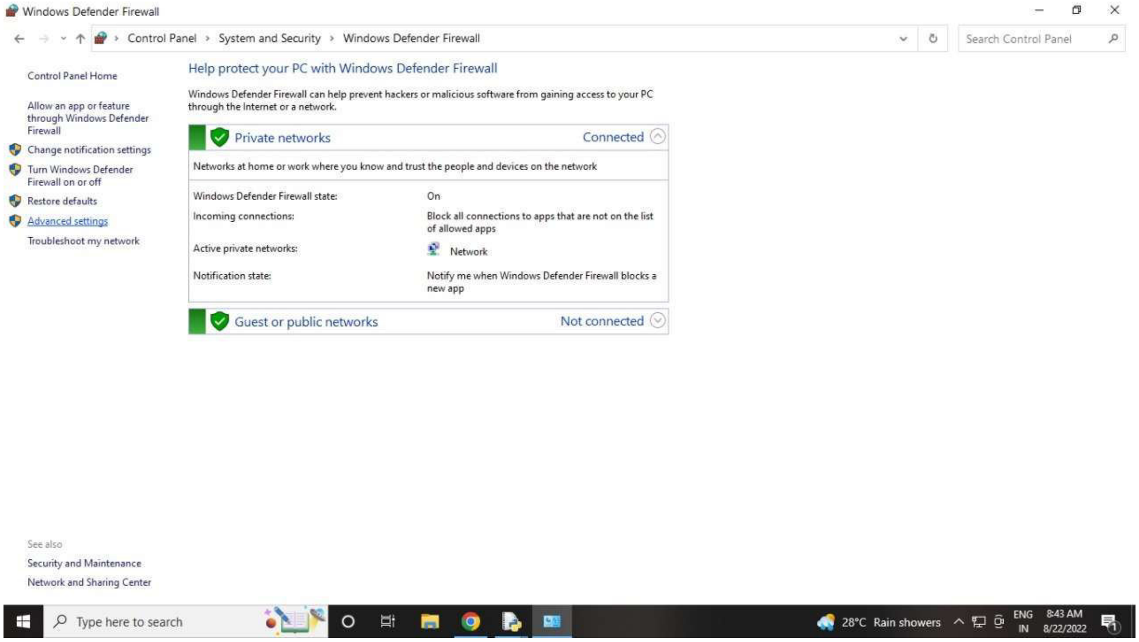
User Accounts
Change account type

Appearance and Personalization

Clock and Region
Change date, time, or number formats

Ease of Access
Let Windows suggest settings
Optimize visual display

2.Go to firewall in search box.



Windows Defender Firewall

Control Panel › System and Security › Windows Defender Firewall

Help protect your PC with Windows Defender Firewall

Windows Defender Firewall can help prevent hackers or malicious software from gaining access to your PC through the Internet or a network.

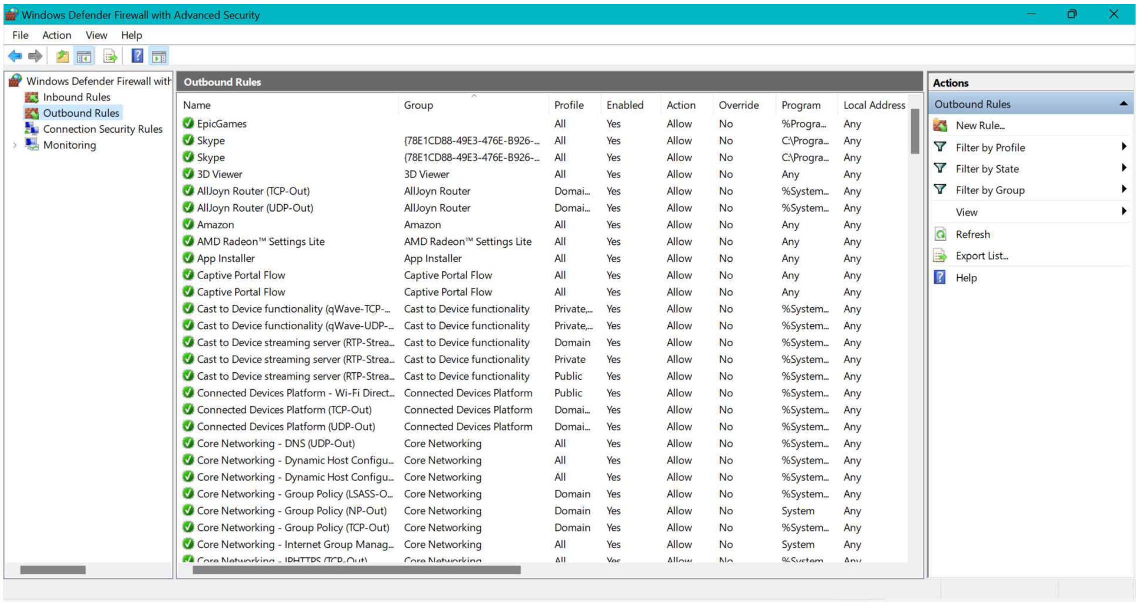
Private networks — Connected

Networks at home or work where you know and trust the people and devices on the network

Windows Defender Firewall state:	On
Incoming connections:	Block all connections to apps that are not on the list of allowed apps
Active private networks:	Network
Notification state:	Notify me when Windows Defender Firewall blocks a new app

Guest or public networks — Not connected

3.In the windows firewall, Click on advanced setting and then click on Outbound Rule.

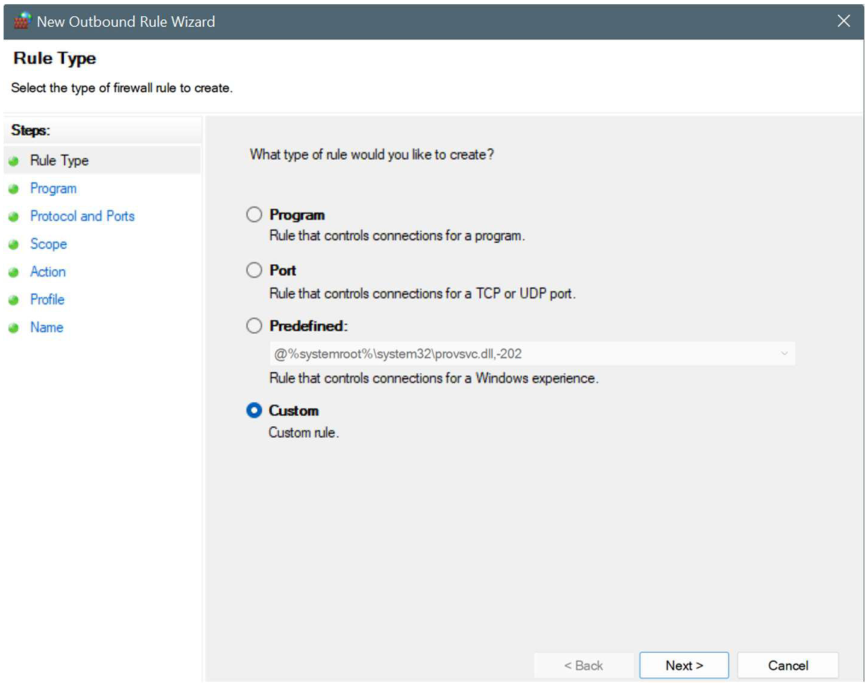


Windows Defender Firewall with Advanced Security

Outbound Rules

Name	Group	Profile	Enabled	Action	Override	Program	Local Address
EpicGames		All	Yes	Allow	No	%Progra...	Any
Skype	{78E1CD88-49E3-476E-B926-...	All	Yes	Allow	No	C:\Progra...	Any
Skype	{78E1CD88-49E3-476E-B926-...	All	Yes	Allow	No	C:\Progra...	Any
3D Viewer	3D Viewer	All	Yes	Allow	No	Any	Any
AllJoyn Router (TCP-Out)	AllJoyn Router	Domai...	Yes	Allow	No	%System...	Any
AllJoyn Router (UDP-Out)	AllJoyn Router	Domai...	Yes	Allow	No	%System...	Any
Amazon	Amazon	All	Yes	Allow	No	Any	Any
AMD Radeon™ Settings Lite	AMD Radeon™ Settings Lite	All	Yes	Allow	No	Any	Any
App Installer	App Installer	All	Yes	Allow	No	Any	Any
Captive Portal Flow	Captive Portal Flow	All	Yes	Allow	No	Any	Any
Captive Portal Flow	Captive Portal Flow	All	Yes	Allow	No	Any	Any
Cast to Device functionality (qWave-TCP-...	Cast to Device functionality	Private,...	Yes	Allow	No	%System...	Any
Cast to Device functionality (qWave-UDP-...	Cast to Device functionality	Private,...	Yes	Allow	No	%System...	Any
Cast to Device streaming server (RTP-Strea...	Cast to Device functionality	Domain	Yes	Allow	No	%System...	Any
Cast to Device streaming server (RTP-Strea...	Cast to Device functionality	Private	Yes	Allow	No	%System...	Any
Cast to Device streaming server (RTP-Strea...	Cast to Device functionality	Public	Yes	Allow	No	%System...	Any
Connected Devices Platform - Wi-Fi Direct...	Connected Devices Platform	Public	Yes	Allow	No	%System...	Any
Connected Devices Platform (TCP-Out)	Connected Devices Platform	Domai...	Yes	Allow	No	%System...	Any
Connected Devices Platform (UDP-Out)	Connected Devices Platform	Domai...	Yes	Allow	No	%System...	Any
Core Networking - DNS (UDP-Out)	Core Networking	All	Yes	Allow	No	%System...	Any
Core Networking - Dynamic Host Configu...	Core Networking	All	Yes	Allow	No	%System...	Any
Core Networking - Dynamic Host Configu...	Core Networking	All	Yes	Allow	No	%System...	Any
Core Networking - Group Policy (LSASS-O...	Core Networking	Domain	Yes	Allow	No	%System...	Any
Core Networking - Group Policy (NP-Out)	Core Networking	Domain	Yes	Allow	No	System	Any
Core Networking - Group Policy (TCP-Out)	Core Networking	Domain	Yes	Allow	No	%System...	Any
Core Networking - Internet Group Manag...	Core Networking	All	Yes	Allow	No	System	Any
Core Networking - IPHTTPS (TCP-Out)	Core Networking	All	Yes	Allow	No	%System	Any

4.Go to new Rule in RHS.


New Outbound Rule Wizard

Rule Type

Select the type of firewall rule to create.

Steps:
- Rule Type
- Program
- Protocol and Ports
- Scope
- Action
- Profile
- Name

What type of rule would you like to create?

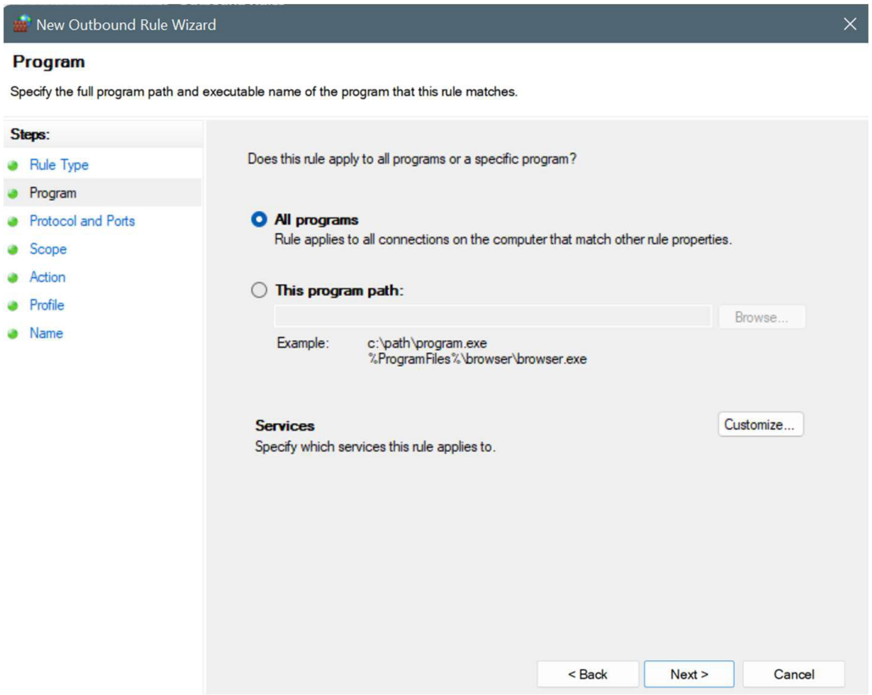
○ **Program**
Rule that controls connections for a program.

○ **Port**
Rule that controls connections for a TCP or UDP port.

○ **Predefined:**
@%systemroot%\system32\provsvc.dll,-202
Rule that controls connections for a Windows experience.

● **Custom**
Custom rule.

5.Go to All Programs.


New Outbound Rule Wizard

Program

Specify the full program path and executable name of the program that this rule matches.

Steps:
- Rule Type
- Program
- Protocol and Ports
- Scope
- Action
- Profile
- Name

Does this rule apply to all programs or a specific program?

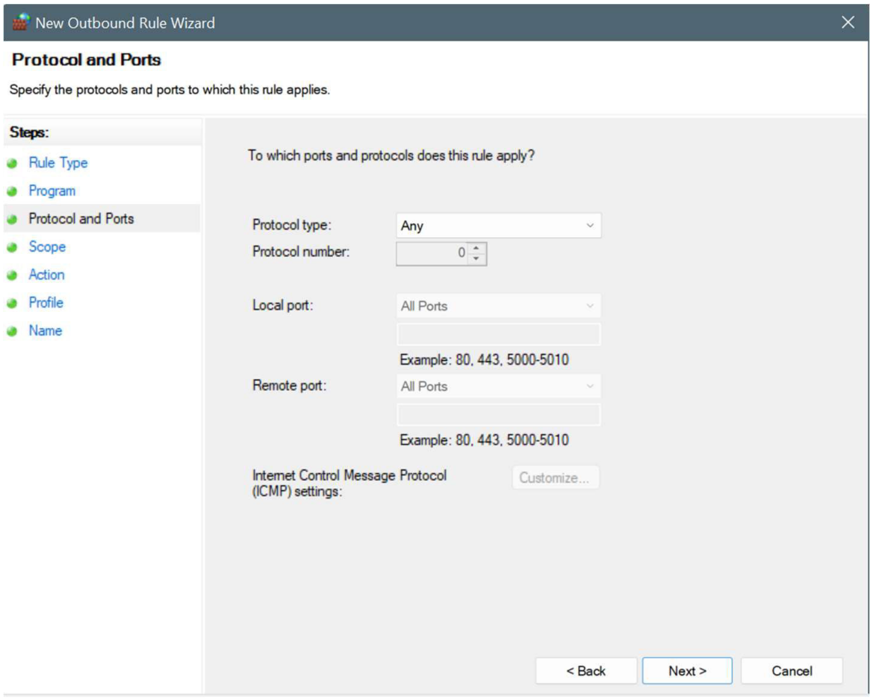
● **All programs**
Rule applies to all connections on the computer that match other rule properties.

○ **This program path:**

Example: c:\path\program.exe
%ProgramFiles%\browser\browser.exe

Services
Specify which services this rule applies to.

6.Select Any and enter IP address.



New Outbound Rule Wizard

Protocol and Ports

Specify the protocols and ports to which this rule applies.

To which ports and protocols does this rule apply?

Protocol type: Any

Protocol number: 0

Local port: All Ports

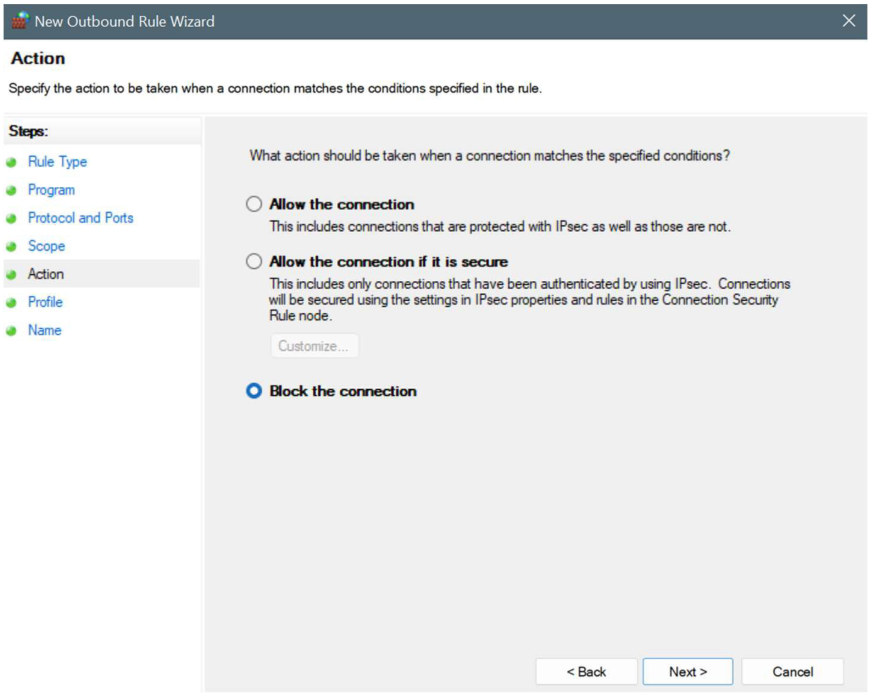
Example: 80, 443, 5000-5010

Remote port: All Ports

Example: 80, 443, 5000-5010

Internet Control Message Protocol (ICMP) settings:

7.Click on Next.



New Outbound Rule Wizard

Action

Specify the action to be taken when a connection matches the conditions specified in the rule.

What action should be taken when a connection matches the specified conditions?

○ **Allow the connection**

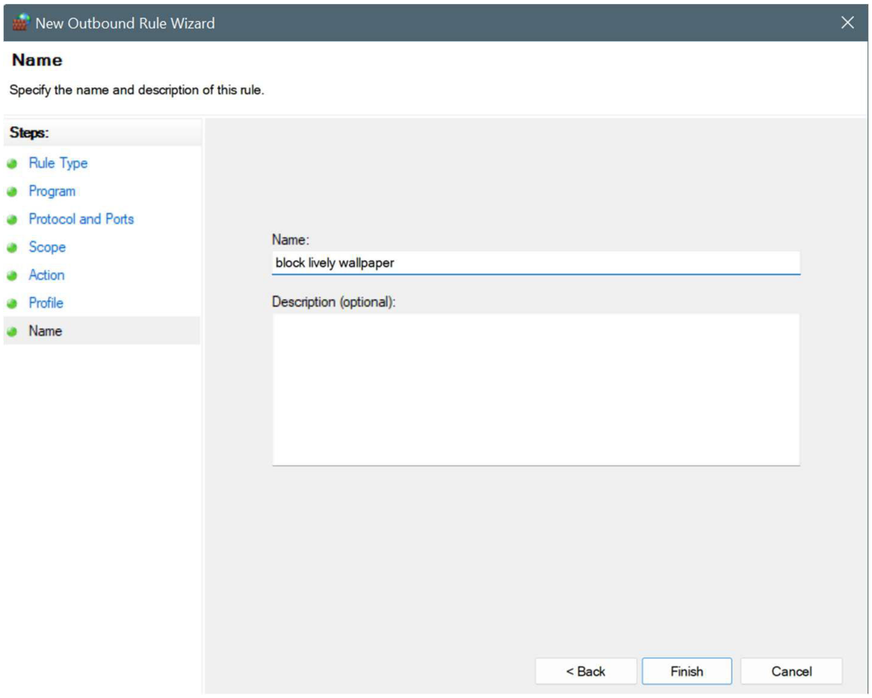
This includes connections that are protected with IPsec as well as those are not.

○ **Allow the connection if it is secure**

This includes only connections that have been authenticated by using IPsec. Connections will be secured using the settings in IPsec properties and rules in the Connection Security Rule node.

● **Block the connection**

8.Click on Finish.



Name

Specify the name and description of this rule.

Name: block lively wallpaper

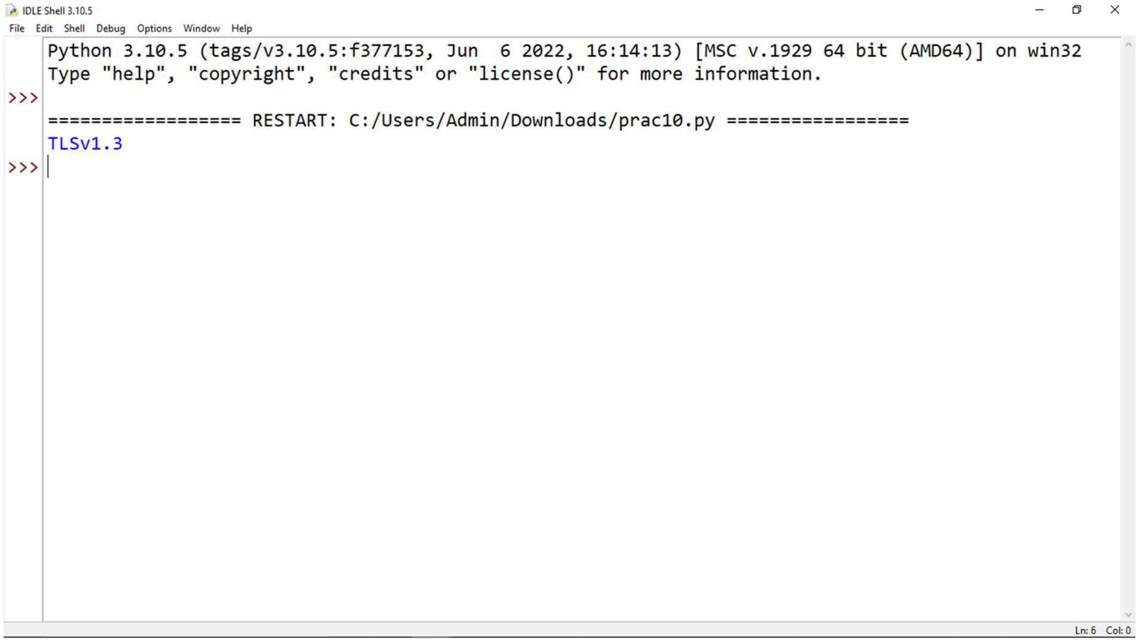
Description (optional):

Practical no: 10(ssl)

Aim:- Write a program to implement ssl.

```
import socket

import ssl

hostname='www.python.org'

context=ssl.create_default_context()


with socket.create_connection((hostname,443))as sock:

   with context.wrap_socket(sock,server_hostname=hostname)as s_sock:

      print(s_sock.version())
```

Output:-



```
Python 3.10.5 (tags/v3.10.5:f377153, Jun  6 2022, 16:14:13) [MSC v.1929 64 bit (AMD64)] on win32
Type "help", "copyright", "credits" or "license()" for more information.
>>>
    ================== RESTART: C:/Users/Admin/Downloads/prac10.py =================
    TLSv1.3
>>>
```