ISS - Digital Assignment 2

Name : S Kailash
Reg. no: 18MIS1074

Program to encrypt and decrypt the sentence - kailash18mis107 wants 10 marks in assignment using elliptic curve cryptography.

CODE:

```
import random
#this is the code to demonstrate elliptic curve cryptography.
plaintext = input("Enter plaintext\n")
if(len(plaintext)%2!=0):
        plaintext=plaintext+' '
#the ord() function is used to convert to ASCII
numbers = [ord(letter) for letter in plaintext]
pairs=[plaintext[i:i+2] for i in range (0,len(plaintext),2)]
print("Letter pairs:")
print(pairs)
arr = list()
for i in range(0,len(numbers)-1,2):
    arr.insert(i,[numbers[i],numbers[i+1]])
print("ASCII value pairs")
print(arr)
pair = list()
for i in range (0,len(arr)):
        pair.insert(i,int(str(arr[i][0])+str(arr[i][1])))
print("Concatenated Values")
print(pair)

#some diffie-hellman stuff

print("Enter the value of n")
n=int(input())
#the curve is a weierstrass equation, of the form y^2=x^3+ax+b, where a,b
are curve parameters
print("Enter the curve parameter a")
a=int(input())
print("Enter the curve parameter b")
b=int(input())
#now, lets parse the polynomial using 2 2d lists - lhs and rhs for left
hand side and right hand side of the equation
lhs=[[]]
rhs=[[]]
lhs.append([])
rhs.append([])
```

```
for i in range(0,n):
    lhs[0].append(i)
    rhs[0].append(i)
    lhs[1].append((i**3+a*i+b)%n)
    rhs[1].append((i**2)%n)
x=[]
y=[]
count=0
for i in range (0,n):
        for j in range (0,n):
                if(lhs[1][i]==rhs[1][j]):
                        count+=1
                        x.append(lhs[0][i])
                        y.append(rhs[0][j])
#print nG values
for i in range(0,count):
        print(i+1,"(",x[i],",",y[i],")")
bx=x[0]
by=y[0]
print("Initial point is :",bx,",",by)
#now, lets generate a random integer 'd',the private key of sender
d=random.randint(0,n)
qx=d*bx
qy=b*by
print("Public key of sender : ",qx,",",qy)
#generate another random integer 'k'
k=random.randint(0,n)
c1xarr=list()
c1yarr=list()
c2xarr=list()
c2yarr=list()
#encryption process
final_ans=list()
for i in pair:
        c1x=k*bx
        c1y=k*by
        print("Value of ciphertext 1 is ",c1x,",",c1y)
        c1xarr.append(c1x)
        c1yarr.append(c1y)
        c2x=k*qx+i
        c2y=k*qy+i
        print("Value of ciphertext2 is ",c2x,",",c2y)
        c2xarr.append(c2x)
        c2yarr.append(c2y)
        mx=c2x-i*c1x
        my=c2y-i*c2x
        print("Decrypted sentence is : ",mx)
```

```
        final_ans.append(mx)

print(final_ans)

#now, convert the ascii back to human-readable letters
string = ''.join(map(str,final_ans))
char_num = 0
op = list()
for i in range(len(string)):
        char_num=char_num*10 + (ord(string[i])-ord('0'))
        if(char_num>=32 and char_num <=122):
                ch = chr(char_num)
                op.append(ch)
                char_num=0
print("Letter character stream : ")
print(op)
print("Decrypted sentence : ")
opstring = ''.join(map(str,op))
print(opstring)
```

OUTPUT:

```
kailash@18mis1074:~/Documents/Winter Semester 2020-'21/ISS/Digital Assignments$ python3 trial2.py
Enter plaintext
kailash18mis107 wants 10 marks in assignment
Letter pairs:
['ka', 'il', 'as', 'h1', '8m', 'is', '10', '7 ', 'wa', 'nt', 's ', '10', ' m', 'ar', 'ks', ' i', 'n ', 'as', 'si', 'gn', 'me', 'nt']
ASCII value pairs
[[107, 97], [105, 108], [97, 115], [104, 49], [56, 109], [105, 115], [49, 48], [55, 32], [119, 97], [110, 116], [115, 32], [49, 48], [32, 109], [97, 1
14], [107, 115], [32, 105], [110, 32], [97, 115], [115, 105], [103, 110], [109, 101], [110, 116]]
Concatenated Values
[10797, 105108, 97115, 10449, 56109, 105115, 4948, 5532, 11997, 110116, 11532, 4948, 32109, 97114, 107115, 32105, 11032, 97115, 115105, 103110, 109101
, 110116]
Enter the value of n
7
Enter the curve parameter a
4
Enter the curve parameter b
2
1 ( 0 , 3 )
2 ( 0 , 4 )
3 ( 1 , 0 )
4 ( 2 , 2 )
5 ( 2 , 5 )
6 ( 5 , 0 )
7 ( 6 , 2 )
8 ( 6 , 5 )
```

```
Initial point is : 0 , 3
Public key of sender :  0 , 6
Value of ciphertext 1 is  0 , 12
Value of ciphertext2 is  10797 , 10821
Decrypted sentence is :  10797
Value of ciphertext 1 is  0 , 12
Value of ciphertext2 is  105108 , 105132
Decrypted sentence is :  105108
Value of ciphertext 1 is  0 , 12
Value of ciphertext2 is  97115 , 97139
Decrypted sentence is :  97115
Value of ciphertext 1 is  0 , 12
Value of ciphertext2 is  10449 , 10473
Decrypted sentence is :  10449
Value of ciphertext 1 is  0 , 12
Value of ciphertext2 is  56109 , 56133
Decrypted sentence is :  56109
Value of ciphertext 1 is  0 , 12
Value of ciphertext2 is  105115 , 105139
Decrypted sentence is :  105115
Value of ciphertext 1 is  0 , 12
Value of ciphertext2 is  4948 , 4972
Decrypted sentence is :  4948
Value of ciphertext 1 is  0 , 12
Value of ciphertext2 is  5532 , 5556
Decrypted sentence is :  5532
Value of ciphertext 1 is  0 , 12
Value of ciphertext2 is  11997 , 12021
Decrypted sentence is :  11997
Value of ciphertext 1 is  0 , 12
Value of ciphertext2 is  110116 , 110140
Decrypted sentence is :  110116
```

```
Value of ciphertext 1 is  0 , 12
Value of ciphertext2 is  11532 , 11556
Decrypted sentence is :  11532
Value of ciphertext 1 is  0 , 12
Value of ciphertext2 is  4948 , 4972
Decrypted sentence is :  4948
Value of ciphertext 1 is  0 , 12
Value of ciphertext2 is  32109 , 32133
Decrypted sentence is :  32109
Value of ciphertext 1 is  0 , 12
Value of ciphertext2 is  97114 , 97138
Decrypted sentence is :  97114
Value of ciphertext 1 is  0 , 12
Value of ciphertext2 is  107115 , 107139
Decrypted sentence is :  107115
Value of ciphertext 1 is  0 , 12
Value of ciphertext2 is  32105 , 32129
Decrypted sentence is :  32105
Value of ciphertext 1 is  0 , 12
Value of ciphertext2 is  11032 , 11056
Decrypted sentence is :  11032
Value of ciphertext 1 is  0 , 12
Value of ciphertext2 is  97115 , 97139
Decrypted sentence is :  97115
Value of ciphertext 1 is  0 , 12
Value of ciphertext2 is  115105 , 115129
Decrypted sentence is :  115105
Value of ciphertext 1 is  0 , 12
Value of ciphertext2 is  103110 , 103134
Decrypted sentence is :  103110
Value of ciphertext 1 is  0 , 12
```

```
Value of ciphertext 1 is  0 , 12
Value of ciphertext2 is  109101 , 109125
Decrypted sentence is :  109101
Value of ciphertext 1 is  0 , 12
Value of ciphertext2 is  110116 , 110140
Decrypted sentence is :  110116
[10797, 105108, 97115, 10449, 56109, 105115, 4948, 5532, 11997, 110116, 11532, 4948, 32109, 97114, 107115, 32105, 11032, 97115, 115105, 103110, 109101
, 110116]
Letter character stream :
['k', 'a', 'i', 'l', 'a', 's', 'h', '1', '8', 'm', 'i', 's', '1', '0', '7', ' ', 'w', 'a', 'n', 't', 's', ' ', '1', '0', ' ', 'm', 'a', 'r', 'k', 's',
 ' ', 'i', 'n', ' ', 'a', 's', 's', 'i', 'g', 'n', 'm', 'e', 'n', 't']
Decrypted sentence :
kailash18mis107 wants 10 marks in assignment
kailash@18mis1074:~/Documents/Winter Semester 2020-'21/ISS/Digital Assignments$
```