VIT®

Vellore Institute of Technology

(Deemed to be University under section 3 of UGC Act, 1956)

Aditi Patra

21BIT0125

Lab 1

Intelligent Cryptography

L55+56

CODE:

```
import random


# Sender side

n = int(input("Enter a number to encrypt: "))

M = bin(n)

n1 = random.randint(1,n)

print("The random number is",n1)

R=bin(n1)

print("The random number in binary form is",R)

if n1 >= n:
```

```
    print("Since the second number is greater than or equal to the to be encrypt value, we cannot continue")
else:
    #Data split
    ds = n - n1
    print("The value after data split",ds)
    S = bin(ds)
    print("The value of binary data split value",S)
    K = random.randint(2**2048, 2**4096) #key should be in 2k bits
    print("The random key is",K)
    CT1 = n1^K #XOR gate
    #Encryption
    CT2 = ds^K #XOR gate
    print("The value of cloud A",CT1)
    print("The value of cloud B",CT2)
    print("The binary value of cloud A is", bin(CT1))
    print("The binary value of cloud B is", bin(CT2))

    # Storing them in seperate files!
    with open("cloudA.txt", "w") as file:
        file.write(str(CT1))
    with open("cloudB.txt", "w") as file:
        file.write(str(CT2))
    with open("key.txt", "w") as file:
        file.write(str(K))
```

```
# Receiver side
with open("cloudA.txt", "r") as file:
    CT1 = int(file.read())
with open("cloudB.txt", "r") as file:
    CT2 = int(file.read())
with open("key.txt", "r") as file:
    K = int(file.read())

CA1 =CT1 ^ K #XOR gate
print("The value of new cloud A",CA1)
#Decryption
CA2 =CT2 ^ K #XOR gate
print("The value of new cloud B",CA2)
#Data merge
M1 = CA1 + CA2
F = bin(M1)
print("The decrypted value is", M1)
print("The binary form of decrypted value is",F)

# To cross check
if M1 == n:
    print("The process is correct")
else:
    print("The process is wrong")
```

cryptofinal.py - C:/Users/patra/Desktop/books/5th sem/infosec/cryptofinal.py (3.9.6)

File Edit Format Run Options Window Help

```
import random

# Sender side
n = int(input("Enter a number to encrypt: "))
M = bin(n)
n1 = random.randint(1,n)
print("The random number is",n1)
R=bin(n1)
print("The random number in binary form is",R)
if n1 >= n:
    print("Since the second number is greater than or equal to the to be encrypt value, we cannot continue")
else:
    #Data split
    ds = n - n1
    print("The value after data split",ds)
    S = bin(ds)
    print("The value of binary data split value",S)
    K = random.randint(2**2048, 2**4096) #key should be in 2k bits
    print("The random key is",K)
    CT1 = n1^K #XOR gate
    #Encryption
    CT2 = ds^K #XOR gate
    print("The value of cloud A",CT1)
    print("The value of cloud B",CT2)
    print("The binary value of cloud A is", bin(CT1))
    print("The binary value of cloud B is", bin(CT2))

    # Storing them in seperate files!
    with open("cloudA.txt", "w") as file:
        file.write(str(CT1))
    with open("cloudB.txt", "w") as file:
        file.write(str(CT2))
    with open("key.txt", "w") as file:
        file.write(str(K))

# Receiver side
with open("cloudA.txt", "r") as file:
    CT1 = int(file.read())
with open("cloudB.txt", "r") as file:
    CT2 = int(file.read())
with open("key.txt", "r") as file:
    K = int(file.read())
```

```
CA1 =CT1 ^ K #XOR gate
print("The value of new cloud A",CA1)
#Decryption
CA2 =CT2 ^ K #XOR gate
print("The value of new cloud B",CA2)
#Data merge
M1 = CA1 + CA2
F = bin(M1)
print("The decrypted value is", M1)
print("The binary form of decrypted value is",F)

# To cross check
if M1 == n:
    print("The process is correct")
else:
    print("The process is wrong")
```

Ln: 34 Col: 26

Key:

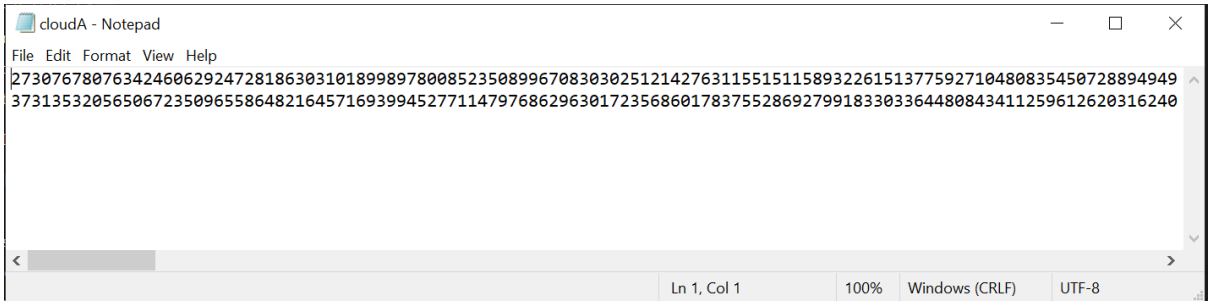
key - Notepad

File Edit Format View Help

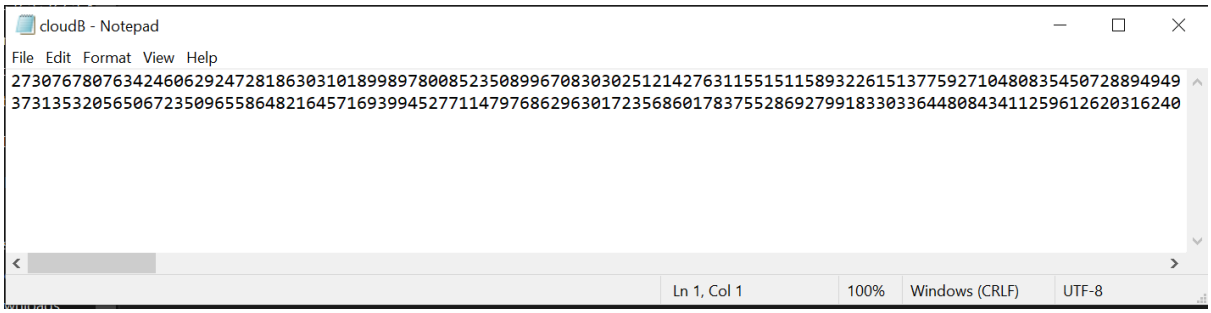
```
27307678076342460629247281863031018998978008523508996708303025121427631155151158932261513775927104808354507288949493731353205650672350965586482164571693994527711479768629630172356860178375528692799183303364480843411259612620316240
```

Ln 1, Col 1 | 100% | Windows (CRLF) | UTF-8

Cloud A:



Cloud B:



OUTPUT: