# Information technology lab - Model lab

**Question:**

# Write Aim and Algorithm for the following

Write a program to generate all the primes between 20 to 50. For each of the prime, generate all possible primitive roots

# OpenSSL:

1. Create a plaintext. txt file with the text " Thiagarajar College of Engineering" and your "reg No"
2. Encrypt using des in all block cipher modes of operation.
3. Display the contents of cipher.bin
4. Decrypt the contents of cipher.bin
5. Display the contents of pt.txt
6. Examine Avalanche effect by changing one bit/character in your plain text file

# Solution:

**Experiment – 1:**

for i in range(20,51): flag = 0

for j in range(2,i): if((i%j) == 0):

flag = 1 break

if(flag == 0):

print("Primitive roots of ",i," :- ") for x in range(2,i):

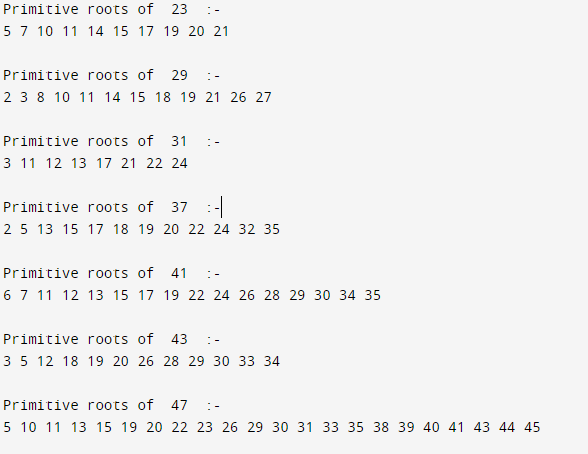
l = []

for y in range(1,i):

if((x\*\*y)%i not in l): l.append((x\*\*y)%i) else: break

if(len(l) == i-1): print(x,end=" ") print("\n")

# Output:



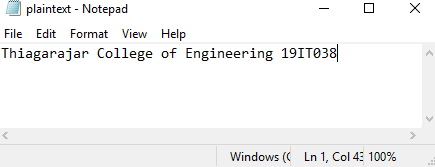
**Experiment – 2:**

Procedure:

* Navigate to openssl\x64\bin directory.



* Create a “plaintext.txt” file with the text “Thiagarajar College of Engineering” and “19IT038”.

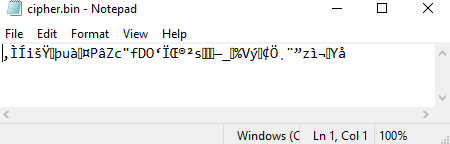


* Encryption of the file “plaintext.txt” is done using DES

*openssl des-cbc -e -in plaintext.txt -out cipher.bin -k "password" -nosalt*



* Displaying the contents of “cipher.bin” file.

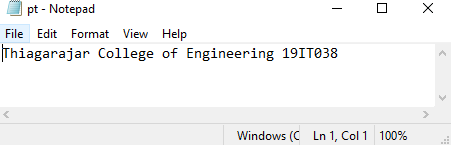


* Decryption of the file “cipher.bin” is done using DES

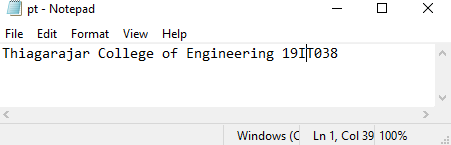
*openssl des-cbc -d -in cipher.bin -out pt.txt -k "password" –nosalt*



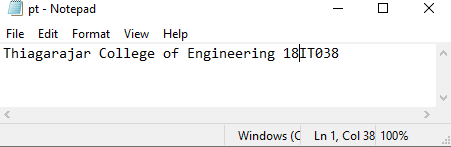
* Displaying the contents of “pt.txt”



* Examine Avalanche effect by changing one bit/character in your plain text file Original data:



Modified data:



openssl enc -des-cbc -in pt.txt -out cipher2.bin -k "password" -nosalt

