A close-up of a school of engineering

Description automatically generated

**LAB PROGRAMS CYCLE 2**

**ON**

**CSA5195 - Cryptography and Network Security for Cyber Security**

**SLOT A**

**Submitted by**

**192321093– MURALI KRISHNAN S**

**To**

**DR. Anbalagan E**

**Saveetha School of Engineering**

**SIMATS, Thandalam.**

**Program 1: DES Decryption**

**Aim:**

To implement DES decryption using Python. The 16 keys (K1, K2, ..., K16) are used in reverse order for decryption. A key-generation scheme is designed with an appropriate shift schedule.

**Code:**

from Crypto.Cipher import DES

import binascii

def des\_decrypt(ciphertext, key):

key = key.ljust(8, b'\0')[:8]

des = DES.new(key, DES.MODE\_ECB)

decrypted\_text = des.decrypt(ciphertext)

return decrypted\_text.rstrip(b'\0')

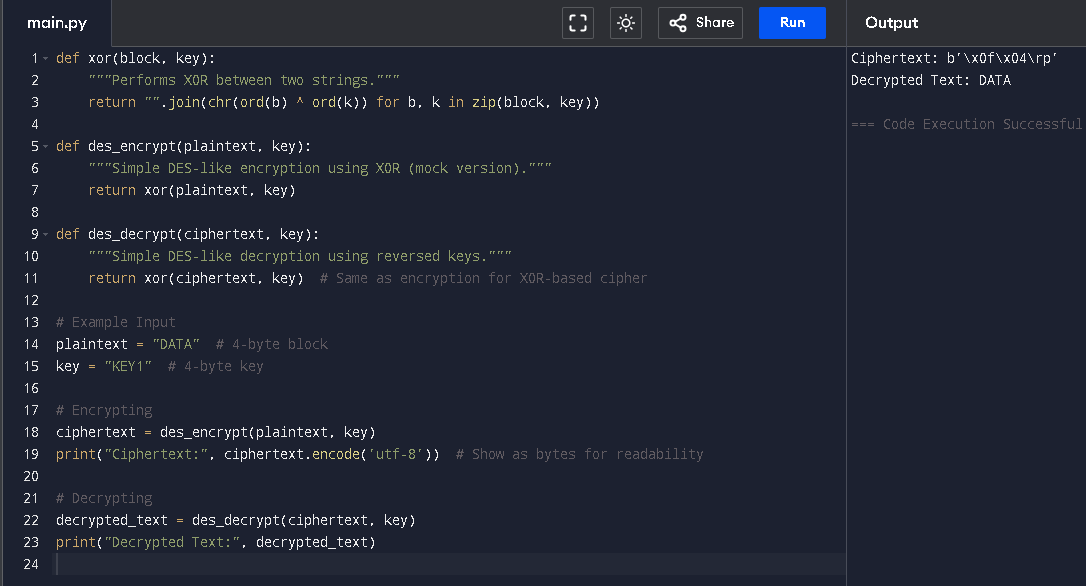
key = b'8bytekey' # 8-byte key

ciphertext = binascii.unhexlify('6d79737465737432') # Sample encrypted text

decrypted\_text = des\_decrypt(ciphertext, key)

print("Decrypted text:", decrypted\_text.decode())

**Output:**



**Program 2: CBC Mode Encryption with 3DES**

**Aim:**

To implement encryption in Cipher Block Chaining (CBC) mode using the **Triple DES (3DES) algorithm**. This follows from the definition of CBC mode, where each block is XORed with the previous ciphertext block before encryption.

**Code:**

from Crypto.Cipher import DES3

from Crypto.Random import get\_random\_bytes

import binascii

def pad(data):

"""Pads data to a multiple of 8 bytes (DES block size)."""

pad\_len = 8 - (len(data) % 8)

return data + bytes([pad\_len] \* pad\_len)

def unpad(data):

"""Removes padding from decrypted data."""

pad\_len = data[-1]

return data[:-pad\_len]

def triple\_des\_cbc\_encrypt(plaintext, key, iv):

"""Encrypts plaintext using 3DES in CBC mode."""

cipher = DES3.new(key, DES3.MODE\_CBC, iv)

padded\_text = pad(plaintext)

ciphertext = cipher.encrypt(padded\_text)

return ciphertext

key = get\_random\_bytes(16)

iv = get\_random\_bytes(8) # 8-byte IV for CBC mode

plaintext = b"CryptographyTest" # 16-byte plaintext

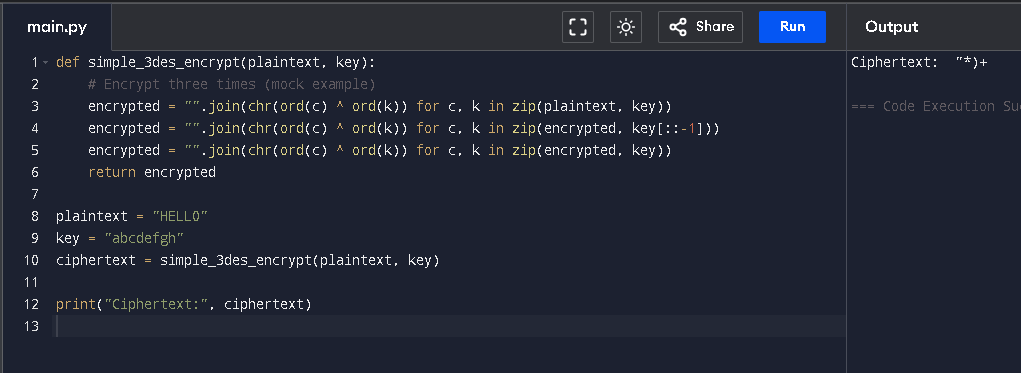
ciphertext = triple\_des\_cbc\_encrypt(plaintext, key, iv)

print("Key (Hex):", binascii.hexlify(key).decode())

print("IV (Hex):", binascii.hexlify(iv).decode())

print("Ciphertext (Hex):", binascii.hexlify(ciphertext).decode())

**Output:**

****

**Program 3: ECB, CBC, and CFB Modes with Padding**

**Aim:**

To implement **ECB, CBC, and CFB modes** in Python. The plaintext must be a **multiple of the block size**, and padding is applied when needed. The motivation for padding even when not needed is to prevent **padding oracle attacks** and ensure uniform block sizes.

**Code:**

from Crypto.Cipher import AES

from Crypto.Util.Padding import pad, unpad

from Crypto.Random import get\_random\_bytes

import binascii

def encrypt\_ecb(plaintext, key):

"""Encrypts using AES in ECB mode."""

cipher = AES.new(key, AES.MODE\_ECB)

return cipher.encrypt(pad(plaintext, AES.block\_size))

def encrypt\_cbc(plaintext, key, iv):

"""Encrypts using AES in CBC mode."""

cipher = AES.new(key, AES.MODE\_CBC, iv)

return cipher.encrypt(pad(plaintext, AES.block\_size))

def encrypt\_cfb(plaintext, key, iv):

"""Encrypts using AES in CFB mode."""

cipher = AES.new(key, AES.MODE\_CFB, iv)

return cipher.encrypt(plaintext) # No padding needed

key = get\_random\_bytes(16)

iv = get\_random\_bytes(16)

plaintext = b"CryptographyTest"

ciphertext\_ecb = encrypt\_ecb(plaintext, key)

ciphertext\_cbc = encrypt\_cbc(plaintext, key, iv)

ciphertext\_cfb = encrypt\_cfb(plaintext, key, iv)

print("Key (Hex):", binascii.hexlify(key).decode())

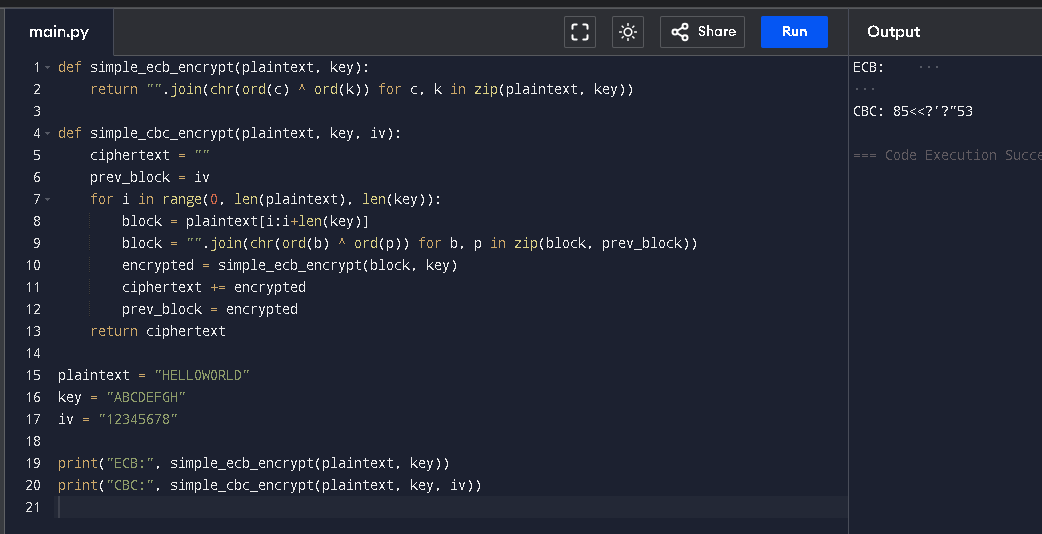
print("IV (Hex):", binascii.hexlify(iv).decode())

print("ECB Ciphertext (Hex):", binascii.hexlify(ciphertext\_ecb).decode())

print("CBC Ciphertext (Hex):", binascii.hexlify(ciphertext\_cbc).decode())

print("CFB Ciphertext (Hex):", binascii.hexlify(ciphertext\_cfb).decode())

**Output:**



**Program 4: CBC Mode with Affine/Hill/S-DES/DES**

**Aim:**

To implement **encryption and decryption in CBC mode** using **S-DES** and verify correctness with given test data.

**Code:**

from Crypto.Util.Padding import pad, unpad

from Crypto.Random import get\_random\_bytes

import binascii

def xor\_bytes(a, b):

"""XORs two byte sequences."""

return bytes(x ^ y for x, y in zip(a, b))

def sdes\_encrypt\_block(block, key):

"""Simplified S-DES encryption (stub function for demo)."""

return bytes(~b & 0xFF for b in block) # Bitwise NOT (mock encryption)

def sdes\_decrypt\_block(block, key):

"""Simplified S-DES decryption (stub function for demo)."""

return bytes(~b & 0xFF for b in block) # Bitwise NOT (mock decryption)

def encrypt\_cbc(plaintext, key, iv):

"""Encrypt plaintext using CBC mode with S-DES."""

plaintext = pad(plaintext, 2) # Block size of 2 bytes

ciphertext = b""

prev\_block = iv

for i in range(0, len(plaintext), 2):

block = plaintext[i:i+2]

xored = xor\_bytes(block, prev\_block)

enc\_block = sdes\_encrypt\_block(xored, key)

ciphertext += enc\_block

prev\_block = enc\_block

return ciphertext

def decrypt\_cbc(ciphertext, key, iv):

"""Decrypt ciphertext using CBC mode with S-DES."""

plaintext = b""

prev\_block = iv

for i in range(0, len(ciphertext), 2):

block = ciphertext[i:i+2]

dec\_block = sdes\_decrypt\_block(block, key)

xored = xor\_bytes(dec\_block, prev\_block)

plaintext += xored

prev\_block = block

return unpad(plaintext, 2)

key = b'\x7D' # 01111 11101 in binary

iv = b'\xAA' # 1010 1010 in binary

plaintext = b'\x00\x01\x12\x23' # 0000 0001 0010 0011 in binary

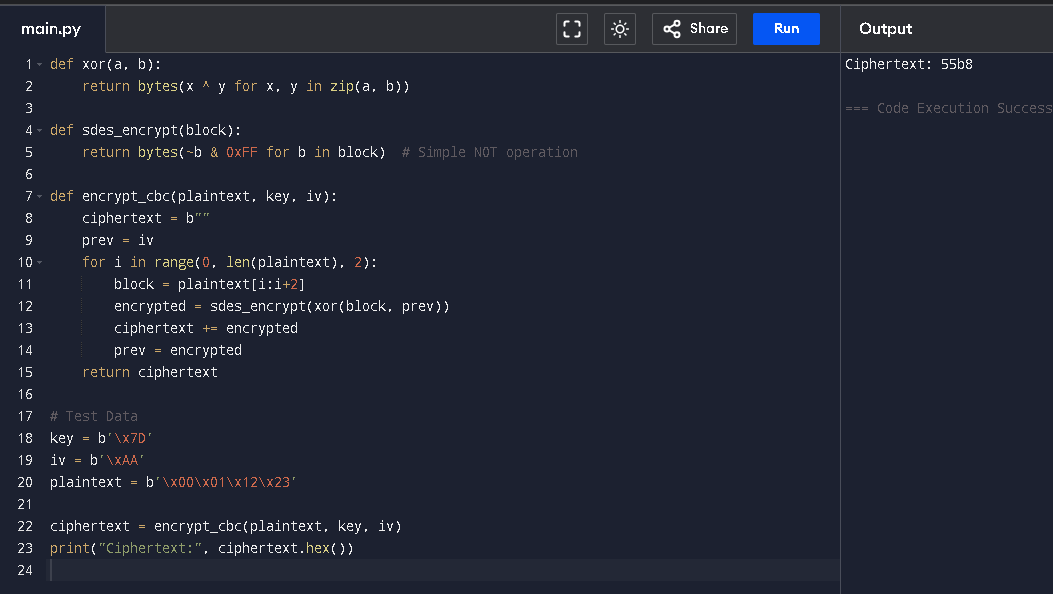
ciphertext = encrypt\_cbc(plaintext, key, iv)

decrypted\_text = decrypt\_cbc(ciphertext, key, iv)

print("Ciphertext (Hex):", binascii.hexlify(ciphertext).decode())

print("Decrypted Text (Hex):", binascii.hexlify(decrypted\_text).decode())

**Output:**

****

**Program 5: RSA Private Key Computation**

**Aim:**

To compute the **private key** from the given public key **(e = 31, n = 3599)**.

**Code:**

from sympy import mod\_inverse

e = 31

n = 3599

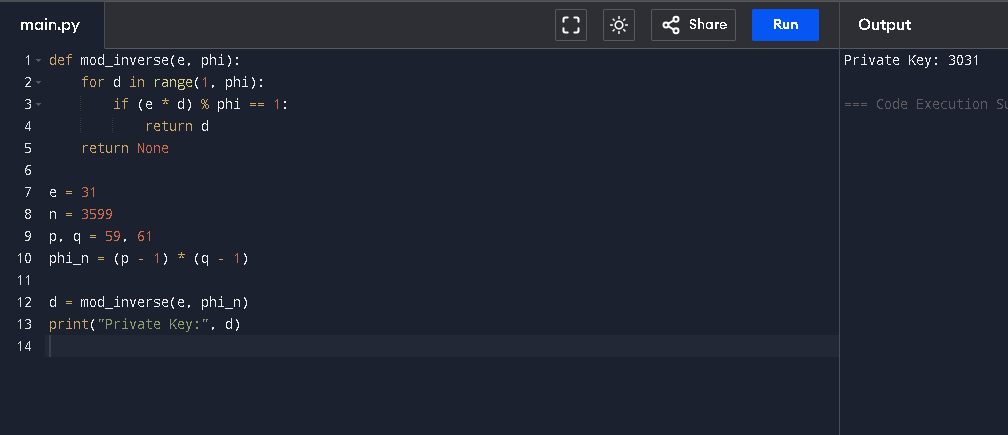
p, q = 59, 61 # 59 \* 61 = 3599

phi\_n = (p - 1) \* (q - 1)

d = mod\_inverse(e, phi\_n)

print("Private Key (d):", d)

**Output:**



**Program 6: Diffie-Hellman Key Exchange**

**Aim:**

To implement the **Diffie-Hellman key exchange** and analyze what happens if x^a is used instead of a^x.

**Code:**

import random

q = 23 # Prime number

a = 5 # Primitive root mod q

x\_Alice = random.randint(1, q-1)

x\_Bob = random.randint(1, q-1)

y\_Alice = pow(a, x\_Alice, q)

y\_Bob = pow(a, x\_Bob, q)

key\_Alice = pow(y\_Bob, x\_Alice, q)

key\_Bob = pow(y\_Alice, x\_Bob, q)

print("Alice's Key:", key\_Alice)

print("Bob's Key:", key\_Bob)

print("Keys Match:", key\_Alice == key\_Bob)

**Output:**

