**Name: Gaurang Vaghela**

**Rollno: TEAD-22561**

**Mini Project Lab**

**Practical 2  
Problem Statement:** Implementation of S-AES (Advanced Encryption Standard)

**Code:**

from Crypto.Cipher import AES

from Crypto.Random import get\_random\_bytes

from Crypto.Util.Padding import pad, unpad

# Key and data

key = get\_random\_bytes(16) # AES-128 => 16 bytes key

data = b"Secret Message!!" # Must be bytes

print("Original Message:", data)

# Encryption

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

ct\_bytes = cipher.encrypt(pad(data, AES.block\_size))

iv = cipher.iv # Initialization Vector

print(f"Encrypted: {ct\_bytes.hex()}")

# Decryption

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

pt = unpad(cipher\_dec.decrypt(ct\_bytes), AES.block\_size)

print(f"Decrypted: {pt.decode()}")

**Output:**

