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:

```
Original Message: b'Secret Message!!'
Encrypted: f50f8a1e076661db929d3f78c1527c20ee3bd8907072a1c68f5da135739a01e2
Decrypted: Secret Message!!
```