Name : Shivam Indrabhan Borse

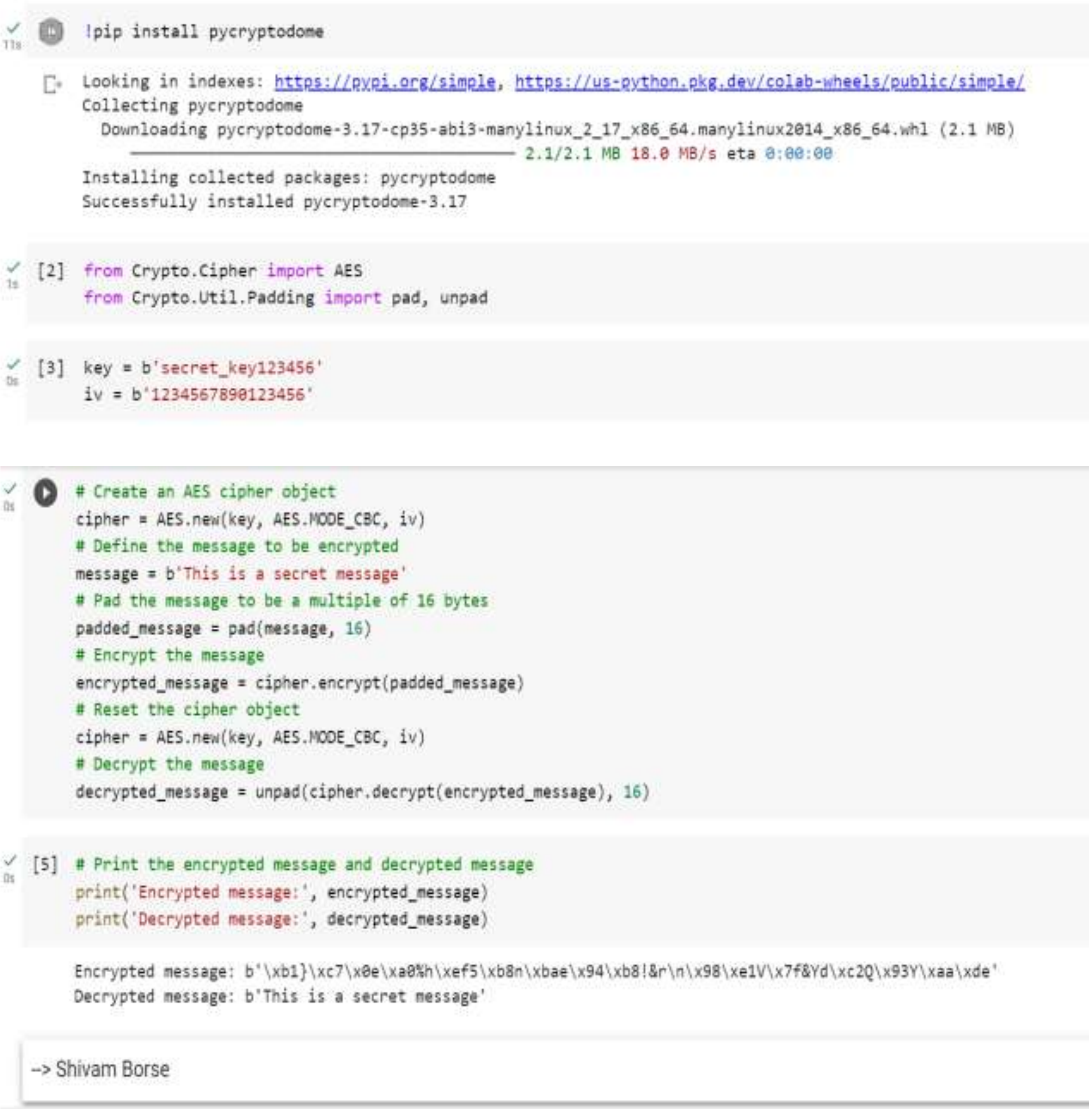
Roll No : 21119

Subject: Mini Project(Cyber Security) Laboratory

Assignment No : 02

Problem statement: Implementation of S-AES

CODE :



```
!pip install pycryptodome
```

```
Looking in indexes: https://pypi.org/simple, https://us-python.pkg.dev/colab-wheels/public/simple/
Collecting pycryptodome
  Downloading pycryptodome-3.17-cp35-abi3-manylinux_2_17_x86_64.manylinux2014_x86_64.whl (2.1 MB)
     ━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━ 2.1/2.1 MB 18.0 MB/s eta 0:00:00
Installing collected packages: pycryptodome
Successfully installed pycryptodome-3.17
```

```
[2] from Crypto.Cipher import AES
    from Crypto.Util.Padding import pad, unpad
```

```
[3] key = b'secret_key123456'
    iv = b'1234567890123456'
```

```
# Create an AES cipher object
cipher = AES.new(key, AES.MODE_CBC, iv)
# Define the message to be encrypted
message = b'This is a secret message'
# Pad the message to be a multiple of 16 bytes
padded_message = pad(message, 16)
# Encrypt the message
encrypted_message = cipher.encrypt(padded_message)
# Reset the cipher object
cipher = AES.new(key, AES.MODE_CBC, iv)
# Decrypt the message
decrypted_message = unpad(cipher.decrypt(encrypted_message), 16)
```

```
[5] # Print the encrypted message and decrypted message
    print('Encrypted message:', encrypted_message)
    print('Decrypted message:', decrypted_message)
```

```
Encrypted message: b'\xb1}\xc7\x0e\xa0%h\xef5\xb8n\xbae\x94\xb8!&r\n\x98\xe1V\x7f&Yd\xc2Q\x93Y\xaa\xde'
Decrypted message: b'This is a secret message'
```

--> Shivam Borse