Name : Shivam Indrabhan Borse

Roll No : 21119

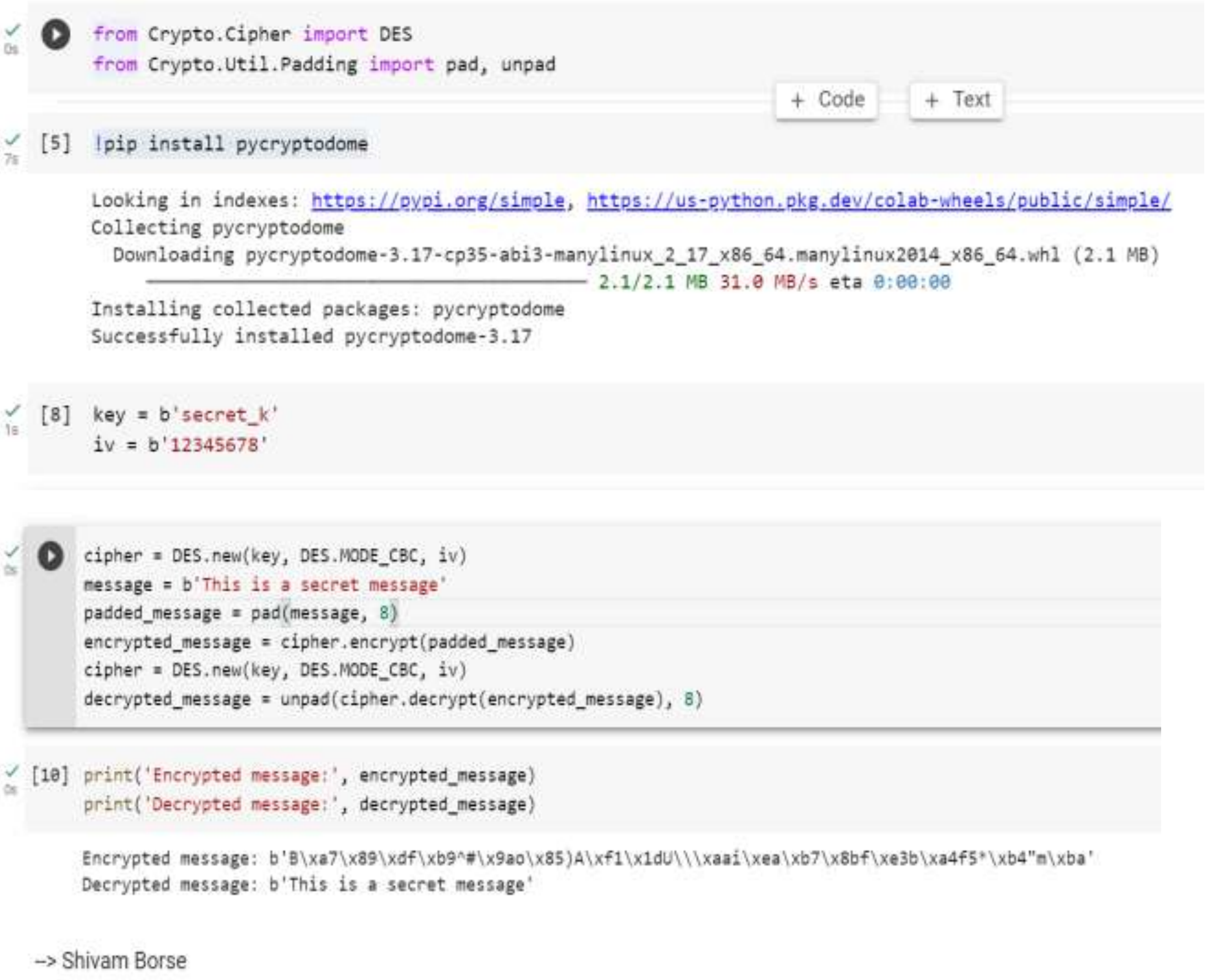
Subject: Mini Project(Cyber Security) Laboratory

Assignment No : 01

Problem statement:

Implementation of S-DES (Data Encryption Standard).

CODE :



```
from Crypto.Cipher import DES
from Crypto.Util.Padding import pad, unpad
```

```
[5] !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 31.0 MB/s eta 0:00:00
Installing collected packages: pycryptodome
Successfully installed pycryptodome-3.17
```

```
[8] key = b'secret_k'
    iv = b'12345678'
```

```
cipher = DES.new(key, DES.MODE_CBC, iv)
message = b'This is a secret message'
padded_message = pad(message, 8)
encrypted_message = cipher.encrypt(padded_message)
cipher = DES.new(key, DES.MODE_CBC, iv)
decrypted_message = unpad(cipher.decrypt(encrypted_message), 8)
```

```
[10] print('Encrypted message:', encrypted_message)
     print('Decrypted message:', decrypted_message)
```

```
Encrypted message: b'B\xa7\x89\xdf\xb9^#\x9ao\x85)A\xf1\x1dU\\\xaai\xea\xb7\x8bf\xe3b\xa4f5*\xb4"m\xba'
Decrypted message: b'This is a secret message'
```

--> Shivam Borse