INSTITUTE OF COMPUTER TECHNOLOGY

B-TECH COMPUTER SCIENCE ENGINEERING 2025-26

SUBJECT:-CRYPTOGRAPHY

NAME: Rahul Prajapati

ENRLL. NO: 23162171020

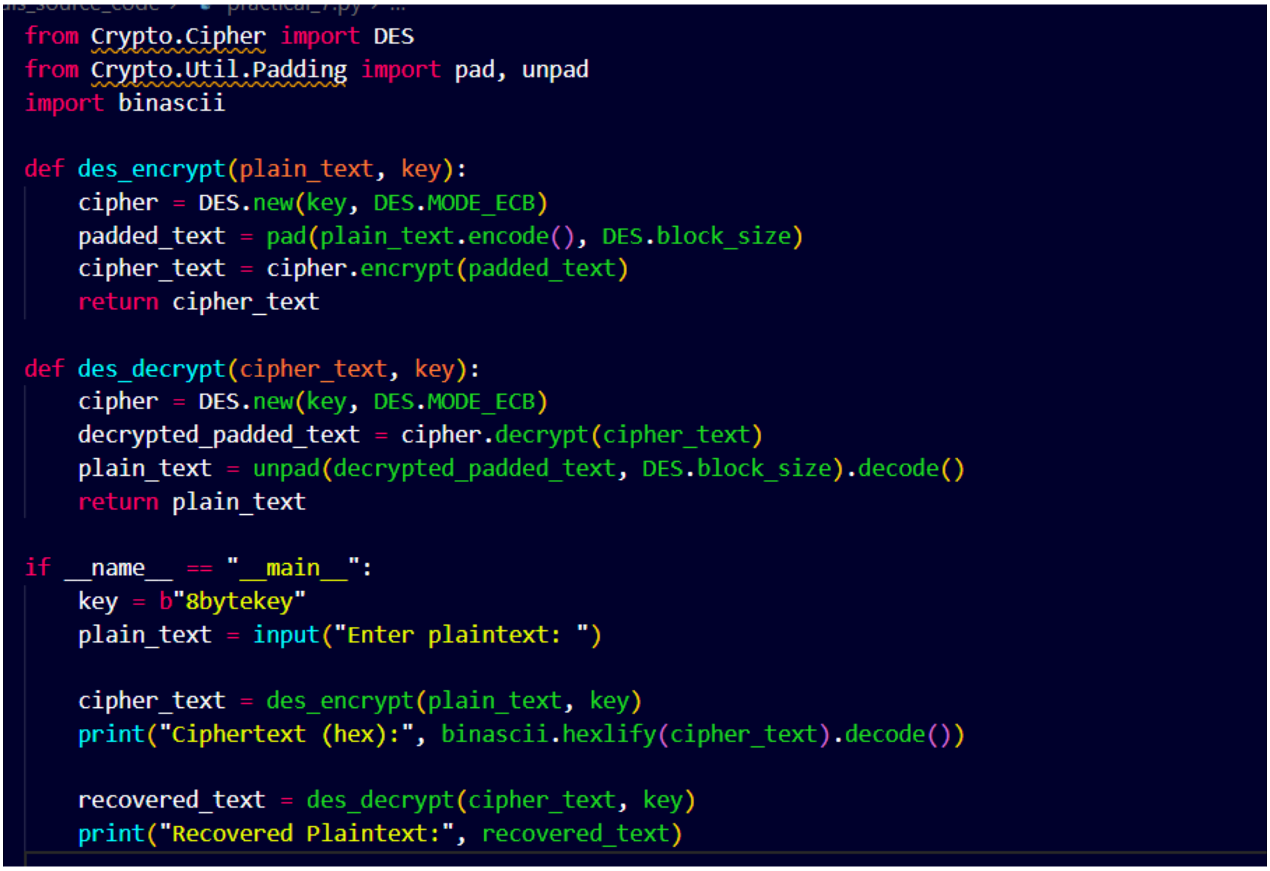
BRANCH: CYBER SECURITY

BATCH: 52

PRACTICAL_7

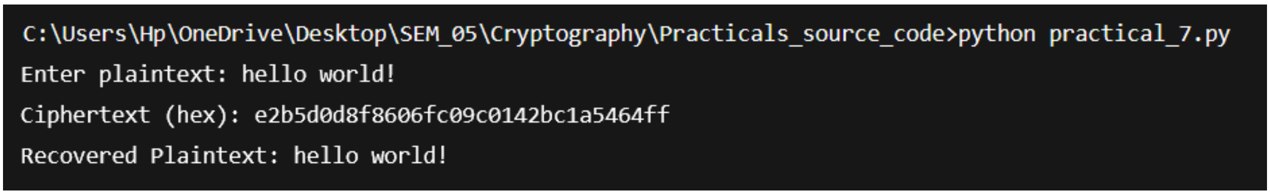
Aim: To implement the Data Encryption Standard (DES) using a fixed 8-byte key, without using modes of operation, to understand the fundamentals of block ciphers, block size restrictions, and direct encryption–decryption.

CODE:



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

def des_encrypt(plain_text, key):
    cipher = DES.new(key, DES.MODE_ECB)
    padded_text = pad(plain_text.encode(), DES.block_size)
    cipher_text = cipher.encrypt(padded_text)
    return cipher_text

def des_decrypt(cipher_text, key):
    cipher = DES.new(key, DES.MODE_ECB)
    decrypted_padded_text = cipher.decrypt(cipher_text)
    plain_text = unpad(decrypted_padded_text, DES.block_size).decode()
    return plain_text

if __name__ == "__main__":
    key = b"8bytekey"
    plain_text = input("Enter plaintext: ")

    cipher_text = des_encrypt(plain_text, key)
    print("Ciphertext (hex):", binascii.hexlify(cipher_text).decode())

    recovered_text = des_decrypt(cipher_text, key)
    print("Recovered Plaintext:", recovered_text)
```

OUTPUT:



```
C:\Users\Hp\OneDrive\Desktop\SEM_05\Cryptography\Practicals_source_code>python practical_7.py
Enter plaintext: hello world!
Ciphertext (hex): e2b5d0d8f8606fc09c0142bc1a5464ff
Recovered Plaintext: hello world!
```