INSTITUTE OF COMPUTER TECHNOLOGY

B-TECH COMPUTER SCIENCE ENGINEERING 2025-26

SUBJECT:-CRYPTOGRAPHY

NAME: Rahul Prajapati

ENRLL. NO: 23162171020

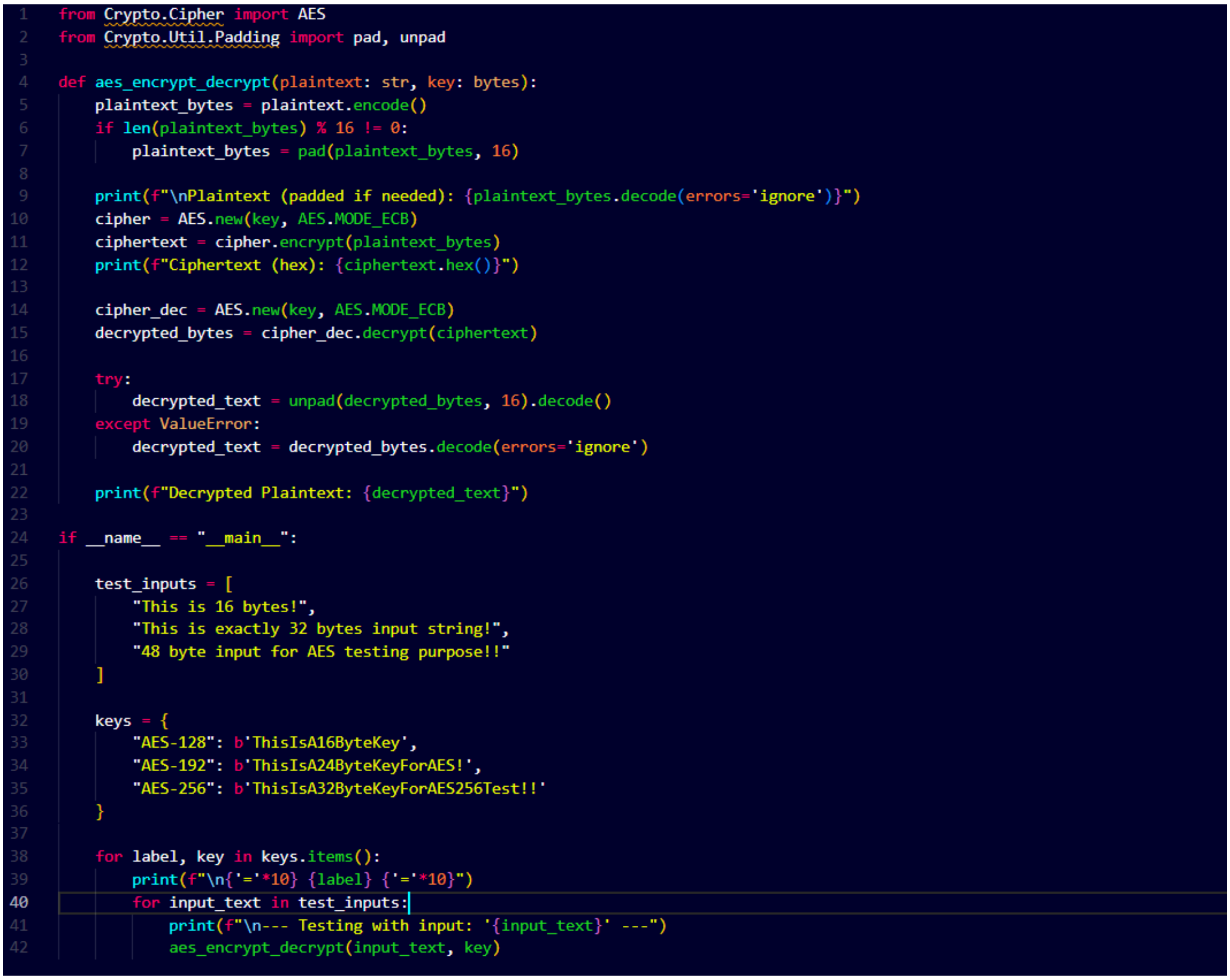
BRANCH: CYBER SECURITY

BATCH: 52

PRACTICAL_8

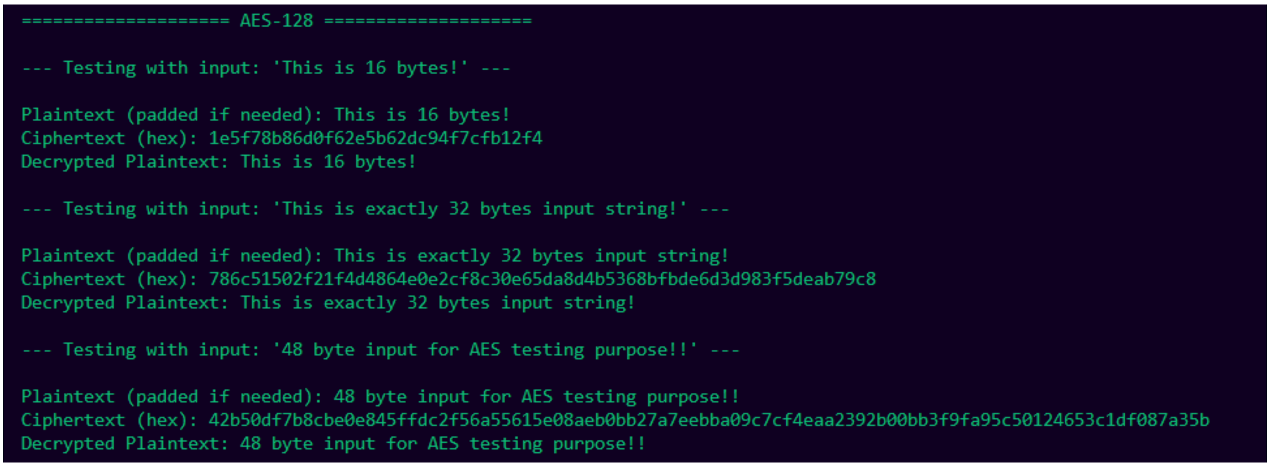
Aim: To implement the Advanced Encryption Standard (AES) using a fixed 16-byte key, without using modes of operation, to understand block sizes, key sizes, and direct encryption–decryption.

CODE:

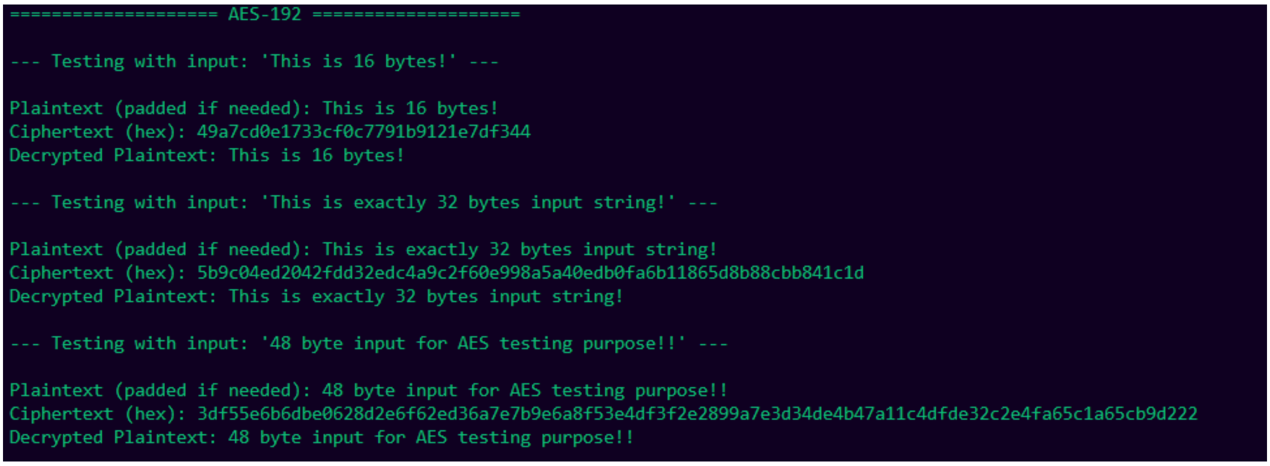


```python
from Crypto.Cipher import AES
from Crypto.Util.Padding import pad, unpad

def aes_encrypt_decrypt(plaintext: str, key: bytes):
    plaintext_bytes = plaintext.encode()
    if len(plaintext_bytes) % 16 != 0:
        plaintext_bytes = pad(plaintext_bytes, 16)

    print(f"\nPlaintext (padded if needed): {plaintext_bytes.decode(errors='ignore')}")
    cipher = AES.new(key, AES.MODE_ECB)
    ciphertext = cipher.encrypt(plaintext_bytes)
    print(f"Ciphertext (hex): {ciphertext.hex()}")

    cipher_dec = AES.new(key, AES.MODE_ECB)
    decrypted_bytes = cipher_dec.decrypt(ciphertext)

    try:
        decrypted_text = unpad(decrypted_bytes, 16).decode()
    except ValueError:
        decrypted_text = decrypted_bytes.decode(errors='ignore')

    print(f"Decrypted Plaintext: {decrypted_text}")

if __name__ == "__main__":

    test_inputs = [
        "This is 16 bytes!",
        "This is exactly 32 bytes input string!",
        "48 byte input for AES testing purpose!!"
    ]

    keys = {
        "AES-128": b'ThisIsA16ByteKey',
        "AES-192": b'ThisIsA24ByteKeyForAES!',
        "AES-256": b'ThisIsA32ByteKeyForAES256Test!!'
    }

    for label, key in keys.items():
        print(f"\n{'='*10} {label} {'='*10}")
        for input_text in test_inputs:
            print(f"\n--- Testing with input: '{input_text}' ---")
            aes_encrypt_decrypt(input_text, key)
```

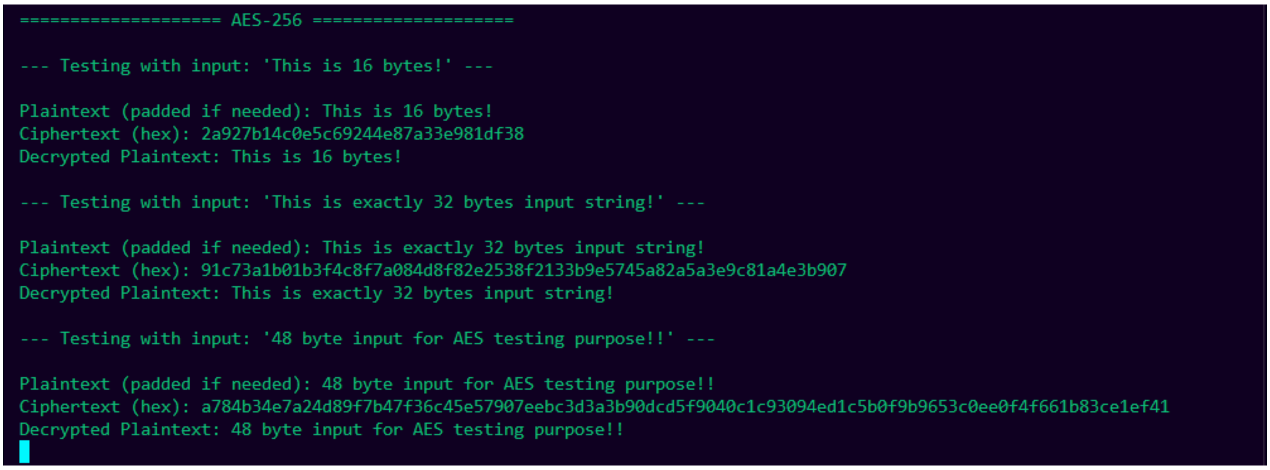
OUTPUT:



```
==================== AES-128 ====================

--- Testing with input: 'This is 16 bytes!' ---

Plaintext (padded if needed): This is 16 bytes!
Ciphertext (hex): 1e5f78b86d0f62e5b62dc94f7cfb12f4
Decrypted Plaintext: This is 16 bytes!

--- Testing with input: 'This is exactly 32 bytes input string!' ---

Plaintext (padded if needed): This is exactly 32 bytes input string!
Ciphertext (hex): 786c51502f21f4d4864e0e2cf8c30e65da8d4b5368bfbde6d3d983f5deab79c8
Decrypted Plaintext: This is exactly 32 bytes input string!

--- Testing with input: '48 byte input for AES testing purpose!!' ---

Plaintext (padded if needed): 48 byte input for AES testing purpose!!
Ciphertext (hex): 42b50df7b8cbe0e845ffdc2f56a55615e08aeb0bb27a7eebba09c7cf4eaa2392b00bb3f9fa95c50124653c1df087a35b
Decrypted Plaintext: 48 byte input for AES testing purpose!!
```



```
==================== AES-192 ====================

--- Testing with input: 'This is 16 bytes!' ---

Plaintext (padded if needed): This is 16 bytes!
Ciphertext (hex): 49a7cd0e1733cf0c7791b9121e7df344
Decrypted Plaintext: This is 16 bytes!

--- Testing with input: 'This is exactly 32 bytes input string!' ---

Plaintext (padded if needed): This is exactly 32 bytes input string!
Ciphertext (hex): 5b9c04ed2042fdd32edc4a9c2f60e998a5a40edb0fa6b11865d8b88cbb841c1d
Decrypted Plaintext: This is exactly 32 bytes input string!

--- Testing with input: '48 byte input for AES testing purpose!!' ---

Plaintext (padded if needed): 48 byte input for AES testing purpose!!
Ciphertext (hex): 3df55e6b6dbe0628d2e6f62ed36a7e7b9e6a8f53e4df3f2e2899a7e3d34de4b47a11c4dfde32c2e4fa65c1a65cb9d222
Decrypted Plaintext: 48 byte input for AES testing purpose!!
```



```
==================== AES-256 ====================

--- Testing with input: 'This is 16 bytes!' ---

Plaintext (padded if needed): This is 16 bytes!
Ciphertext (hex): 2a927b14c0e5c69244e87a33e981df38
Decrypted Plaintext: This is 16 bytes!

--- Testing with input: 'This is exactly 32 bytes input string!' ---

Plaintext (padded if needed): This is exactly 32 bytes input string!
Ciphertext (hex): 91c73a1b01b3f4c8f7a084d8f82e2538f2133b9e5745a82a5a3e9c81a4e3b907
Decrypted Plaintext: This is exactly 32 bytes input string!

--- Testing with input: '48 byte input for AES testing purpose!!' ---

Plaintext (padded if needed): 48 byte input for AES testing purpose!!
Ciphertext (hex): a784b34e7a24d89f7b47f36c45e57907eebc3d3a3b90dcd5f9040c1c93094ed1c5b0f9b9653c0ee0f4f661b83ce1ef41
Decrypted Plaintext: 48 byte input for AES testing purpose!!
```