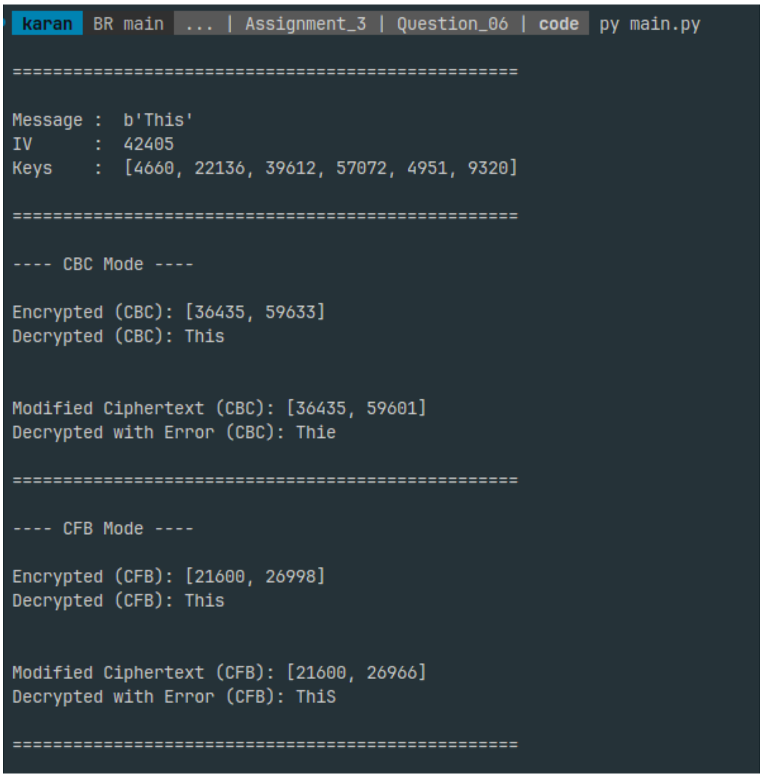
Question Number 6

- Use your implementation of Sypher004 in that you did in one of the earlier assignments.
- Implement its decryption.
- Now implement CBC and CFB modes of operation shown in class with the encryption and decryption of Sypher004.
- For CFB use t = 4.
- Assume that your test message is a multiple of 16-bits.
- Now simulate error in transmission by flipping some bits in one of the cipher-text blocks.
- Show the error propagation in the decrypted message by comparing it with original message.

Solution.

a) All code are implemented in `code` directory.

b) **Output**



```
karan  BR main  ... | Assignment_3 | Question_06 | code  py main.py

==================================================

Message :  b'This'
IV      :  42405
Keys    :  [4660, 22136, 39612, 57072, 4951, 9320]

==================================================

---- CBC Mode ----

Encrypted (CBC): [36435, 59633]
Decrypted (CBC): This


Modified Ciphertext (CBC): [36435, 59601]
Decrypted with Error (CBC): Thie

==================================================

---- CFB Mode ----

Encrypted (CFB): [21600, 26998]
Decrypted (CFB): This


Modified Ciphertext (CFB): [21600, 26966]
Decrypted with Error (CFB): ThiS

==================================================
```