Programming using Cryptography APIs

```
#!/usr/bin/python3

from Crypto.Cipher import AES
from Crypto.Util import Padding

key_hex_string = '00112233445566778899AABBCCDDEEFF'
iv_hex_string  = '000102030405060708090A0B0C0D0E0F'
key = bytes.fromhex(key_hex_string)
iv  = bytes.fromhex(iv_hex_string)
data = b'The quick brown fox jumps over the lazy dog'
print("Length of data: {0:d}".format(len(data)))

# Encrypt the data piece by piece
cipher = AES.new(key, AES.MODE_CBC, iv)                    ①
ciphertext  = cipher.encrypt(data[0:32])                   ②
ciphertext += cipher.encrypt(Padding.pad(data[32:], 16))   ③
print("Ciphertext: {0}".format(ciphertext.hex()))

# Encrypt the entire data
cipher = AES.new(key, AES.MODE_CBC, iv)                    ④
ciphertext = cipher.encrypt(Padding.pad(data, 16))         ⑤
print("Ciphertext: {0}".format(ciphertext.hex()))

# Decrypt the ciphertext
cipher = AES.new(key, AES.MODE_CBC, iv)                    ⑥
plaintext = cipher.decrypt(ciphertext)                     ⑦
print("Plaintext: {0}".format(Padding.unpad(plaintext, 16)))
```

- We use **PyCryptodome** package's APIs.
- Line:
  1. Initialize cipher
  2. Encrypts first 32 bytes of data
  3. Encrypts the rest of the data
  4. Initialize cipher (start new chain)
  5. Encrypt the entire data
  6. Initialize cipher for decryption
  7. Decrypt

Attack on ciphertext's integrity

- Attacker makes changes to ciphertext (Line 2)

```
data = b'The quick brown fox jumps over the lazy dog'

# Encrypt the entire data
cipher = AES.new(key, AES.MODE_OFB, iv)
ciphertext  = bytearray(cipher.encrypt(data))          ①

# Change the 10th byte of the ciphertext
ciphertext[10] = 0xE9                                  ②

# Decrypt the ciphertext
cipher = AES.new(key, AES.MODE_OFB, iv)
plaintext = cipher.decrypt(ciphertext)                 ③
print("Original  Plaintext: {0}".format(data))
print("Decrypted Plaintext: {0}".format(plaintext))
```

- Result

```
Original  Plaintext: b'The quick brown fox jumps over the lazy dog'
Decrypted Plaintext: b'The quick grown fox jumps over the lazy dog'
```