Lab 3 - Task 3: Corrupted Ciphertext Across Modes (AES-128)

Objective

Demonstrate how a 1-bit error in ciphertext propagates differently in AES-128 modes: ECB, CBC, CFB, and OFB. Produce evidence using OpenSSL and hexdumps.

Setup

- Plaintext: 80 bytes of ASCII 'A' (0x41).
- KEY (hex): 00112233445566778899aabbccddeeff
- IV (hex): 0102030405060708090a0b0c0d0e0f10 (for CBC/CFB/OFB).
- Fault injected at ciphertext byte index 29 (0-based).

Commands (copy-paste)

```
KEY=00112233445566778899aabbccddeeff
IV=0102030405060708090a0b0c0d0e0f10
python3 - <<'PY'
open('m64.txt','wb').write(b'A'*80)
PY
openssl enc -aes-128-ecb -e -in m64.txt -out ecb.bin -K $KEY -nosalt
openssl enc -aes-128-cbc -e -in m64.txt -out cbc.bin -K $KEY -iv $IV -nosalt
openssl enc -aes-128-cfb -e -in m64.txt -out cfb.bin -K $KEY -iv $IV -nosalt
openssl enc -aes-128-ofb -e -in m64.txt -out ofb.bin -K $KEY -iv $IV -nosalt
python3 - <<'PY'
for name in ['ecb.bin','cbc.bin','cfb.bin','ofb.bin']:
    b=bytearray(open(name,'rb').read()); b[29]^=1
    open(name.replace('.bin','_corrupt.bin'),'wb').write(b)
PY
openssl enc -aes-128-ecb -d -in ecb_corrupt.bin -out ecb_corrupt.txt -K $KEY -nosalt
openssl enc -aes-128-cbc -d -in cbc_corrupt.bin -out cbc_corrupt.txt -K $KEY -iv $IV -nosalt
openssl enc -aes-128-cfb -d -in cfb_corrupt.bin -out cfb_corrupt.txt -K $KEY -iv $IV -nosalt
openssl enc -aes-128-ofb -d -in ofb_corrupt.bin -out ofb_corrupt.txt -K $KEY -iv $IV -nosalt
```

Expected Error Propagation (why)

- AES block size = 16. Index 29 lies in block 1 (bytes 16..31), offset 13.
- ECB: only the affected 16-byte block becomes garbage; others unchanged.
- CBC: current block becomes garbage; in the next block, the same bit position flips.
- CFB: current byte flips and the following segment appears corrupted; later bytes recover.
- OFB: only that byte's bit flips; no further propagation.

Evidence (hexdump examples to capture)

```
xxd -g 1 -l 64 m64.txt
xxd -g 1 -l 64 ecb_corrupt.txt
xxd -g 1 -l 64 cbc_corrupt.txt
xxd -g 1 -l 64 cfb_corrupt.txt
xxd -g 1 -l 64 ofb_corrupt.txt
```

Lab 3 - Task 3: Corrupted Ciphertext Across Modes (AES-128)

Result and Conclusion

The experiment confirms the distinct error propagation patterns of the four modes. ECB corrupts the current block only; CBC corrupts the current block and flips one bit in the next; CFB affects the current byte and a subsequent segment; OFB confines the error to the single flipped byte. Therefore, chaining modes (CBC/CFB) and stream-like OFB behave very differently from ECB under faults.