Task 3

For this task, a text file was encrypted using AES-128 cipher in ECB, CBC,CFB and OFB modes as per instructions. The commands used are as follows:

aes-128-ecb

Key generation: `openssl rand -hex 16`

```
Encryption: openssl enc -aes-128-ecb -in task3_plaintext.txt
-out aes-128-ecb_ciphertext.bin -K
2b4f786e9b2a0c9d1367ab5ae54e1ad5

Decryption: openssl enc -aes-128-ecb -d -in
aes-128-ecb_ciphertext.bin -out
aes-128-ecb_decrypted_text.txt -K
2b4f786e9b2a0c9d1367ab5ae54e1ad5
```

```
     aes-128-cbc
Key generation: openssl rand -hex 16
Iv generation: openssl rand -hex 16
Encryption: openssl enc -aes-128-cbc -e -in
task3_plaintext.txt -
out aes-128-cbc_ciphertext.bin -K
57432f4d8f45c93ed923ebdeb5f6e049  -iv
d3acf35e63b2fa3cb790cc0e493
7ba20
Decryption: openssl enc -aes-128-cbc -d -in
aes-128-cbc_ciphertex
t.bin -out aes-128-cbc_decrypted_text.txt -K
57432f4d8f45c93ed923ebdeb5f6e049  -iv  d3acf35e63b2fa3c
b790cc0e4937ba20
```

```
     aes-128-cfb
Key generation: openssl rand -hex 16
Iv generation: openssl rand -hex 16
Encryption: openssl enc -aes-128-cfb -e -in
task3_plaintext.txt -
out aes-128-cfb_ciphertext.bin -K
0335f06014c5475501aae723d7962f06 -iv
d0e28497f8d366922cee6a85b6870
bc9
Decryption: openssl enc -aes-128-cfb -d -in
aes-128-cfb_ciphertex
t.bin -out aes-128-cfb_decrypted_text.txt -K
0335f06014c5475501aae723d7962f06 -iv d0e28497f8d366922c
ee6a85b6870bc9


     aes-128-ofb
Key generation: openssl rand -hex 16
Iv generation: openssl rand -hex 16
Encryption: openssl enc -aes-128-ofb -e -in
task3_plaintext.txt -out aes-128-ofb_ciphertext.bin  -K
77e0ee99c983d6a794f0139b00f12a29  -iv
40419ad244263a2c4bf49b5beb3988d4

Decryption: openssl enc -aes-128-ofb -d -in
aes-128-ofb_ciphertext.bin -out
aes-128-ofb_decrypted_text.txt  -K
77e0ee99c983d6a794f0139b00f12a29  -iv
40419ad244263a2c4bf49b5beb3988d4
```

The amount of information recoverable by decrypting the corrupted file

1. ECB: Blocks except for the corrupted block will be decrypted correctly.
2. CBC: Corrupted block and its next block will be decrypted incorrectly. The rest of the file will not be affected.
3. CFB: Corrupted blocks and its subsequent blocks will be affected.
4. OFB: Only the affected block will be decrypted incorrectly.

Reasons behind:

1. In ECB mode, each block of plaintext is encrypted independently.
2. each plaintext block is XORed with the previous ciphertext block before encryption.
3. In CFB mode, ciphertext blocks are XORed with the output of the encryption function to produce the plaintext. So an error in one ciphertext block will propagate to the corresponding part of the plaintext and potentially affect subsequent blocks.
4. Errors in the ciphertext will not propagate, as each block is decrypted independently of other blocks.

Implication: In all modes, the impact of corruption is typically limited to specific blocks, but the extent of the impact varies based on the mode's propagation properties.