Task 4

ECB

Key generation:openssl rand -hex 16

Encryption:openssl enc -aes-128-ecb -e -in task4_plaintext.txt -out aes-128-ecb_ciphertext.bin -K e37faf1b0f6f4b85872d9b639978d5e6

CBC

Key generation:openssl rand -hex 16

Iv generation:openssl rand -hex 16

Encryption:openssl enc -aes-128-cbc -e -in task4_plaintext.txt -out aes-128-cbc_ciphertext.bin -K cc8d9d03a91eef8a7f39f476fec338d4 -iv 1d622fc33f209f761ac0b4e96e049bdf

CFB

key generation: openssl rand -hex 16

iv generation: openssl rand -hex 16

Encryption:openssl enc -aes-128-cfb -e -in task4_plaintext.txt -out aes-128-cfb_ciphertext.bin -K dcf24241232a3093e4522a104f4c00bb -iv 3db7ff7ea2263c55353d7a610bfc646a

OFB

Key generation: openssl rand -hex 16

Iv generation: openssl rand -hex 16

Encryption: openssl enc -e -aes-128-ofb -in task4_plaintext.txt -out aes-128-ofb_ciphertext.bin -K ec776af9b2c45ad64607e3a97f690afc -iv bee562984b15cdca4a4065880d3aa780

From the size of the ciphertext files, it is evident that CFB and OFB doesn’t have padding as each byte is encrypted individually, they don't require padding to align plaintext blocks. On the otherhand, ECB and CBC encryption modes require padding to ensure that plaintexts of arbitrary length are aligned with the fixed block size of the encryption algorithm.