Solution of Exercisesheet 6

Exercise 6-1

Exercise 6-2

Task: Show that Π_{CBC} is not CCA-secure by demonstrating a successful adversary.
Assume n = 3
The adversary $\mathcal{A}$ can choose the two messages $m_0 = m_0^1||m_0^2 = 000\ 000$ and $m_1 = m_1^1||m_1^2 = 111\ 111$ which he sends to the challenger. Then he gets the ciphertext $c_b = (c_b^0||c_b^1||c_b^2) = (IV||f_k(IV \oplus m_b^1)||f_k(f_k(IV \oplus m_b^1) \oplus m_b^2))$ back.
Then $\mathcal{A}$ flipps the last bit from c_b^2, so $(c_b^2)' = c_b^2 \oplus 001$ and asks the decryption oracle for the decryption of $c_b' = c_b^0||c_b^1||(c_b^2)'$. Because $c_b' \neq c_b$ the decryption oracle answers with $m' = f_k^{-1}(c_b^1) \oplus c_b^0||f_k^{-1}(c_b^2) \oplus c_b^1 = f_k^{-1}(f_k(IV \oplus m_b^1)) \oplus IV||f_k^{-1}((c_b^2)') \oplus f_k(IV \oplus m_b^1) = m_b^1||f_k^{-1}((c_b^2)') \oplus f_k(IV \oplus m_b^1)$
m_b^1 is now either m_0^1 or m_1^1 because the change in $(c_b^2)'$ doesn't impact m_b^1. So the adversary can say for sure, if the recieved civertext c_b is the encoding for m_0 or m_1.
$\Rightarrow \Pi_{CBC}$ mode is not CCA-secure

Exercise 6-3