Übung 3, 1)

a) CBC

$$c_i = F_K\left(m_i \oplus c_{i-1}\right)$$

$$c_0 = IV$$

$$Enc_K := F_K\left(m_i \oplus c_{i-1}\right), \text{ mit } c_0 = IV, m_i = m_1 \dots m_e$$

$$Dec_K := F_K^{-1}\left(c_i\right) \oplus c_{i-1}$$

Korrektheit:

$$Dec_K\left(Enc_K\left(m_i^o\right)\right) = m_i^o$$

$$Dec_K\left(F_K\left(m_i^o \oplus c_{i-1}\right)\right) = m_i^o$$

$$F_K^{-1}\left(F_K\left(m_i^o \oplus c_{i-1}^o\right)\right) \oplus c_{i-1}^o = m_i^o$$

$$m_i^o \oplus c_{i-1}^o \oplus c_{i-1} = m_i^o$$

$$m_i^o = m_i^o$$

b) OFB

$i+1$: wie oft ausgeführt wird

$$Enc_k = f_k(IV_{i-1})^{(n)} \oplus m_i = c_i$$

$$Dec_k = f_k(IV_{i-1})^{n} \oplus c_i = m_i$$

Korrektheit:

$$Dec_k(Enc_k(m_i)) = m_i$$

$$Dec_k\underbrace{\left(f_k(IV_{i-1})^{n} \oplus m_i\right)}_{c_i} = m_i$$

$$\underbrace{f_k(IV_{i-1})^{n} \oplus c_i}_{m_i} = m_i$$

$$m_i = m_i$$

c) CTR

$$Dec_k = f_k(counter_i) \oplus \overset{c_i}{\curvearrowright} c_i = m_i$$