4b) CTR modified

$$Enc_k = f_k(m_i \oplus (IV+i))$$

$$\underline{\underline{Dec_k = f_k^{-1}(c_i) \oplus (IV+i)}}$$

Korrektheit:

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

$$Dec_k(f_k(m_i \oplus (IV+i))) = m_i$$

$$f_k^{-1}(f_k(m_i \oplus (IV+i)) \oplus (IV+i)) = m_i$$

$$m_i \oplus (IV+i) \oplus (IV+i) = m_i$$

$$\underline{\underline{m_i = m_i}}$$