


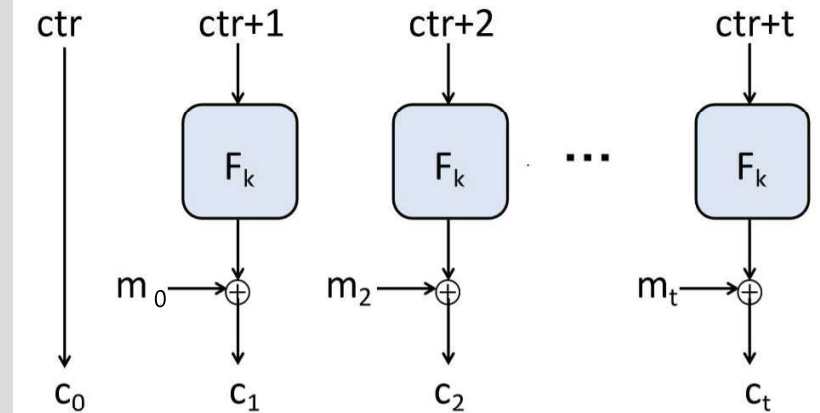
실습 #1



•CTR(Counter)

IV를 1씩 증가시키고, 그 값을 F_k 의 입력으로 넣는다. F_k 의 출력값과 현재 블록의 메시지(m_i)와 XOR 연산을 한다. 연산의 결과가 현재 블록의 암호문(c_{i+1})이다. IV는 초기 암호문(c_0)이다.

$Enc_k(m_0, \dots, m_t)$
 $c_0(ctr) \leftarrow \{0,1\}^n$
 for $i=0$ to t
 $c_{i+1} = m_i \oplus F_k(ctr + i)$
 return (c_0, \dots, c_{t+1})

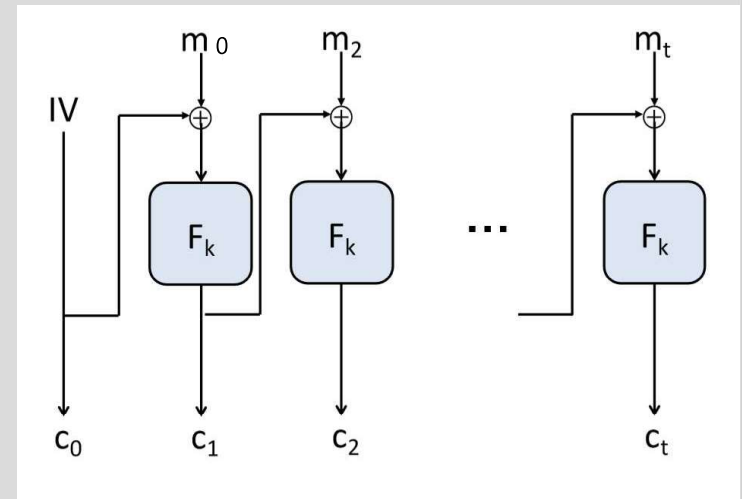


$Dec_k(c_0, \dots, c_{t+1})$
 for $i=1$ to $t+1$
 $m_{i-1} = c_i \oplus F_k(ctr + i)$
 return (m_0, \dots, m_t)

• CBC(Chipher-Block Chaining)

- 1976년 IBM에 의해 개발

이전 블록의 암호문(c_i)과 현재 블록의 평문(m_i)을 XOR 연산한 결과를 F_k 의 입력으로 넣는다. F_k 의 출력이 현재 블록의 암호문(c_{i+1})이다. IV는 초기 암호문(c_0)으로 사용한다.



$Enc_k(m_0, \dots, m_t)$

$c_0(IV) \leftarrow \{0,1\}^n$

for $i=0$ to t

$c_{i+1} = F_k(m_i \oplus c_i)$

return (c_0, \dots, c_{t+1})

$Dec_k(c_0, \dots, c_{t+1})$

for $i=1$ to $t+1$

$m_{i-1} = F_k^{-1}(c_i) \oplus c_{i-1}$

return (m_0, \dots, m_t)

역함수!!