Mode of operation

https://youtu.be/74-c3OTpcSo

Contents

CryptoCraft LAB

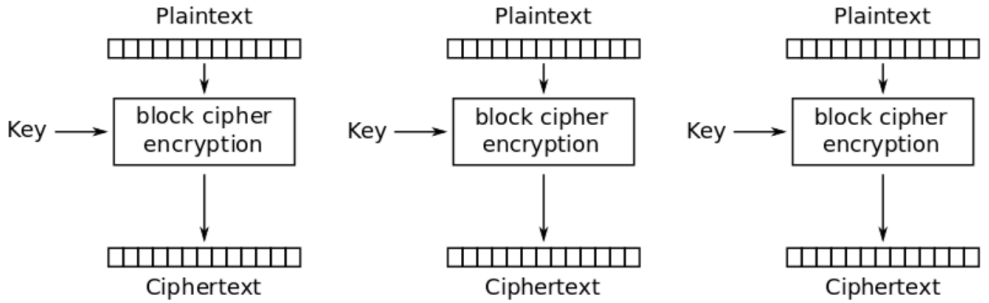
Mode of operation

- 운영모드 (Mode of operation)
  - 하나의 키로 블록암호를 반복적으로 안전하게 이용하는 절차
  - 블록암호는 블록 단위로 동작 → 가변 길이 데이터를 블록단위로 나누어야 함
  - 나눠진 블록들을 **암호화하는 방식**을 운영방식이라고 함

- 운영모드의 목적
  - **Confidentiality** : 인가되지 않은 사용자 또는 객체가 정보의 내용을 알 수 없도록 하는 것
  - **Authenticity** : 받은 정보가 정말로 원송신자로부터 온 것인지 확인할 수 있는 것
  - **Integrity** : 인가되지 않은 사용자 또는 객체가 정보를 함부로 수정할 수 없도록 하는 것

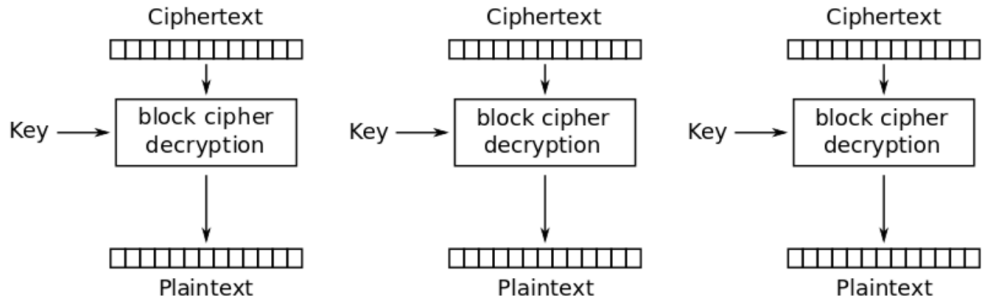
ECB

- ECB (Electronic Code Block) Mode
  - 길이가 b bits를 초과하는 메시지는 b bits로 나눔
  - 각 블록은 **개별적으로** 암호화됨



Electronic Codebook (ECB) mode encryption

- ECB Mode 공식
  - 암호화 : $y_i = e_k(x_i),\ i \geq 1$
  - 복호화 : $x_i = e_k^{-1}(y_i) = e_k^{-1}(e_k(x_i))\ ,\ i \geq 1$



Electronic Codebook (ECB) mode decryption

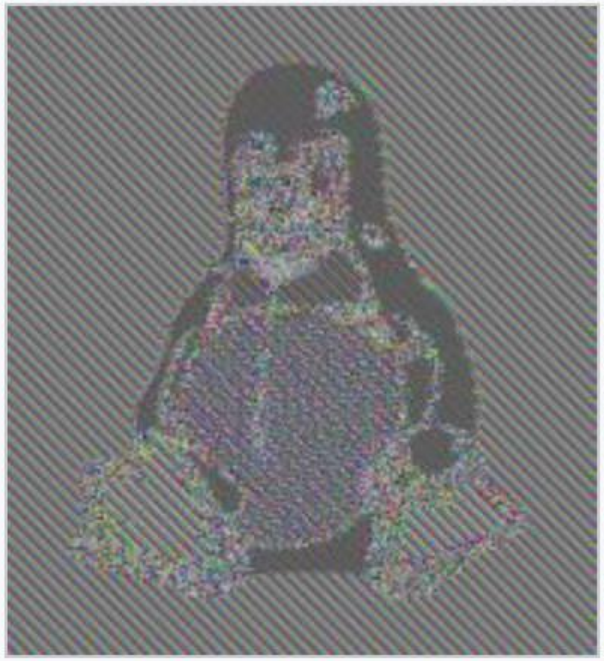
ECB

- Advantages of ECB Mode
  - 송신자와 수신자 사이에 블록 동기화가 필요 X
  - 노이즈에 의한 비트 오류 발생 시 대응되는 블록에만 영향을 미침
  - 블록암호 연산 병렬화 가능 → 고속 구현에 용이

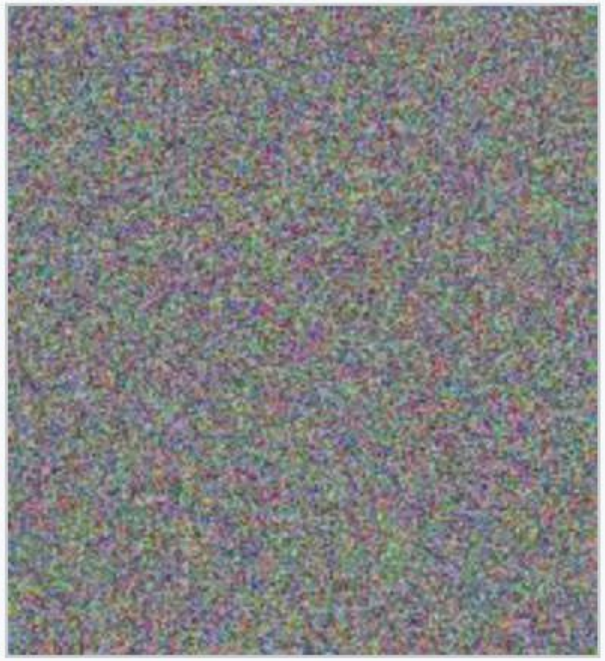
- Disadvantage of ECB Mode
  - 동일한 평문은 동일한 암호문을 생성함 → 암호문 블록으로부터 평문을 유추 가능

ECB

Original Image



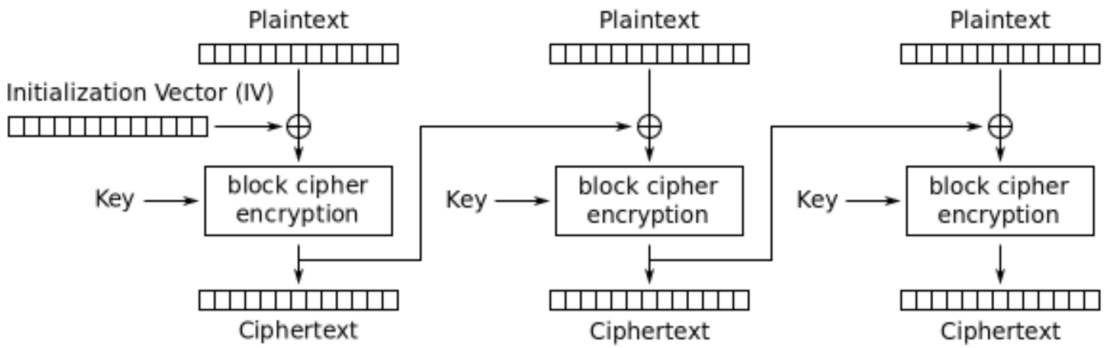
Encrypted using ECB mode



Encrypted using CBC mode

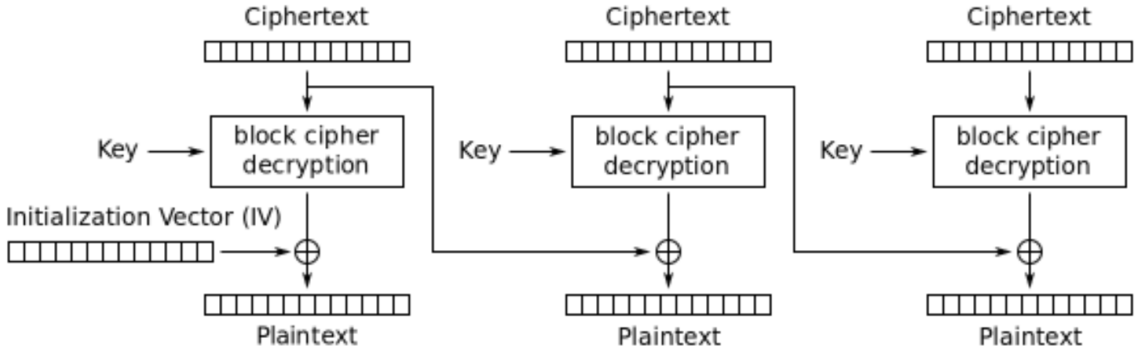
CBC

- CBC(Cipher Block Chaining) Mode
  - 모든 블록의 암호화가 **상호 연결됨**
  - 첫 블록의 암호화는 초기화 벡터를 이용
  - 그 외 블록의 암호화는 y_{i-1}을 x_i 암호화할 때 이용



Cipher Block Chaining (CBC) mode encryption

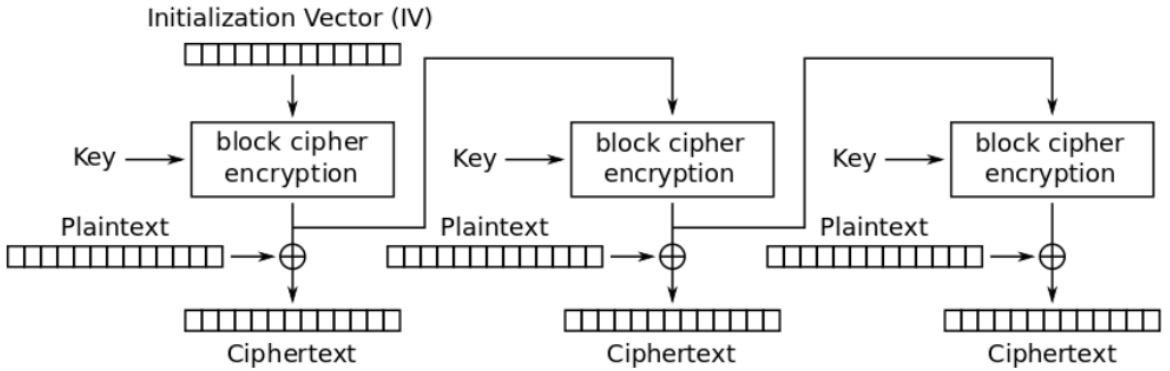
- CBC Mode 공식
  - 첫 번째 블록 암호화 : $y_1 = e_k(x_1 \oplus IV)$
  - 그 외 블록 암호화 : $y_i = e_k(x_i \oplus y_{i-1}),\ i \geq 2$
  - 첫 번째 블록 복호화 : $x_1 = d_k(y_1) = e_k^{-1}(y_1) \oplus IV$
  - 그 외 블록 복호화 : $x_i = d_k(y_i) = e_k^{-1}(y_i) \oplus y_{i-1},\ i \geq 2$



Cipher Block Chaining (CBC) mode decryption

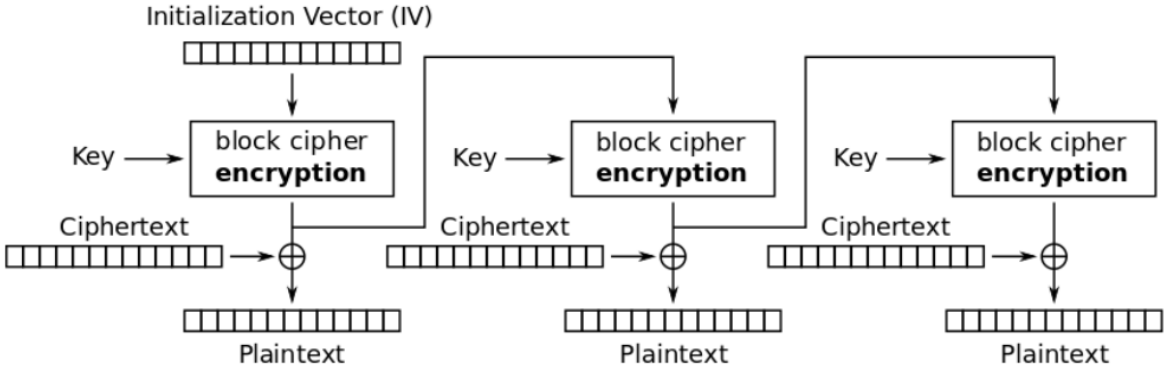
OFB

- OFB(Output FeedBack) Mode
  - 첫 번째 블록은 초기화 벡터를 암호화 함
  - 암호문의 출력은 b 비트의 키 스트림 s_i를 생성
  - s_i와 평문을 XOR 연산을 통해 암호화
  - s_i는 다음 블록 암호화할 때 사용됨.



Output Feedback (OFB) mode encryption

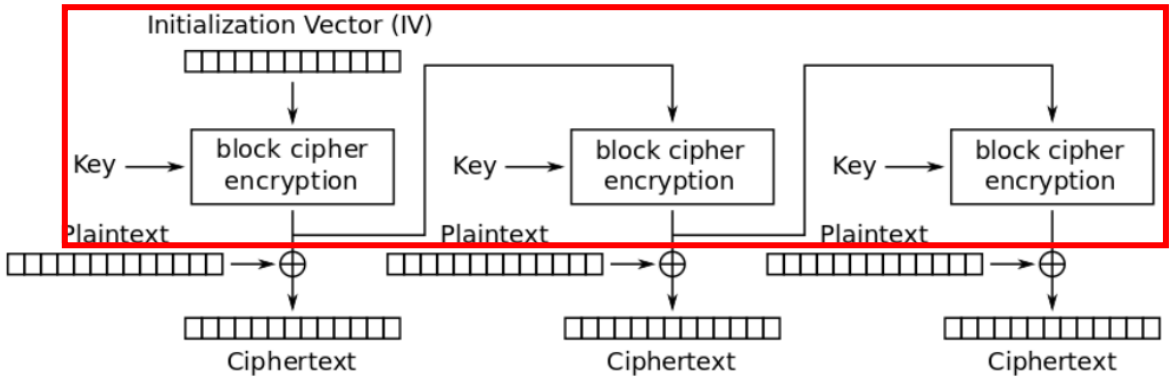
- OFB Mode 공식
  - 첫 번째 블록 암호화 : $s_1 = e_k(IV), \quad y_1 = (s_1 \oplus x_1)$
  - 그 외 블록 암호화 : $s_i = e_k(s_{i-1}), \quad y_i = (s_i \oplus x_i), \ i \geq 2$
  - 첫 번째 블록 복호화 : $s_1 = e_k(IV), \quad x_1 = (s_1 \oplus y_1)$
  - 그 외 블록 복호화 : $s_i = e_k(s_{i-1}), \quad x_i = (s_i \oplus y_i), \ i \geq 2$



Output Feedback (OFB) mode decryption

OFB

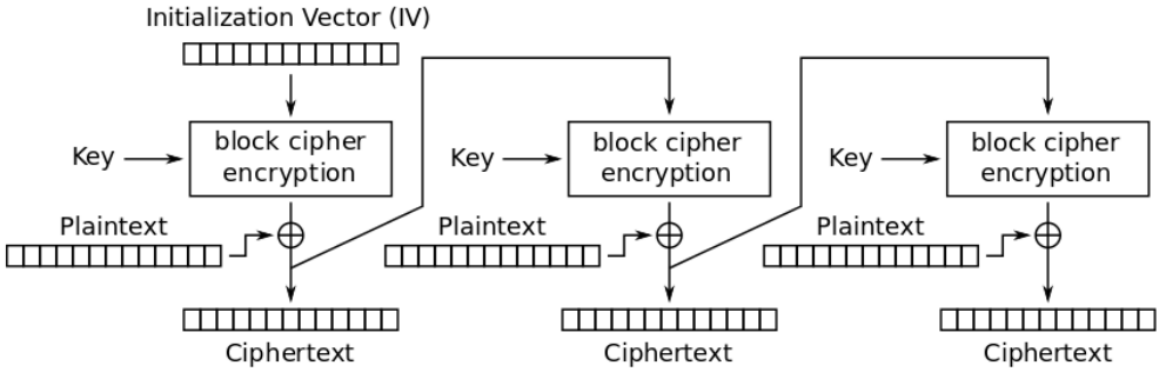
- OFB Mode의 특징
  - Nonce인 초기화 벡터를 사용 → 같은 내용의 두 평문에 대한 암호화 결과가 다름
  - XOR 연산으로 인해 복호화할 때 e_k^{-1}대신 e_k가 사용됨 → 암호화와 복호화가 같은 구조
  - 블록암호의 계산이 평문과 독립적 → s_i를 미리 계산 가능



Output Feedback (OFB) mode encryption

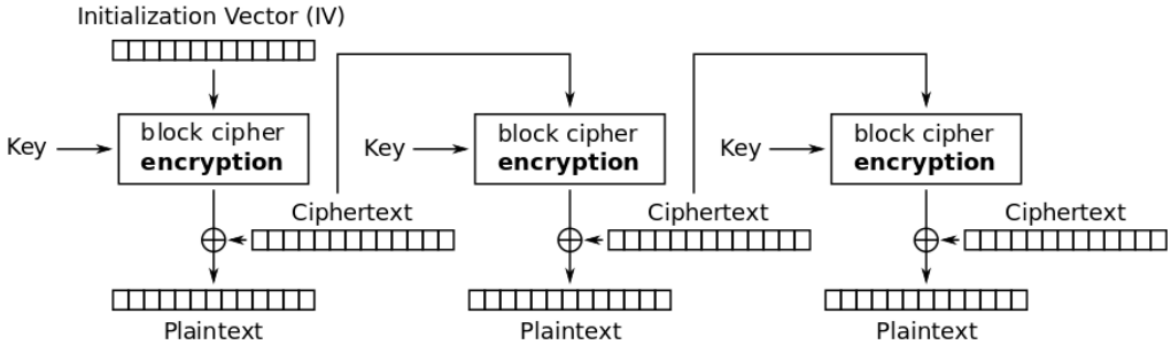
CFB

- CFB(Cipher FeedBack) Mode
  - 첫 번째 블록은 초기화 벡터를 암호화 함
  - 암호문의 출력은 b 비트의 키 스트림 s_i를 생성
  - s_i와 평문을 XOR 연산을 통해 암호화
  - y_i 는 다음 블록 암호화할 때 사용됨
  - 블록 암호화의 출력을 피드백하는 게 아니라 암호문을 피드백함



Cipher Feedback (CFB) mode encryption

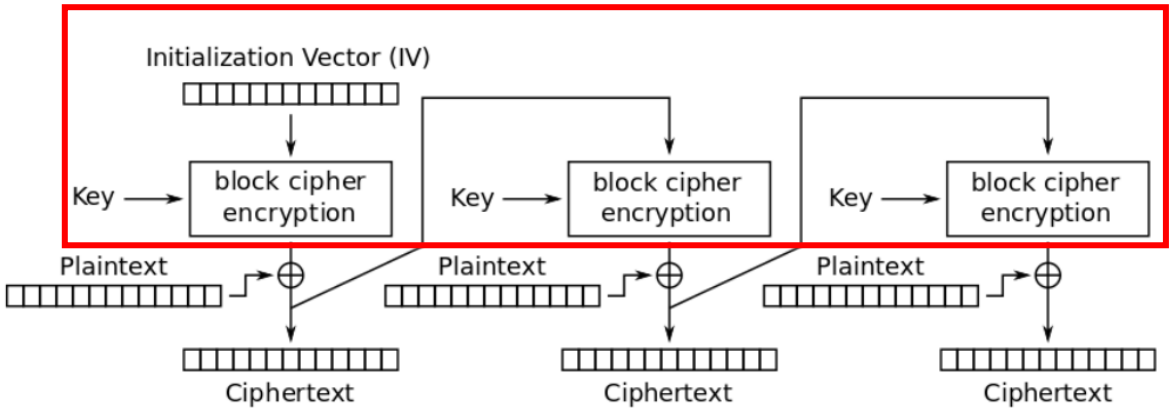
- CFB Mode 공식
  - 첫 번째 블록 암호화 : $y_1 = e_k(IV) \oplus x_1$
  - 그 외 블록 암호화 : $y_i = e_k(y_{i-1}) \oplus x_i,\ i \geq 2$
  - 첫 번째 블록 복호화 : $\mathrm{x}_1 = e_k(IV)\ \oplus y_1$
  - 그 외 블록 복호화 :$x_i = e_k(y_{i-1}) \oplus y_i,\ i \geq 2$



Cipher Feedback (CFB) mode decryption

CFB

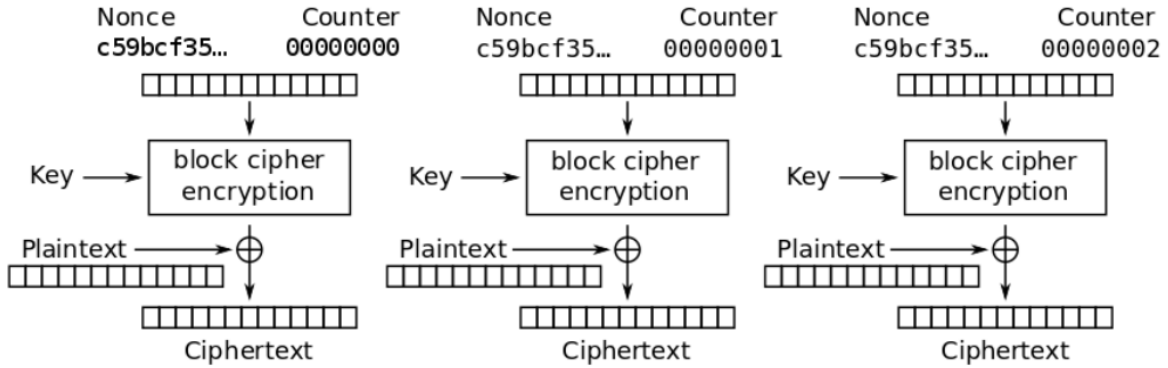
- CFB Mode의 특징
  - Nonce인 초기화 벡터를 사용 → 같은 내용의 두 평문에 대한 암호화 결과가 다름
  - XOR 연산으로 인해 복호화할 때 e_k^{-1}대신e_k가 사용됨 → 암호화와 복호화가 같은 구조
  - OFB 모드와 비슷한 형태를 가지지만 블록 암호화의 출력을 피드백하는 게 아니라 암호문을 피드백 → s_i 미리 계산 불가능
  - 짧은 길이의 평문을 암호화하는 경우에 많이 사용됨



Cipher Feedback (CFB) mode encryption

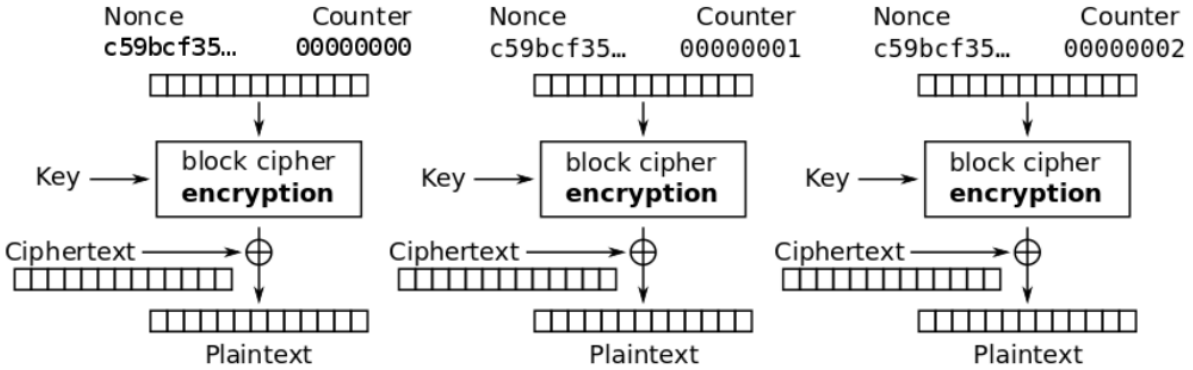
CTR

- CTR (CounTeR) Mode
  - 숫자(count)와 nonce를 결합하여 블록 암호의 입력으로 사용
  - 암호문의 출력은 b 비트의 키 스트림 s_i를 생성
  - s_i와 평문을 XOR 연산을 통해 암호화
  - 각 블록은 개별적으로 암호화됨



Counter (CTR) mode encryption

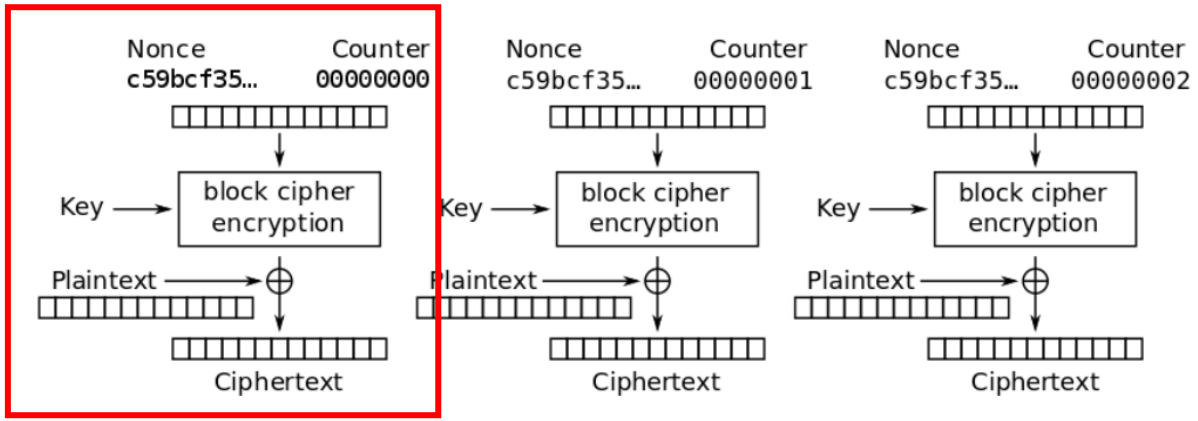
- CTR Mode 공식
  - 암호화 : $y_i = e_k(IV||CTR_i) \oplus x_i,\ i \geq 1$
  - 복호화 :$x_i = e_k(IV||CTR_i) \oplus y_i,\ i \geq 1$



Counter (CTR) mode decryption

CTR

- CTR Mode 특징
  - 송신자와 수신자 사이에 블록 동기화가 필요 X
  - 노이즈에 의한 비트 오류 발생 시 대응되는 블록에만 영향을 미침
  - 블록암호 연산 병렬화 가능 → 고속 구현에 용이



Counter (CTR) mode encryption

Q & A