Block Cipher Mode of Operation

목차

- 블록 암호 시스템 운영 모드
  - ECB
  - CBC
  - CFB
  - OFB
  - CTR

블록 암호시스템 운영모드

Reference: (Stallings, 2014; Forouzan, 2008; Rolf Oppliger, 2011; Rolf Oppliger, , 2021)
Reference: https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-38a.pdf

- 동기
  - 블록 암호시스템은 하나의 고정 크기 블록에 대해 동작
    - DES는 64비트 블록, AES는 128비트 블록
  - 그러나 실제 평문 길이는 가변적
    - 대부분 블록 크기를 초과하는 데이터의 암호화, 복호화 필요
  - 임의 길이 평문에 대해 블록 암호시스템을 반복 적용하는 방법 필요
- 블록 암호시스템 운영모드(Block cipher mode of operation)
  - ECB (Electronic Code Book)
  - CBC (Cipher Block Chaining)
  - CFB (Cipher Feedback)
  - OFB (Output Feedback)
  - CTR (Counter)

  } **기밀성(confidentiality) 제공을 위한 운영 모드들**

패딩 (padding)

Reference: Reference: https://datatracker.ietf.org/doc/html/rfc2315

PKCS#7 패딩

- 블록 크기 K 바이트(K<256), 메시지 크기 L 바이트에 대해,
- L mod K = K-1 → 1의 바이트 표현 1개를 메시지 끝에 추가
- L mod K = K-2 → 2의 바이트 표현 2개를 메시지 끝에 추가
- L mod K = K-3 → 3의 바이트 표현 3개를 메시지 끝에 추가
- …
- L mod K = 0 → K의 바이트 표현 K개를 메시지 끝에 추가

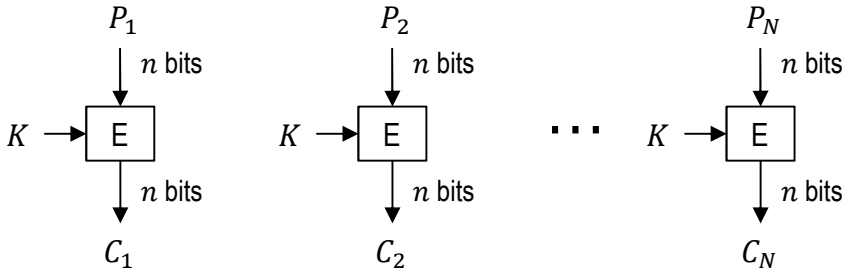
- 예) 블록 크기 8 바이트, 메시지 M=AABBCC → 패딩 후 → M=AABBCC0505050505
- 예) 블록 크기 8 바이트, 메시지 M=1122334455667788 → 패딩 후 → M=11223344556677880808080808080808

비트 패딩

- 메시지 끝에 비트 1을 부착한 후 블록 크기의 배수가 될 때까지 비트 0을 추가
- 예) 블록 크기 8 바이트, 메시지 M=AABBCC → 패딩 후 → M=AABBCC8000000000
- 예) 블록 크기 8 바이트, 메시지 M=1122334455667788 → 패딩 후 → M=11223344556677888000000000000000

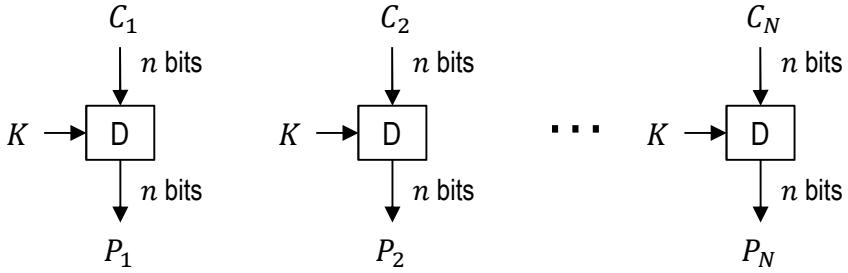
ECB (Electronic Code Book)

Reference: (Stallings, 2014; Forouzan, 2008; Rolf Oppliger, 2011; Rolf Oppliger, , 2021)
Reference: https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-38a.pdf



Encryption $(i = 1 \sim N)$:

$$C_i = E_K(P_i)$$



Decryption $(i = 1 \sim N)$:

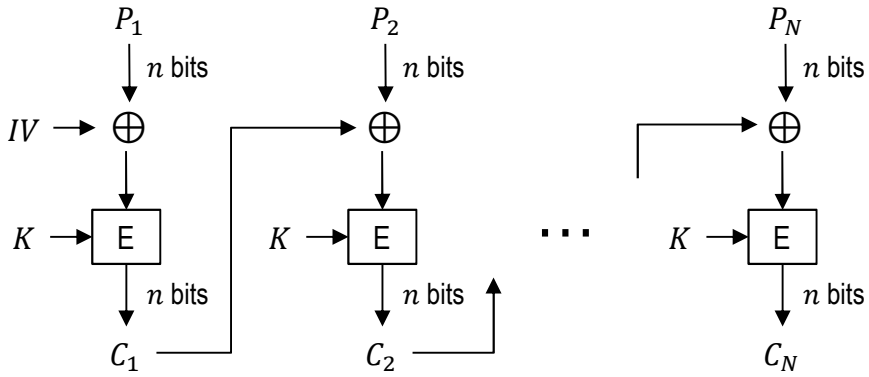
$$P_i = D_K(C_i)$$

ECB (Electronic Code Book)

- **암호화 →** 블록 크기 n 비트보다 큰 평문 메시지는 n 비트 단위의 평문 블록(들)로 분할 후 각 평문 블록에 대해 블록 암호화 적용하여 암호문 블록 생성
- **복호화 →** 각 암호문 블록에 대해 블록 복호화 적용하여 평문 블록 생성
- **패딩 →** 최초 평문에서 분할된 마지막 블록이 블록 크기보다 작은 경우 패딩 적용
- **오류 전파 →** 전송 중 특정 암호문 블록의 단일 비트 오류 발생 시 해당 블록에만(일반적으로 해당 블록의 절반 이상 비트들에) 영향 미치며, 다른 블록들로의 오류 전파 없음
- **병렬 처리 →** 블록 간 독립성이 있으므로 암호화 및 복호화 시 병렬처리 적용 가능
- **단점 →** 평문 내 동일 내용 블록들은 동일한 암호문 블록들로 생성되어, 평문의 통계적 정보가 공격자에게 알려질 수 있으며, 암호문 블록(들)의 삭제, 순서 변경 등의 공격이 가해질 수 있음.

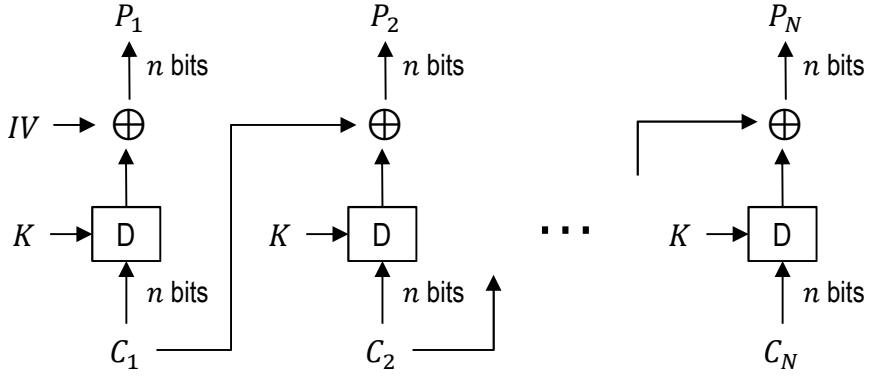
CBC (Cipher Block Chaining)

Reference: (Stallings, 2014; Forouzan, 2008; Rolf Oppliger, 2011; Rolf Oppliger, , 2021)
Reference: https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-38a.pdf



Encryption $(i = 2 \sim N)$:

$$C_1 = E_K(P_1 \oplus IV), \qquad C_i = E_K(P_i \oplus C_{i-1})$$



Decryption $(i = 2 \sim N)$:

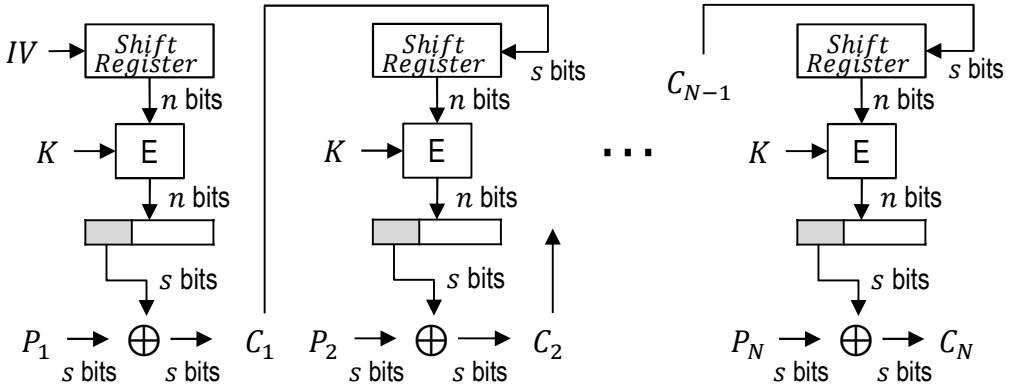
$$P_1 = D_K(C_1) \oplus IV, \qquad P_i = D_K(C_i) \oplus C_{i-1}$$

CBC (Cipher Block Chaining)

- **암호화 →** 각 평문 블록을 직전 암호문 블록과 XOR한 결과에 대해 블록 암호화 적용하여 암호문 블록을 생성. 최초 평문 블록의 경우, IV(Initialization Vector)가 직전 암호문 블록 대신 사용됨. IV 값에 대해 송수신측 간 사전 합의 필요
- **복호화 →** 각 암호문 블록을 블록 복호화한 결과를 직전 암호문 블록과 XOR하여 평문 블록을 생성
- **오류 전파 →** 전송 중 특정 암호문 블록 C_i 내 단일 비트 오류가 발생한 경우, 수신측 복호화를 통해 얻어지는 대응하는 평문 P_i (의 대부분의 비트들)와 직후 평문 P_{i+1} 내 오류 발생하며(복호화된 P_{i+1}의 경우 1 비트만 오류 발생), P_{i+2}부터의 복호화된 평문 블록(들)에는 오류 전파 없음
- **병렬 처리 →** 체인 메커니즘으로 인해 암호화 시 병렬 처리 활용 불가. 복호화 시 암호문 블록들이 준비되어 있다면 병렬 처리 적용 가능
- **특징 →** 하나의 평문 메시지 내 동일 내용 블록들이어도 서로 다른 암호문 블록들로 변환됨

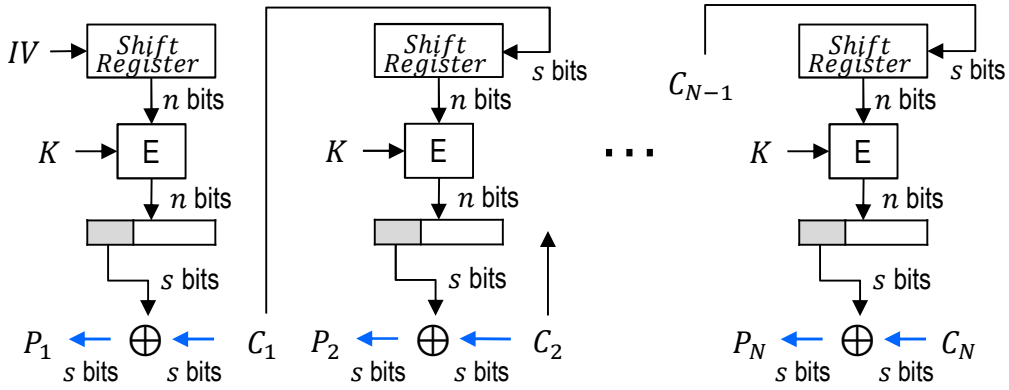
CFB (Cipher Feedback)

Reference: (Stallings, 2014; Forouzan, 2008; Rolf Oppliger, 2011; Rolf Oppliger, , 2021)
Reference: https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-38a.pdf



Encryption $(i = 2 \sim N)$: $SR_1 = IV,\ C_1 = P_1 \oplus MSB_s\left(E_K(SR_1)\right)$

$SR_i = LSB_{n-s}(SR_{i-1}) \parallel C_{i-1},\ C_i = P_i \oplus MSB_s\left(E_K(SR_i)\right)$



Decryption $(i = 2 \sim N)$: $SR_1 = IV,\ P_1 = C_1 \oplus MSB_s\left(E_K(SR_1)\right)$

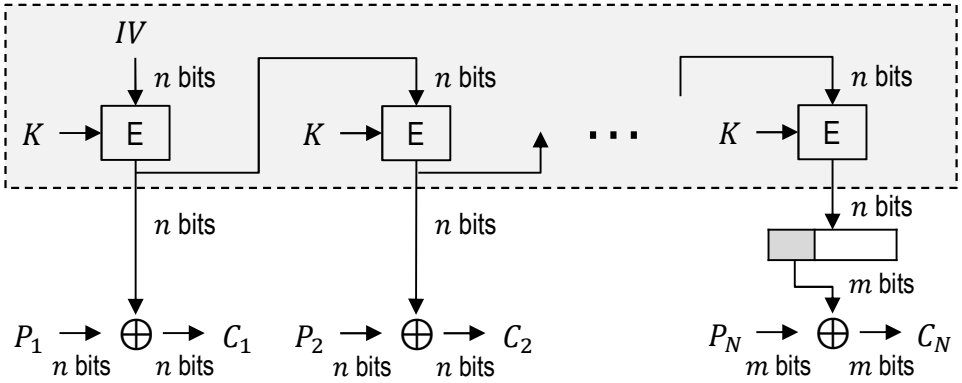
$SR_i = LSB_{n-s}(SR_{i-1}) \parallel C_{i-1},\ P_i = C_i \oplus MSB_s\left(E_K(SR_i)\right)$

CFB (Cipher Feedback)

- **전송 단위** → CFB 모드의 전송 단위 s 비트는 블록 암호 시스템이 사용하는 블록 크기 n 보다 적은 크기로 설정 가능($1 \le s \le n$). 예를 들어 1 비트 CFB, 8비트 CFB 등. 평문 메시지는 s 비트 크기의 세그먼트(segment)로 분할됨
- **Shift register(쉬프트 레지스터)** → shift register의 내용은 직전 shift register의 내용을 왼쪽으로 s 비트 쉬프트한 후 빈 부분을 직전 생성된 s 비트 암호문 블록으로 채워 만들어짐. 최초 shift register의 내용은 Initialization Vector (IV) 값으로 초기화됨.
- **암호화** → shift register의 내용을 블록 암호화한 결과의 최상위 s 비트들과 평문 세그먼트를 XOR하여 암호문 세그먼트 생성
- **복호화** → shift register의 내용을 블록 암호화한 결과의 최상위 s 비트들과 암호문 세그먼트를 XOR하여 평문 세그먼트 생성
- **패딩** → 패딩 필요 없음 (CFB 평문 세그먼트 크기 s가 원하는 데이터 단위(예: 8 bits)로 고정 설정된 경우)
- **오류 전파** → 전송 중 특정 암호문 세그먼트 C_i 내 단일 비트 오류가 발생한 경우, 수신측에서 복호화된 평문 세그먼트 P_i 내에서도 동일 위치의 단일 비트 오류 발생하며, 오류 세그먼트가 shift register에 남아 있는 동안 이후 복호화되는 평문들에도 영향 미침
- **특징** → 암호화 및 복호화를 위해 블록 암호시스템의 암호화 모듈만 사용됨

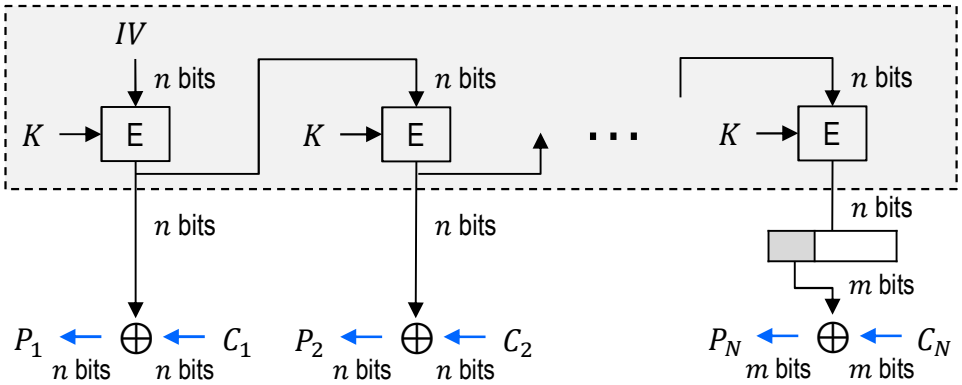
OFB (Output Feedback)

Reference: (Stallings, 2014; Forouzan, 2008; Rolf Oppliger, 2011; Rolf Oppliger, , 2021)
Reference: https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-38a.pdf



Encryption $(i = 2 \sim N)$:

$$O_1 = E_K(IV),\ O_i = E_K(O_{i-1}),\ C_i = P_i \oplus O_i,\ C_N = P_N \oplus MSB_m(O_N)$$



Decryption $(i = 2 \sim N)$:

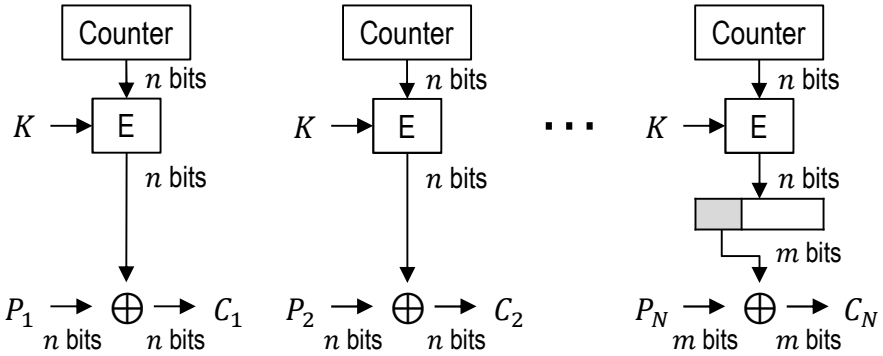
$$O_1 = E_K(IV),\ O_i = E_K(O_{i-1}),\ P_i = C_i \oplus O_i,\ P_N = C_N \oplus MSB_m(O_N)$$

OFB (Output Feedback)

- **암호화** → 블록암호시스템의 직전 출력을 블록 암호화한 결과와 평문 블록을 XOR하여 암호문 블록 생성. 블록암호시스템의 최초 입력은 Initialization Vector (IV) 값을 사용하며 이 값은 nonce여야 함
- **복호화** → 블록암호시스템의 직전 출력을 블록 암호화한 결과와 암호문 블록을 XOR하여 평문 블록 생성
- **패딩 불필요** → encryption 블록 크기가 n 비트이고, 마지막 평문 블록이 m 비트인 경우($m \leq n$), encryption 출력의 최상위 m비트들만 취하여 마지막 평문 블록과 XOR 수행
- **오류 전파** → 전송 중 특정 암호문 블록 C_i 내 단일 비트 오류가 발생한 경우, 수신측에서 복호화된 평문 블록 P_i 내에서도 동일 위치의 단일 비트 오류가 발생하지만 이후 복호화되는 평문 블록에는 영향 없음
- **특징** → 암호화 및 복호화를 위해 블록 암호시스템의 암호화 모듈만 사용됨

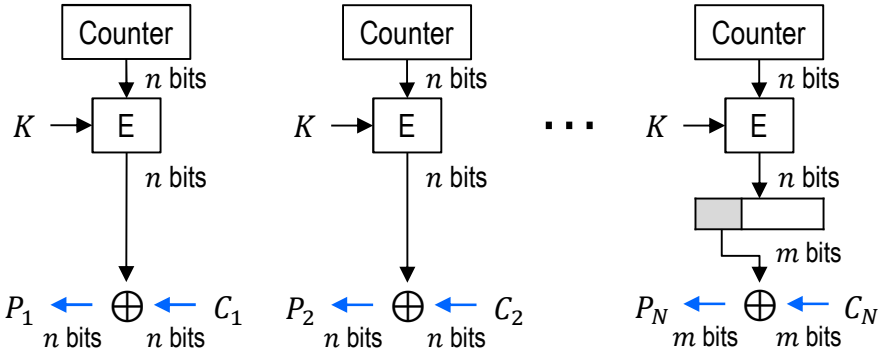
CTR (Counter)

Reference: (Stallings, 2014; Forouzan, 2008; Rolf Oppliger, 2011; Rolf Oppliger, , 2021)
Reference: https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-38a.pdf



Encryption $(i = 1 \sim N)$:

$$C_i = P_i \oplus E_K(CTR_i), \quad C_N = P_N \oplus MSB_m\left(E_K(CTR_N)\right)$$



Decryption $(i = 1 \sim N)$:

$$P_i = C_i \oplus E_K(CTR_i), \quad P_N = C_N \oplus MSB_m\left(E_K(CTR_N)\right)$$

CTR (Counter)

- **암호화** → 카운터를 블록 암호화한 결과와 평문 블록을 XOR하여 암호문 블록 생성
- **복호화** → 카운터를 블록 암호화한 결과와 암호문 블록을 XOR하여 평문 블록 생성
- **카운터** → 최초 초기화된 값 사용되며 다음 블록 처리 시 그 값을 1 만큼 증가함(n 비트 카운터의 경우 모듈로 2^n 연산 적용). 카운터의 초기값은 nonce여야 함
- **패딩 불필요** → encryption 블록 크기가 n 비트이고, 마지막 평문 블록이 m 비트인 경우($m \leq n$), 카운터를 암호화한 결과의 최상위 m비트들만 취하여 마지막 평문 블록과 XOR 수행
- **오류 전파** → 전송 중 암호문 블록 내 단일 비트 오류 발생 시 복호화된 평문 블록 내 동일 위치 비트에만 영향 미침
- **특징** → 암호화 및 복호화를 위해 블록 암호시스템의 암호화 모듈만 사용됨

References

- Rolf Oppliger, Cryptography 101: From Theory To Practice, 2021
- Rolf Oppliger, Contemporary Cryptography, 2011
- Behrouz A. Forouzan, Cryptography and Network Security, McGraw-Hill, 2008
- William Stallings, Cryptography and Network Security: Principles and Practice, Sixth Edition, Prentice Hall, 2014
- Christof Paar, Jan Pelzl, Understanding Cryptography: A Textbook for Students and Practitioners, Springer, 2010
- 김명환, 수리암호학개론, 2019
- 정민석, 암호수학, 경문사, 2017
- 최은미, 정수와 암호론, 북스힐, 2019
- 이민섭, 정수론과 암호론, 교우사, 2008