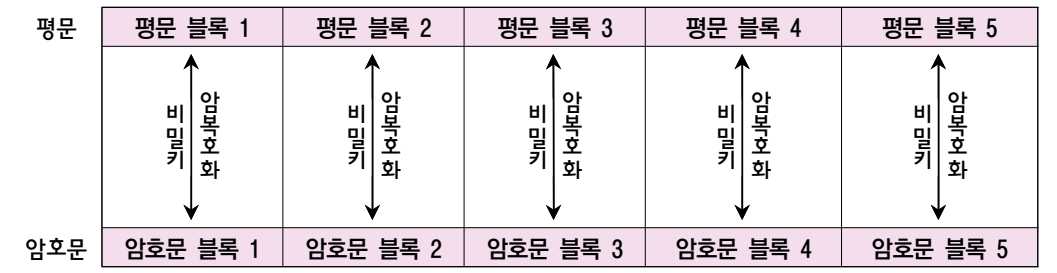
10. ECB 모드

ECB(Electric CodeBook mode)는 가장 **단순한** 운영모드이다.



• 평문은 여러 개의 블록으로 분할된다.(예 : DES에서는 64bit, AES에서는 128bit)
→ 만일, 마지막 블록 길이가 다른 블록과 다르면 **덧붙이기**(paddding)를 한다.

• 평문 블록과 암호문 블록이 일대일의 관계를 유지한다.**(짧은 메시지에 응용)**
→ 암호화한 평문 블록이 그대로 암호문 블록이 된다.(다른 블록과 연관이 없다)
→ 암호화 및 복호화 과정에서 모든 블록은 개별적(독립적)으로 취급된다.
→ 같은 내용을 가지는 평문 블록은 같은 암호문 블록으로 변환된다.

• ECB는 기밀성이 가장 낮은 모드로 안전성에 문제가 있다.(거의 사용되지 않는 모드)
→ 암호문을 분석하면 평문 속에 같은 패턴이 반복되는 것을 알 수 있다.
→ 이를 이용하여 암호문을 해독할 수 있다.

• ECB는 ECB는 특정 하나의 블록만을 대상으로 암복호화 하는 환경에서는 효과적이다.
→ 암호화 대상 데이터가 기본 블록 단위보다 큰 경우에는 사용을 권고하지 않는다.

• ECB는 각 블록을 병렬적으로 처리할 수 있다.(중간 블록에서도 암복호화가 될 수 있다)

• ECB는 전송 도중에 단일비트 오류는 다른 블록에 영향을 주지 않는다.(오류전파 안됨)
→ 암호문 블록의 단일비트 오류는 대응하는 평문 블록의 거의 모든 비트에서 오류 발생

◈ **ECB에서 평문과 암호문 사이의 관계**

• 암호 : $C_i = E_K(P_i)$

• 복호 : $P_i = D_K(C_i)$

기출문제 분석

1. <보기>에서 블록암호 모드 중 초기 벡터(initialization vector)가 필요하지 않은 모드를 모두 고른 것은? [2019년 서울 9급]

------<보기>----------

ㄱ. CTR 모드 ㄴ. CBC 모드 ㄷ. ECB 모드

---

① ㄱ ② ㄷ ③ ㄴ, ㄷ ④ ㄱ, ㄴ, ㄷ

♤ 블록암호 모드

모드	유형(type)	초기 벡터	오류 전파	암호 병행처리
ECB	**블록 암호**	필요 없음(none)	No	가능
CBC	**블록 암호**	필요함(yes)	**Yes**	**불가**
CFB	스트림 암호	필요함(yes)	**Yes**	**불가**
OFB	스트림 암호	필요함(yes)	No	**불가**
CTR	스트림 암호	필요함(yes) - 카운터	No	가능

정답 : ②

2. 다음에서 설명하는 블록암호 운영모드는? [2021년 지방 9급]

○ 단순한 모드로 평문이 한 번에 하나의 평문 블록으로 처리된다.
○ 각 평문 블록은 동일한 키로 암호화된다.
○ 주어진 하나의 키에 대하여 평문의 모든 블록에 대한 유일한 암호문이 존재한다.

---

① CBC(Cipher Block Chaining Mode) ② CTR(Counter Mode)
③ CFB(Cipher-Feed Back Mode) ④ ECB(Electronic Code Book Mode)

♤ 대칭키 암호 운영모드

ECB 모드	• Electric CodeBook mode(전자 부호표 모드) • 가장 **단순**한 모드이다. 평문을 n개의 블록으로 분할한다. • 평문 블록과 암호문 블록이 일대일의 관계를 유지한다.**(짧은 메시지에 응용)** • 같은 내용을 가지는 평문 블록은 같은 암호문 블록으로 변환된다.

정답 : ④

3. 다음에서 설명하는 AES 운영모드는? [2022년 국회 9급]

◇ 블록단위로 동작한다.
◇ 각 블록을 병렬적으로 처리할 수 있다.
◇ 블록이 독립적으로 동작하여 한 블록에서의 에러가 다른 블록에 영향을 주지 않는다.

---

① CTR ② OFB ③ CFB ④ CBC ⑤ ECB

♤ 운영모드

모드	유형(type)	초기 벡터	오류 전파	암호 병행처리	복호 병행처리
ECB	**블록 암호**	필요 없음(none)	No	가능	가능
CBC	**블록 암호**	필요함(yes)	**Yes**	**불가**	가능
CFB	**비동기식** 스트림 암호	필요함(yes)	**Yes**	**불가**	가능
OFB	동기식 스트림 암호	필요함(yes)	No	**불가**	**불가**
CTR	동기식 스트림 암호	필요함 - 카운터	No	가능	가능

· 주어진 내용으로는 CTR도 정답이 될 수 있다.

정답 : ⑤