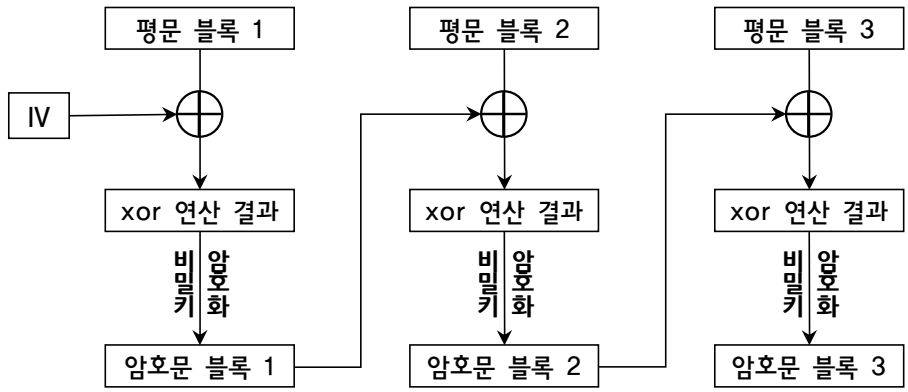
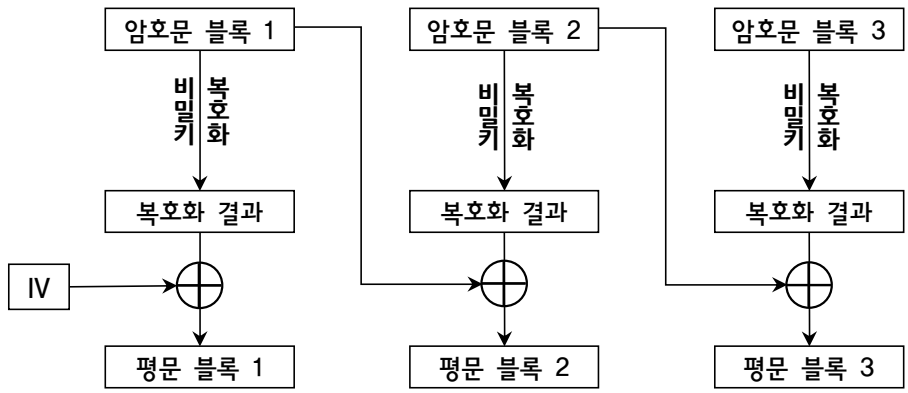
11. CBC 모드

CBC는 평문 블록과 이전 단계의 암호문 블록을 XOR 연산 후, **암호화**를 수행한다.

〈CBC 암호화 과정〉



〈CBC 복호화 과정〉



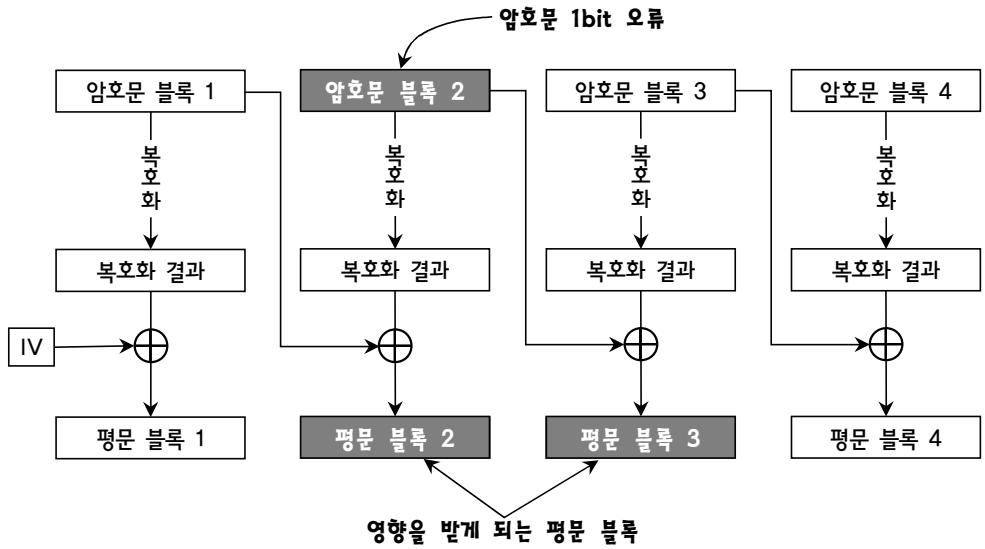
◈ CBC에서 평문과 암호문 사이의 관계

- 암호 : C_0 = IV, $C_i = E_K(P_i \oplus C_{i-1})$ → XOR 연산 후, 암호화를 수행
- 복호 : C_0 = IV, $P_i = D_K(C_i) \oplus C_{i-1}$

◈ CBC 모드 특징

- CBC는 각 블록을 병렬적으로 **암호** 처리할 수 없다.(블록 사이에 연관성이 존재하므로)
- 암호화된 블록은 전송되지만, 다음 블록 암호에 사용되므로 메모리에 저장되어야 한다.
- 초기 벡터 또는 평문의 첫 번째 블록 내용이 바뀌면 모든 암호문이 변경된다.
- 평문 블록 1과 2의 내용이 같아도 암호문 블록 1과 2의 내용은 반드시 같지는 않다.
- 정상적인 복호화를 위해서는 암호문 블록의 순서가 올바르게 배치되어 있어야 한다.

◈ n번째 암호문 블록이 전송 도중에 1비트 오류가 발생하면



- n, (n+1)번째 평문 블록은 정상적으로 복호화 불가, (n+2)번째부터는 정상적으로 복호화

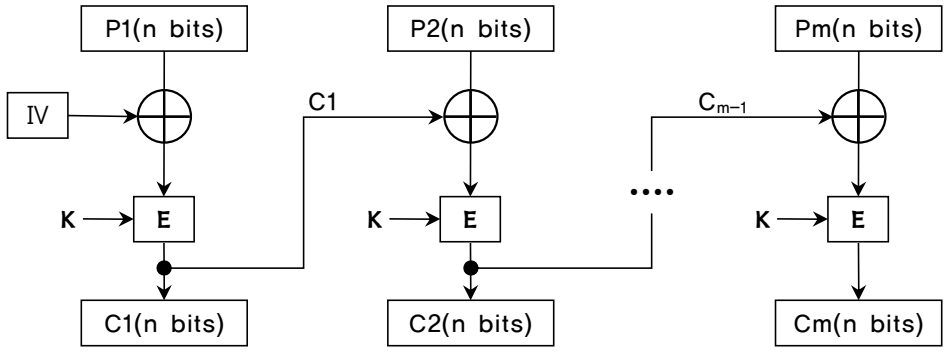
n번째 평문 블록	• n번째 평문 블록에서는 **대부분의 비트에서 오류** 발생 • 암호문 블록 2가 복호화에서 많은 변화를 거친 후 XOR 연산에 사용되므로 • 즉, 암호문 블록 2는 복호화 과정에서 혼돈과 확산을 거치게 된다.
(n+1)번째 평문 블록	• (n+1)번째 평문 블록에서는 **1비트 오류** 발생 • 암호문 블록 2가 단순하게 XOR 연산에만 사용되기 때문이다. • **오류 위치** : 관련 암호문의 오류 비트와 같은 위치에서 **1비트 오류** 발생

// 초기 벡터(IV, initialization vector)

- 첫 번째 평문 블록을 암호화할 때는 "이전 단계의 암호문 블록"이 없다.
- "이전 단계의 암호문 블록"을 대신할 허구의 블록이 필요하다. 이를 "초기 벡터"라 한다.
- 초기 벡터는 송수신자 사이에 **미리 약속**되어야 하지만, **반드시 비밀일 필요는 없다.**
- 하지만, 초기 벡터는 암호 안전성에 중요하므로 변조되면 안 되고, 비밀을 유지하는 것이 좋다.
- 초기 벡터는 통상적으로 암호화 때마다 랜덤 비트열을 사용한다.(예 : 타임스탬프를 초기 벡터로 사용)
- 만약, 초기 벡터의 비밀유지가 가능하면 송수신자 사이에 고정된 값을 사용해도 무방하다.

기출문제 분석

1. 다음의 블록 암호 운용모드는? [2019년 지방 9급]



E : 암호화 K : 암호화 키

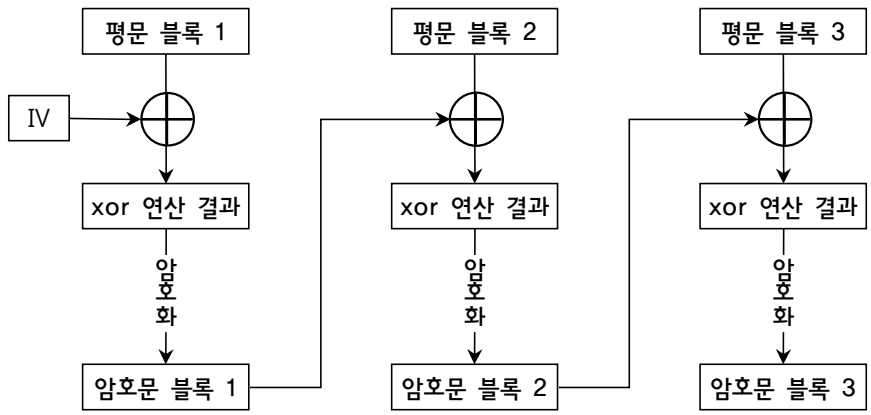
P1, P2, ... Pm : 평문 블록 C1, C2, ..., Cm : 암호 블록

IV : 초기 벡터 ⊕ : XOR

① 전자 코드북 모드(electronic code book mode)
② 암호 블록 연결 모드(cipher block chaining mode)
③ 암호 피드백 모드(cipher feedback mode)
④ 출력 피드백 모드(output feedback mode)

♤ CBC 모드

• CBC는 평문 블록과 이전 단계의 암호문 블록을 XOR 연산 후, 암호화를 수행한다.



정답 : ②

2. 대칭키 암호 운영모드로서 평문 블록 P1, P2, P3, …, Pn을 암호화하는 CBC(cipher block chaining) 모드에 대한 설명으로 옳은 것만을 〈보기〉에서 모두 고르면? [2020년 국회 9급]

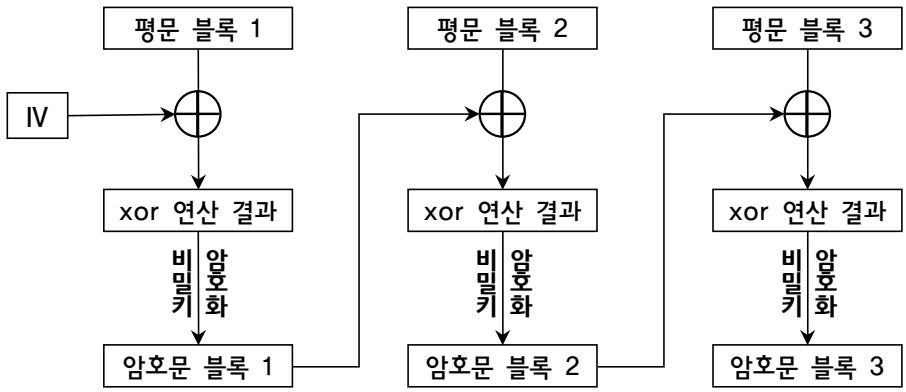
----<보기>----------

ㄱ. 평문이 달라지면 초기벡터는 매번 새롭게 랜덤으로 생성된다.
ㄴ. 평문 블록이 동일하면 대응하는 암호문 블록도 동일하다.
ㄷ. P2에 발생한 에러는 P2 블록 이후의 모든 암호화 과정에 파급된다.
ㄹ. 암호화 과정은 평문 블록 P1부터 Pn까지 순차적으로 진행된다.
ㅁ. 암호화 및 복호화를 하는데 암호화 알고리즘만 있어도 된다.

---

① ㄱ, ㄴ, ㄹ ② ㄱ, ㄴ, ㅁ ③ ㄱ, ㄷ, ㄹ
④ ㄴ, ㄷ, ㄹ ⑤ ㄷ, ㄹ, ㅁ

♤ CBC(cipher block chaining) 모드 암호화 과정



◈ CBC에서 평문과 암호문 사이의 관계

• 암호 : $C_0 = \text{IV},\ C_i = E_K(P_i \oplus C_{i-1})$ → XOR 연산 후, 암호화를 수행
• 복호 : $C_0 = \text{IV},\ P_i = D_K(C_i) \oplus C_{i-1}$ → 별도의 복호 알고리즘이 필요

◈ 초기 벡터(IV, initialization vector)

• "이전 단계의 암호문 블록"을 대신할 허구의 블록이 필요하다. 이를 "초기 벡터"라 한다.
• 초기 벡터는 통상적으로 암호화 때마다 **랜덤 비트열**을 사용한다.(예 : 타임스탬프를 초기 벡터로 사용)

ㄴ. 평문 블록이 동일하면 대응하는 암호문 블록도 동일하다.(×)
→ 평문 블록이 동일해도 대응하는 암호문 블록은 다르다. 이유는 **이전 암호문이 영향**을 끼치므로
ㅁ. 암호화 및 복호화를 하는데 암호화 알고리즘만 있어도 된다.(×)
→ CBC는 **복호화 알고리즘도 필요**하다.

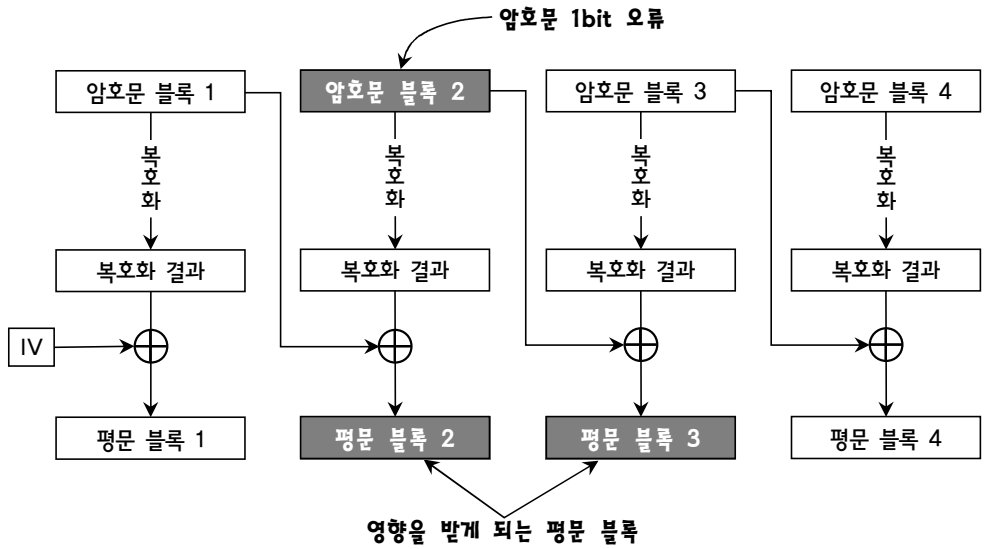
정답 : ③

3. 블록암호 운용모드에 대한 설명으로 옳지 않은 것은? [2020년 지방 9급]

① CFB는 블록 암호화를 병렬로 처리할 수 없다.
② ECB는 IV(Initalization Vector)를 사용하지 않는다.
③ CBC는 암호문 블록에 오류가 발생한 경우 복호화 시 해당 블록만 영향을 받는다.
④ CTR는 평문 블록마다 서로 다른 카운터 값을 사용하여 암호문 블록을 생성한다.

♤ **운용모드**

〈CBC에서 암호문 블록에 오류가 발생한 경우〉



• n번째 암호문 블록 오류 발생 : n, (n+1)번째 평문 블록은 정상적으로 복호화 불가

정답 : ③

4. 다음의 블록암호 모드 중 각 평문 블록을 이전 암호문 블록과 XOR한 후 암호화되어 안전성을 높이는 모드는? [2014년 서울 9급]

① ECB 모드 ② CBC 모드 ③ CTR 모드
④ OFB 모드 ⑤ CFB 모드

♤ **CBC 모드 – Cipher Block Chaining mode(암호 블록 연쇄 모드)**

• 평문 블록과 이전 단계의 암호문 블록을 XOR 연산 후, 암호화를 수행한다.

정답 : ②

5. 다음 중 Cipher Block Chaining 운용모드의 암호화 수식을 제대로 설명한 것은? (단, Pi는 i번째 평문 블록을, Ci는 i번째 암호문 블록을 의미한다) [2016년 서울 9급]

① $C_i = E_K(P_i)$

② $C_i = E_K(P_i \oplus C_{i-1})$

③ $C_i = E_K(C_{i-1}) \oplus P_i$

④ $C_i = E_K(P_i) \oplus C_{i-1}$

♤ CBC 모드

• 암호 : $C_i = E_K(P_i \oplus C_{i-1})$ → XOR 연산 후, 암호화를 수행

• 복호 : $P_i = D_K(C_i) \oplus C_{i-1}$ → 복호화를 수행 후, XOR 연산

정답 : ②