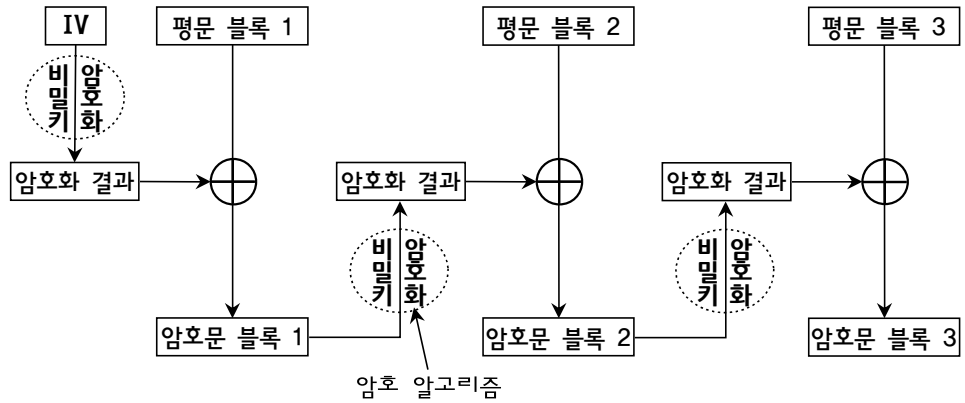
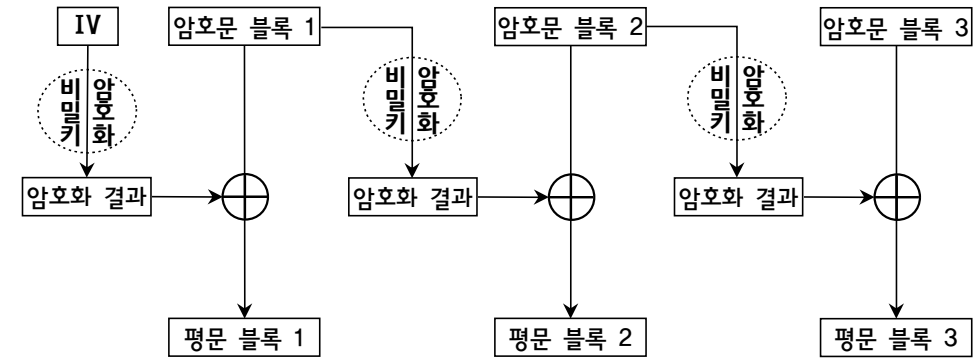
12. CFB 모드(암호문 피드백 모드)

이전 단계의 **암호문 블록(결과물)**을 암호 알고리즘의 **입력**으로 사용 - **피드백** 원리
다음은 CFB 모드에서 **평문**블록 크기와 **암호문**블록 **크기**가 **같은** 특별한 경우이다.

〈CFB 모드 암호화 과정(특별한 경우 - 단순)〉



〈CFB 모드 복호화 과정(특별한 경우 - 단순)〉



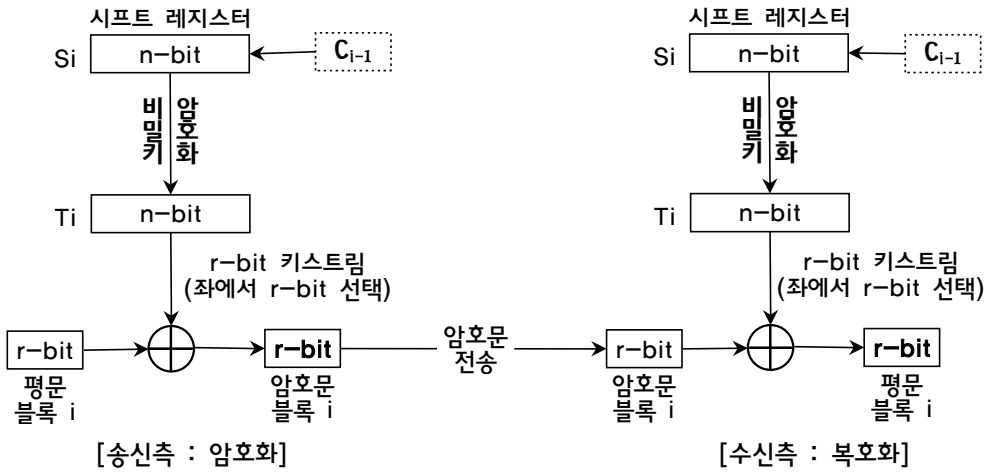
• CFB 모드는 복호화 과정에서 복호화를 하는 것이 아니고, "암호화"를 수행한다.(주의!)

◈ CFB에서 평문과 암호문 사이의 관계

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

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

◈ CFB 모드에서 i 번째 블록의 암복호화 과정(일반적인 경우 – 복잡)



- CFB 모드는 n-bit 시프트 레지스터 값(S)을 암복호화 한다.
  → 암복호화 결과는 n-bit가 된다.(Ti)
- 암호화 과정은 r-bit 평문 블록과 r-bit 시프트 레지스터를 xor 연산한다.
- 복호화 과정은 r-bit 암호문 블록과 r-bit 시프트 레지스터를 xor 연산한다.
- CFB는 키스트림이 이전 암호문에 의존하는 **비동기식 스트림 암호**이다.(그림 참조)
- CFB는 덧붙이기(paddding)가 필요하지 않다.
  → 이유는, 블록 크기 r-bit 단위로 적절하게 선택하여 암복호화를 하므로
- CFB는 암복호화 수행 전에 64 또는 128bit를 입력 받을 때까지 기다리지 않아도 된다.
- CFB는 작은 블록 크기(r-bit)의 데이터에 대해서도 암복호화가 가능하다.
  → 작은 크기의 데이터를 암복호화 하므로 ECB, CBC에 비해 처리 효율성이 낮다.
- CFB는 각 블록을 **병렬**적으로 **암호** 처리할 수 없다.(블록 사이에 연관성이 존재하므로)

◈ CFB에서 평문과 암호문 사이의 관계(구체적인 설명)

암호 : $C_i = P_i \oplus SelectLeft_r(E_K(ShiftLeft_r(S_{i-1}) | C_{i-1}))$

복호 : $P_i = C_i \oplus SelectLeft_r(E_K(ShiftLeft_r(S_{i-1}) | C_{i-1}))$

- $SelectLeft_r$은 입력값의 왼쪽 최상위 r-bit를 추출하는 함수이다.
- $ShiftLeft_r$은 입력값을 왼쪽으로 r-bit 이동시키는 함수이다.(왼쪽으로 r-bit는 제거된다)
- 연산자 |는 연접(concatenation)을 나타낸다.

탐구

암복호화 병렬처리

[질문] 블록암호 운영모드 중에서 ECB과 CTR은 암복호화 병렬처리가 되고, CBC와 CFB는 복호화만 병렬처리가 되는 걸로 알고 있습니다. 정확히 어떻게 되는지 궁금합니다.

〈CBC와 CFB의 복호화〉

- 암호문이 복호화 되기 위해서는 이전 암호문 블록과 현재 암호문 블록이 있어야 한다.
- 즉, CBC와 CFB의 복호화에는 2개의 암호문 블록이 있어야 평문을 복원할 수 있다.

↓복호화에서 2개의 암호문 블록이 필요한 이유

- **CBC** : 현재 암호문 블록을 복호화한 후에 이전 암호문 블록과 XOR 연산해서 평문을 구하므로
- **CFB** : 이전 암호문 블록을 복호화한 후에 현재 암호문 블록과 XOR 연산해서 평문을 구하므로

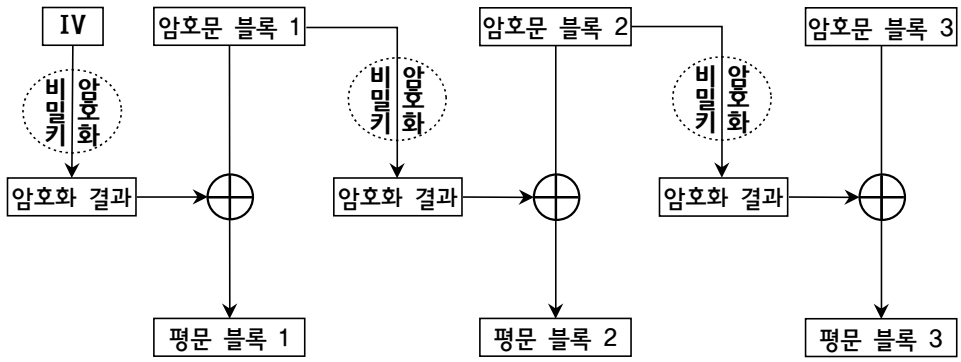
◈ **복호화에서 병행처리 기준**

- 만약, 복호화에서 병행처리 기준을 **엄격**하여 적용하여
- 모든 암호문 블록이 다른 블록과 전혀 연관없이 평문을 복원해야 하는 기준이면
- CBC와 CFB의 복호화는 병행처리라고 할 수 없다.

↓해서, 교재에 따라서

- CBC와 CFB의 복호화는 병행처리가 가능하다. 라고 하는 경우도 있고
- CBC와 CFB의 복호화는 병행처리가 아니다. 라고 하는 경우도 있다.

〈CFB 모드 복호화 과정〉



- **CFB** 모드에서 **평문 블록 2**가 복호화 되려면, **암호문 블록 1과 2**가 필요하다.

기출문제 분석

1. 블록암호(Block Cipher) 모드에 대한 설명으로 옳지 않은 것은? [2019년 국회 9급]

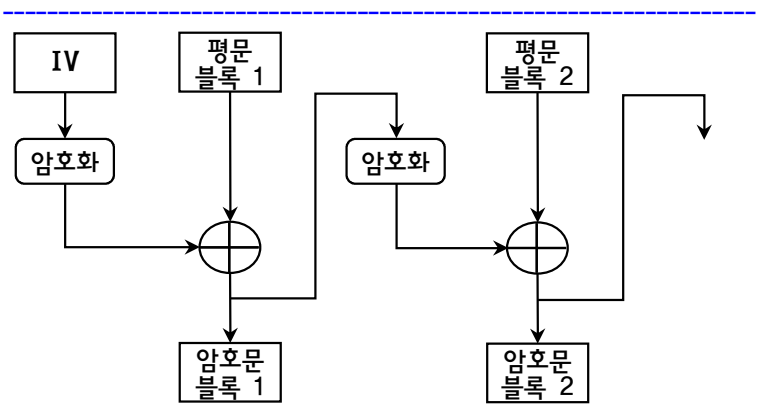
① ECB(Electronic CodeBook) 모드는 평문 블록을 암호화한 것이 그대로 암호문 블록이 된다.
② CBC(Cipher Block Chaining) 모드는 암호화 전에 XOR 연산을 수행한다.
③ CFB(Cipher FeedBack) 모드는 평문 블록을 암호 알고리즘으로 직접 암호화한다.
④ OFB(Output FeedBack) 모드는 암호 알고리즘의 출력을 암호 알고리즘의 입력으로 피드백한다.
⑤ CTR(CounTeR) 모드는 스트림 암호의 일종으로 카운터의 값이 암호화의 입력이 된다.

♤ CFB(Cipher FeedBack) 모드

• CFB 모드는 암호문 블록을 암호 알고리즘으로 직접 암호화한다.

정답 : ③

2. 다음 그림이 나타내는 블록암호 운용모드는? [2015년 국회 9급]



① ECB ② CBC ③ CFB ④ OFB ⑤ CTR

♤ CFB(Cipher-FeedBack mode) : 암호 피드백 모드

• 이전 단계의 **암호문 블록(결과물)**을 암호 알고리즘의 **입력**으로 사용 - 피드백 원리

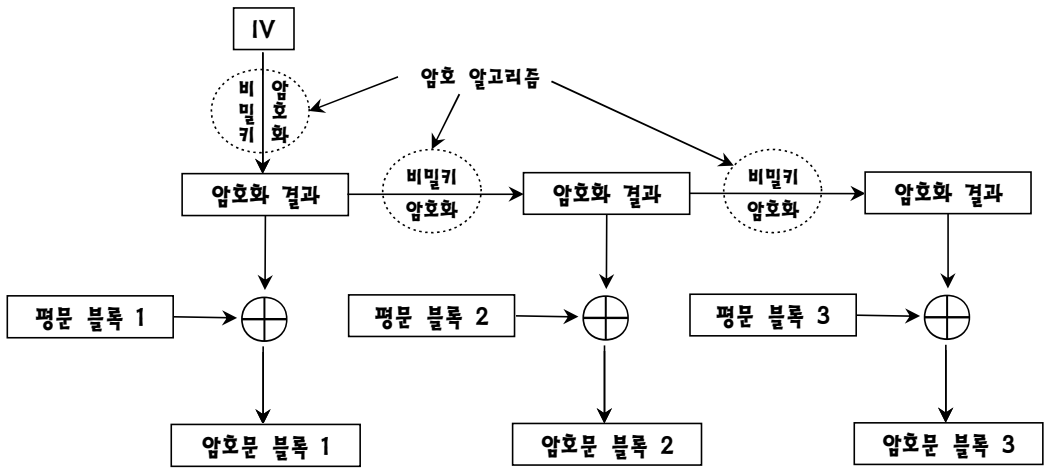
정답 : ③

3. 키 k에 대한 블록암호 알고리즘 E_k, 평문블록 M_i, Z_0는 초기벡터, $Z_i = E_k(Z_i - 1)$가 주어진 경우, 이때 i=1, 2, ..., n에 대해 암호블록 C_i를 $C_i = Z_i \oplus M_i$로 계산하는 운영모드는? (단, $\oplus$는 배타적 논리합이다) [2020년 국가 9급]

① CBC ② ECB ③ OFB ④ CTR

♤ 운영모드 – OFB

〈OFB 모드 암호화 과정〉



• 암호 : $C_i = Z_i \oplus M_i = E_k(Z_i - 1) \oplus M_i$ → 암호 알고리즘의 출력 결과를 평문블록과 XOR 연산

정답 : ③

탐구

왜? CFB 모드에서는 복호화 단계에서 암호화를 하는가?

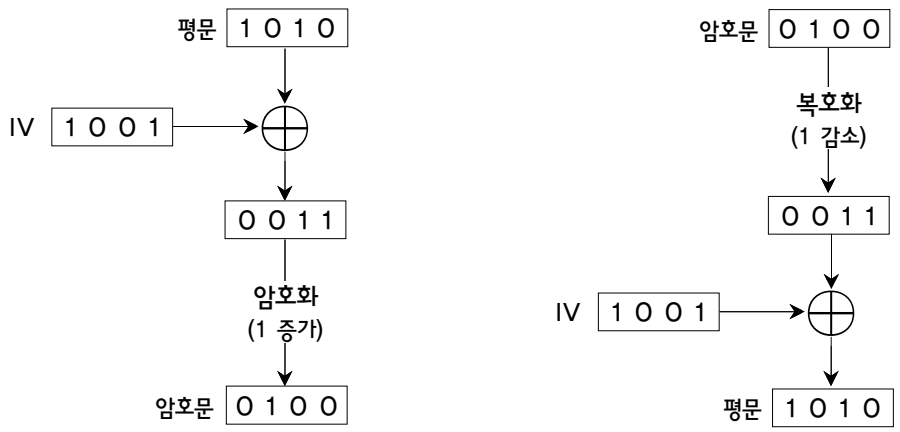
먼저, CBC 모드와 CFB 모드를 비교하면 다음과 같다.

- CBC 모드는 암호화 단계에서는 암호화를 하고, 복호화 단계에서는 복호화를 한다.
- CFB 모드는 암호화 단계에서는 암호화를 하고, **복호화 단계에서도 암호화**를 한다.
- 왜? CFB 모드에서는 복호화 단계에서 복호화를 하지 않고, 암호화를 하는가?

[가정] 암호화 및 복호화 과정을 단순히 다음과 같다고 가정하고 설명하기로 한다.

- 암호화는 암호화 대상을 1 증가시키고
- 복호화는 복호화 대상을 1 감소시키는 것으로 약속한다.

◈ CBC 모드



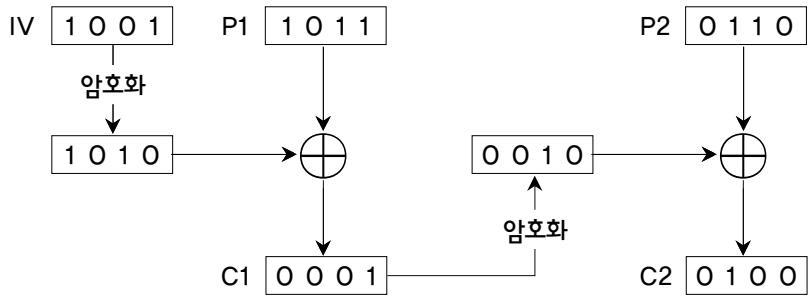
- CBC는 암호화 단계에서는 암호화, 복호화 단계에서는 복호화를 하므로 쉽게 이해한다.

◈ CFB 모드

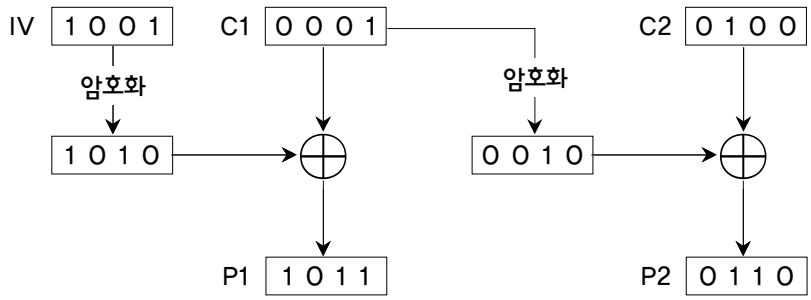
다음은 CFB 모드의 암호화 / 복호화 과정이다.
암호화는 **대상을 1 증가**시키고, 복호화는 **대상을 1 감소**시키는 것으로 **가정**한다.

---

① CFB 모드 암호화



② CFB 모드 복호화



(주) P_i는 평문, C_i는 암호문을 의미한다.

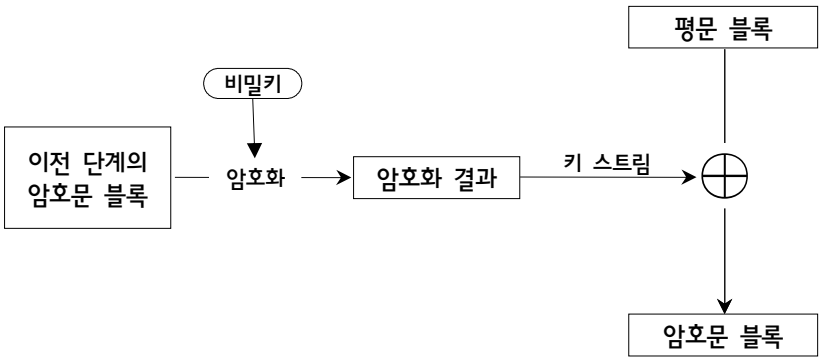
• CFB 모드는 암호화 단계에서는 암호화를 하고, **복호화 단계에서도 암호화**를 한다.
→ 평문을 암호화한 결과와 XOR 연산을 실시하기 때문이다.(이해가 되는지?)
→ 주어진 그림을 잘 분석하기 바란다.

[정리] CFB, OFB, CTR 모드에서는 **복호화 단계에서도 암호화**를 실시한다.(분석이 필요)
→ ECB, CBC 모드에서는 복호화 단계에서는 복호화를 한다.(당연)

탐구

CFB 모드와 스트림 암호

다음은 CFB 모드에 의한 암호화에서 중간 과정이다.



① CFB 모드에서 암호문 블록은 "평문 블록과 암호 알고리즘의 출력 결과"를 XOR 연산해서 생성된다.
→ 이전 출력물인 "암호문 블록"이 암호 알고리즘으로의 입력으로 피드백하므로 "암호 피드백 모드"라 한다.

② 즉, 이전 단계에서 암호화된 문자열이 다시 암호화되어 키 스트림으로 사용되고 있다.
→ 키 스트림(key steam)은 "키 수열"이라고도 한다.

③ 결과적으로, CFB 모드 원리는 스트림 암호 원리와 유사하다.
→ 스트림 암호에서 "자기 동기식 스트림 암호"라 한다.

④ 스트림 암호에서는 "평문과 난수열"을 XOR 연산해서 암호문을 생성한다.

⑤ CFB 모드와 스트림 암호를 비교해보면, CFB 모드의 "암호 알고리즘의 출력 결과"가 스트림 암호의 "난수열"에 대응된다.
→ 여기서, 암호 알고리즘의 출력 결과는 계산에 의한 것이지 난수는 아니다
→ 따라서, CFB 모드는 이론적으로 해독 불가능한 것은 아니다.