알기 쉬운

정보보호개론 3판

흥미로운 암호 기술의 세계

INFORMATION SECURITY and CRYPTOGRAPHY

INFINITYBOOKS
인피니티북스

CHAPTER 5 블록 암호 모드

Section 01
블록 암호 모드

1.1 블록 암호와 스트림 암호

1.2 모드란?

1.3 평문 블록과 암호문 블록

1.4 적극적인 공격자 맬로리

1.1 블록 암호와 스트림 암호

- **블록 암호(block cipher)**
  - 어느 특정 비트 수의「집합」을 한 번에 처리하는 암호 알고리즘
  - 이「집합」을 **블록(block)**
  - 블록의 비트 수를 **블록 길이(block length)**
    - DES나 트리플 DES의 블록 길이는 64비트
    - DES: 64비트 평문, 64비트 암호문
    - AES: 블록 길이는 128비트, 128비트 암호문

Quiz 1 비트와 바이트

- 8비트를 1바이트라고 한다. 그러면 128 비트 블록은 몇 바이트인가?

1.1 블록 암호와 스트림 암호

- **스트림 암호(stream cipher)**는 데이터의 흐름(스트림)을 순차적으로 처리해 가는 암호 알고리즘
- 1비트, 8비트, 혹은 32비트 등의 단위로 암호화와 복호화

1.2 모드란?

- 모드란:
  - 긴 평문을 블록으로 나누어 암호화
  - 각 블록에 암호 알고리즘을 반복해서 사용하여 긴 평문 전체를 암호화

블록암호 주요 모드

- ECB 모드 : Electric CodeBook mode(전자 부호표 모드)
- CBC 모드 : Cipher Block Chaining mode(암호 블록 연쇄 모드)
- CFB 모드 : Cipher-FeedBack mode(암호 피드백 모드)
- OFB 모드 : Output-FeedBack mode(출력 피드백 모드)
- CTR 모드 : CounTeR mode(카운터 모드)

1.3 평문 블록과 암호문 블록

- 평문 블록 : 블록 암호 알고리즘에서 암호화 대상이 되는 평문
  평문 블록의 길이는 블록 암호 알고리즘의 블록의 길이와 같다.
- 암호문 블록 : 블록 암호 알고리즘을 써서 평문 블록 암호를 암호화한 암호문

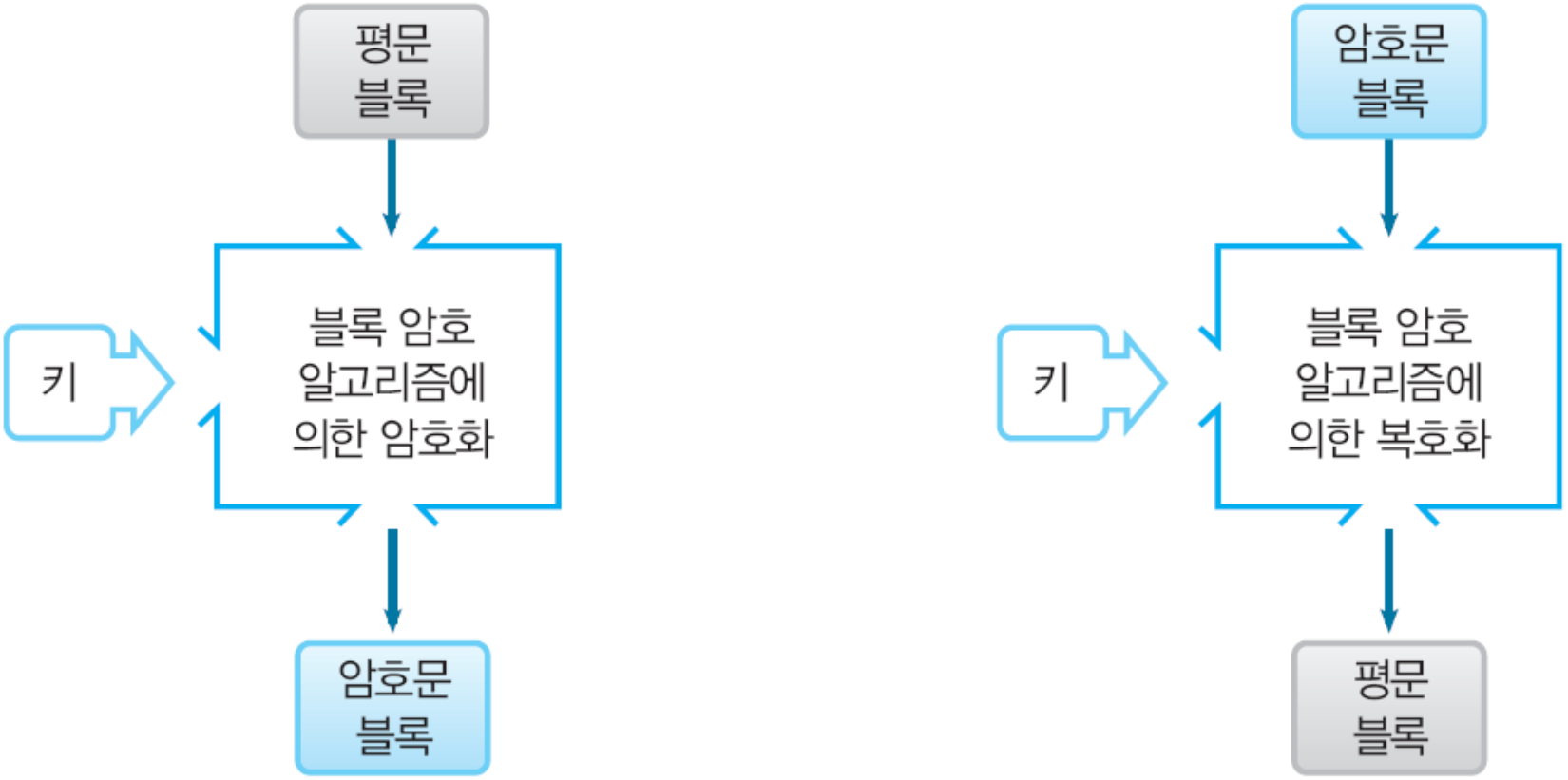


그림 5-1 • 평문 블록과 암호문 블록

1.4 적극적 공격자 맬로리

- 도청
- 위장
- 변조
- 공격자: **맬로리**(Mallory)

Section 02
ECB 모드

2.1 ECB 모드란?

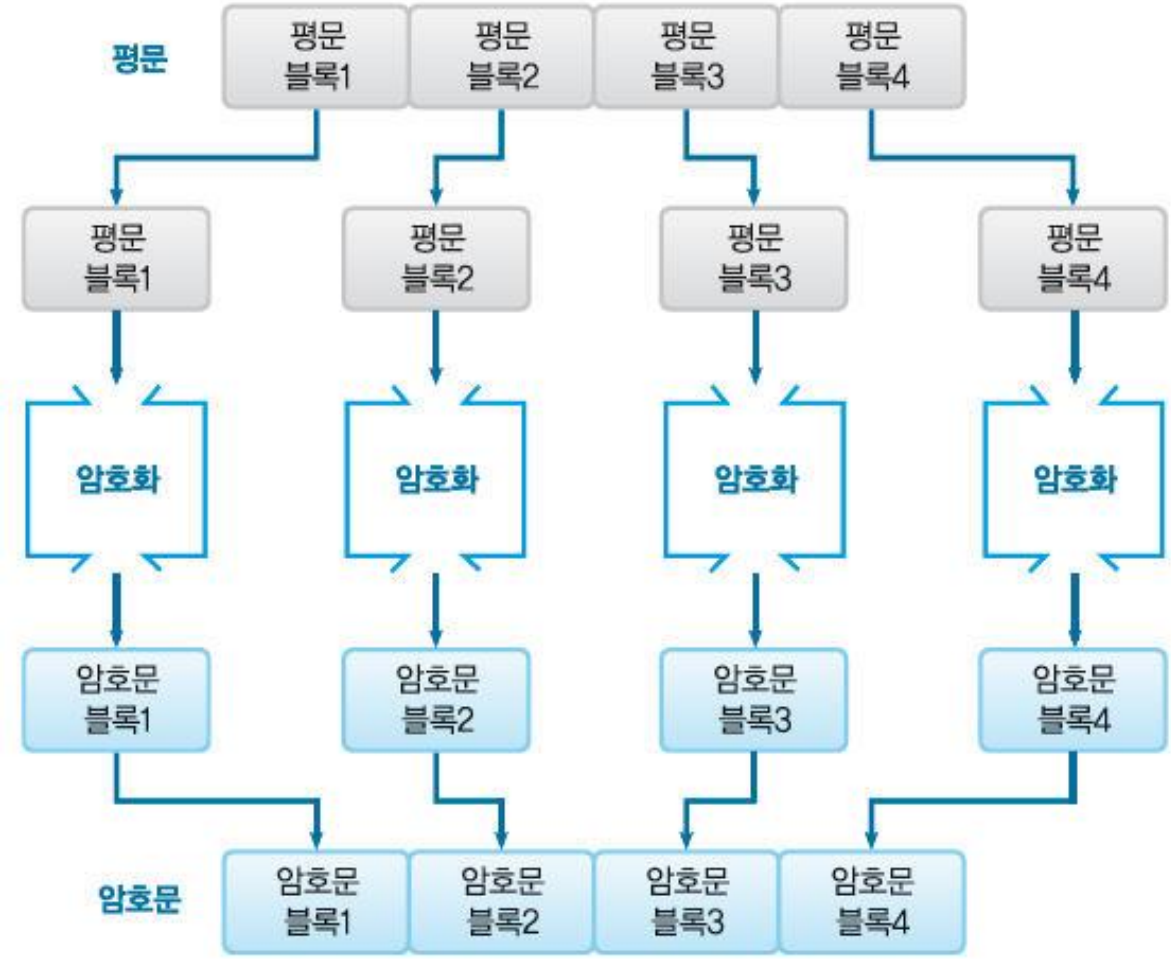
2.2 ECB 모드의 특징

2.3 ECB 모드에 대한 공격

2.1 ECB 모드란?

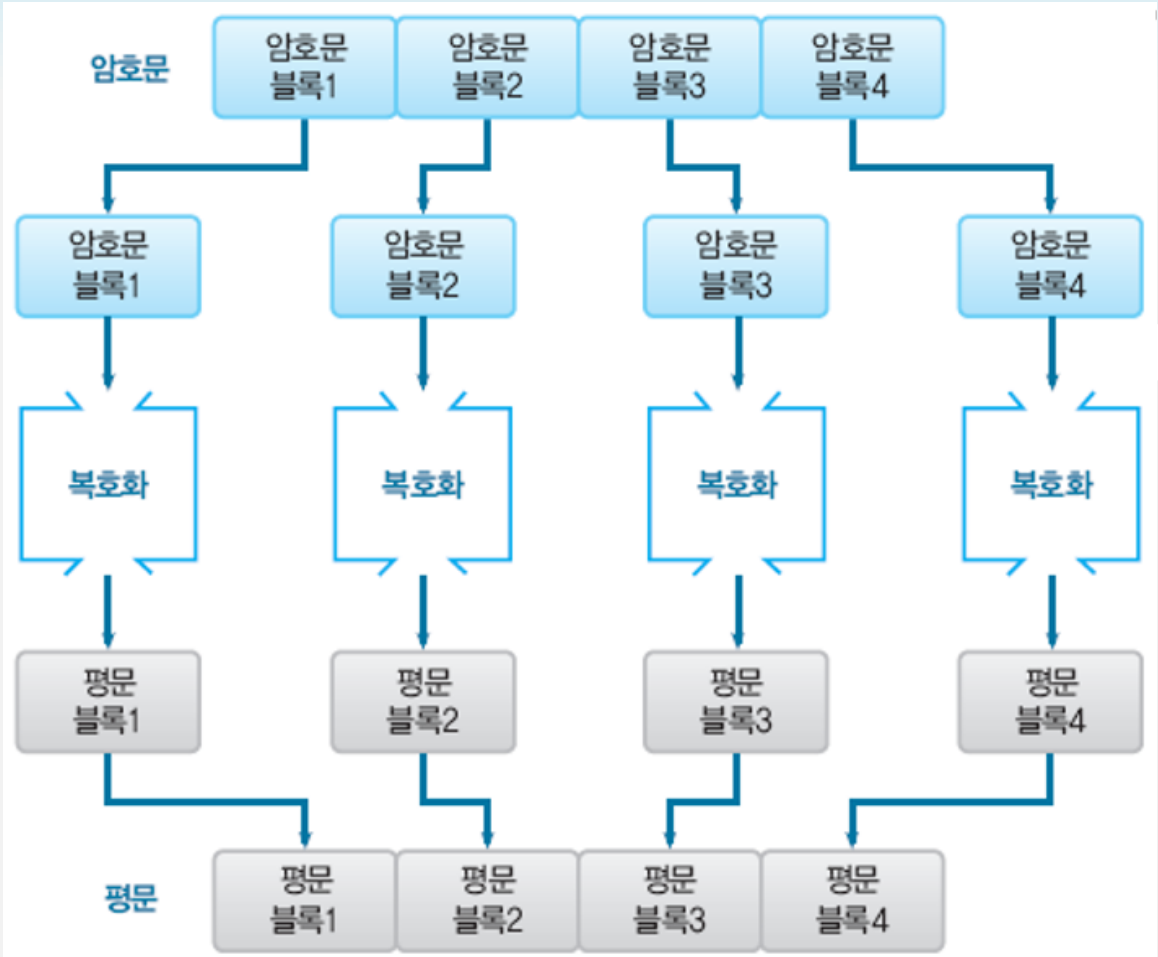
- 평문 블록을 암호화한 것이 그대로 암호문 블록
- **패딩**(padding)
  - 마지막 평문 블록이 블록 길이에 미치지 못할 경우에 추가하여 블록 길이가 되도록 맞춤
  - 안전하지 않음

ECB 모드에 의한 암호화



(a) ECB 모드에 의한 암호화

ECB 모드에 의한 복호화



(b) ECB 모드에 의한 복호화

그림 5-2 • ECB 모드(전자 코드북 모드)

2.2 ECB 모드의 특징

- 가장 기밀성이 낮은 모드
- 평문 블록과 암호문 블록이 일대일 관계
- 암호문을 살펴보는 것만으로도 평문 속에 패턴 반복성 감지
  - 평문 속에 같은 값을 갖는 평문 블록이 여러 개 존재하면 그 평문 블록은 동일한 암호문 블록으로 변환
- 안전하지 않다

2.3 ECB 모드에 대한 공격

- 어느 은행의 송금 의뢰 데이터가 다음 3개의 블록으로 구성
  - 블록1 = 송금자의 은행계좌번호
  - 블록2 = 수신자의 은행계좌번호
  - 블록3 = 송금액
- 송금 의뢰 데이터를 받은 은행은 지정된 금액을 송금자로부터 수신자의 계좌로 이동
- A-5374의 계좌로부터 B-6671의 계좌로 1억 원을 송금하라는 송금 의뢰 데이터를 만들어보자

예 : 평문과 암호문

- 평문 블록1 = 41 2D 35 33 37 34 20 20 20 20 20 20 20 20 20 20 (송금자:A-5374)
- 평문 블록2 = 42 2D 36 36 37 31 20 20 20 20 20 20 20 20 20 20 (수신자:B-6671)
- 평문 블록3 = 31 30 30 30 30 30 30 30 30 20 20 20 20 20 20 20 (송금액:100000000)

- 암호화 하자
  - 암호문 블록1 = 59 7D DE CC EF EC BA 9B BF 83 99 CF 60 D2 59 B9 (송금자:????)
  - 암호문 블록2 = DF 49 2A 1C 14 8E 18 B6 53 1F 38 BD 5A A9 D7 D7 (수신자 :????)
  - 암호문 블록3 = CD AF D5 9E 39 FE FD 6D 64 8B CC CB 52 56 8D 79 (송금액:????)

예 : 맬로리의 공격

- 공격자 맬로리가 암호문 블록의 1과 2의 내용을 바꾼다
  - 암호문 블록1 = DF 49 2A 1C 14 8E 18 B6 53 1F 38 BD 5A A9 D7 D7 (송금자:????)
  - 암호문 블록2 = 59 7D DE CC EF EC BA 9B BF 83 99 CF 60 D2 59 B9 (수신자 :????)
  - 암호문 블록3 = CD AF D5 9E 39 FE FD 6D 64 8B CC CB 52 56 8D 79 (송금액:????)
- 은행이 이것을 복호화 하면 다음과 같이 된다
  - 평문 블록1 = 42 2D 36 36 37 31 20 20 20 20 20 20 20 20 20 20 (송금자:B-6671)
  - 평문 블록2 = 41 2D 35 33 37 34 20 20 20 20 20 20 20 20 20 20 (수신자:A-5374)
  - 평문 블록3 = 31 30 30 30 30 30 30 30 30 20 20 20 20 20 20 20 (송금액:100000000)

예 : 맬로리의 공격 결과

- 원래는 A-5374의 계좌에서 B-6671의 계좌로 1억 원을 송금하라는 지시였는데 B-6671의 계좌에서 A-5374의 계좌로 1억 원을 송금하라는 정반대의 지시가 되어 버림
- 암호문을 해독하지 않고 평문 조작 가능

예 : 맬로리가 할 수 있는 공격

- 암호문 블록의 순서 변경
- 암호문 블록 삭제
- 암호문 블록 복제

Quiz 2 ECB 모드에 대한 공격

- 지금 당신이 적극적인 공격자 맬로리라고 하자. 어떤 컴퓨터 시스템의 패스워드 파일이 아래와 같이 ECB 모드로 암호화되어 있다는 것을 알았다고 해보자.

암호문 블록 1= 1D C1 6A 10 8D 52 2E 04 01 D4 B5 53 47 D6 E0 36 (사용자 1의 이름)
암호문 블록 2= AA DE F1 DF 96 79 8D 22 4F 65 B8 49 9E 11 3E 0D (사용자 1의 패스워드)
암호문 블록 3= 8E D0 E3 40 91 6C E7 75 E2 8E 83 BE 29 E8 3D 56 (사용자 2의 이름)
암호문 블록 4= 1E 96 43 46 C0 71 91 74 F4 97 D9 5E 1B 02 68 F7(사용자 2의 패스워드)
암호문 블록 5= 4A 35 8D D8 A2 CF 86 99 5B B1 A1 26 9C A7 59 06(사용자 3의 이름)
암호문 블록 6= 65 27 28 03 55 C0 BA 7A 8C CF C6 99 95 FB 12 5B(사용자 3의 패스워드)

이 암호화된 패스워드 파일을 어떻게 바꿔 쓰면 이 컴퓨터 시스템을 공격할 수 있는가?

Section 03
CBC 모드

3.1 CBC 모드란?

3.2 초기화 벡터

3.3 CBC 모드의 특징

3.4 CBC 모드에 대한 공격

3.5 패딩 오라클 공격

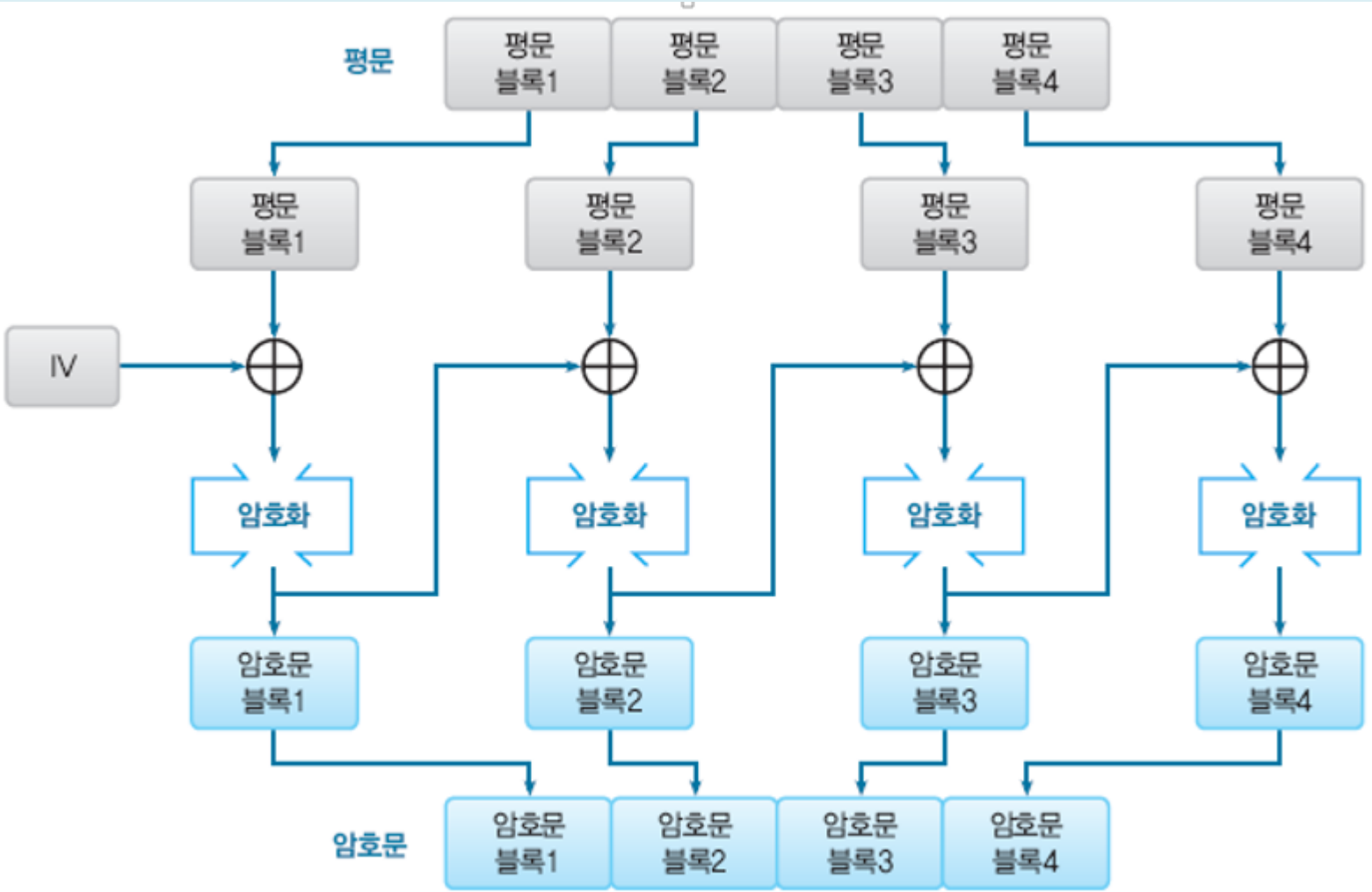
3.6 초기화 벡터(IV) 공격

3.7 CBC 모드 활용의 예

3.1 CBC 모드란?

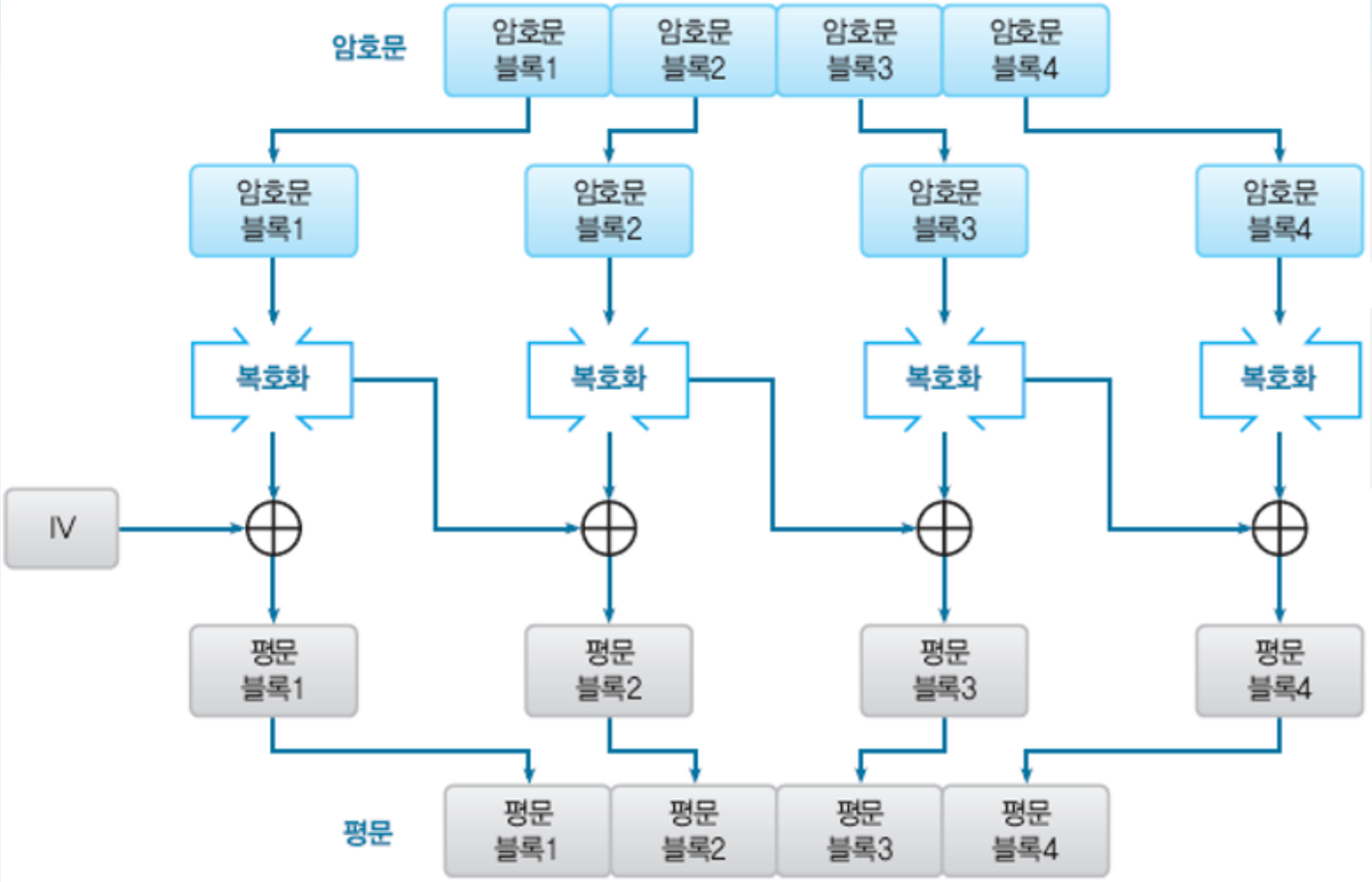
- **CBC 모드**
  - Cipher Block Chaining 모드(암호 블록 연쇄 모드)의 약자이다. 암호문 블록을 마치 체인처럼 연결시키기 때문에 붙여진 이름
  - CBC 모드에서는 1 단계 앞에서 수행되어 결과로 출력된 암호문 블록에 평문 블록을 XOR 하고 나서 암호화를 수행
  - 각각의 암호문 블록은 단지 현재 평문 블록 뿐만 아니라 그 이전의 평문 블록들의 영향도 받게 됨

CBC 모드에 의한 암호화



(a) CBC 모드에 의한 암호화

CBC 모드에 의한 복호화



(b) CBC 모드에 의한 복호화

그림 5-3 • CBC 모드(암호 블록 체이닝 모드)

3.2 초기화 벡터

- **초기화 벡터(initialization vector)**
  - 최초의 평문 블록을 암호화할 때는「1 단계 앞의 암호문 블록」이 존재하지 않으므로 「1 단계 앞의 암호문 블록」을 대신할 비트열인 한 개의 블록을 준비할 필요

Quiz 3 CBC 모드의 초기화 벡터

- CBC모드에서 항상 같은 값의 초기화 벡터를 사용했다고 가정해보자. 이 경우 암호 해독자에게 어떤 단서를 주게 되는 것일까?

3.3 CBC 모드의 특징

- 평문 블록은 반드시 「1 단계 앞의 암호문 블록」과 XOR을 취하고 나서 암호화
  - 따라서 만약 평문 블록1과 2의 값이 같은 경우라도 암호문 블록1과 2의 값이 같아진다고는 할 수 없고, ECB 모드가 갖고 있는 결점이 CBC 모드에는 없다.
- 암호문 블록3을 만들고 싶다면 적어도 평문 블록의 1, 2, 3까지가 갖추어져 있어야만 함

ECB 모드와 CBC 모드

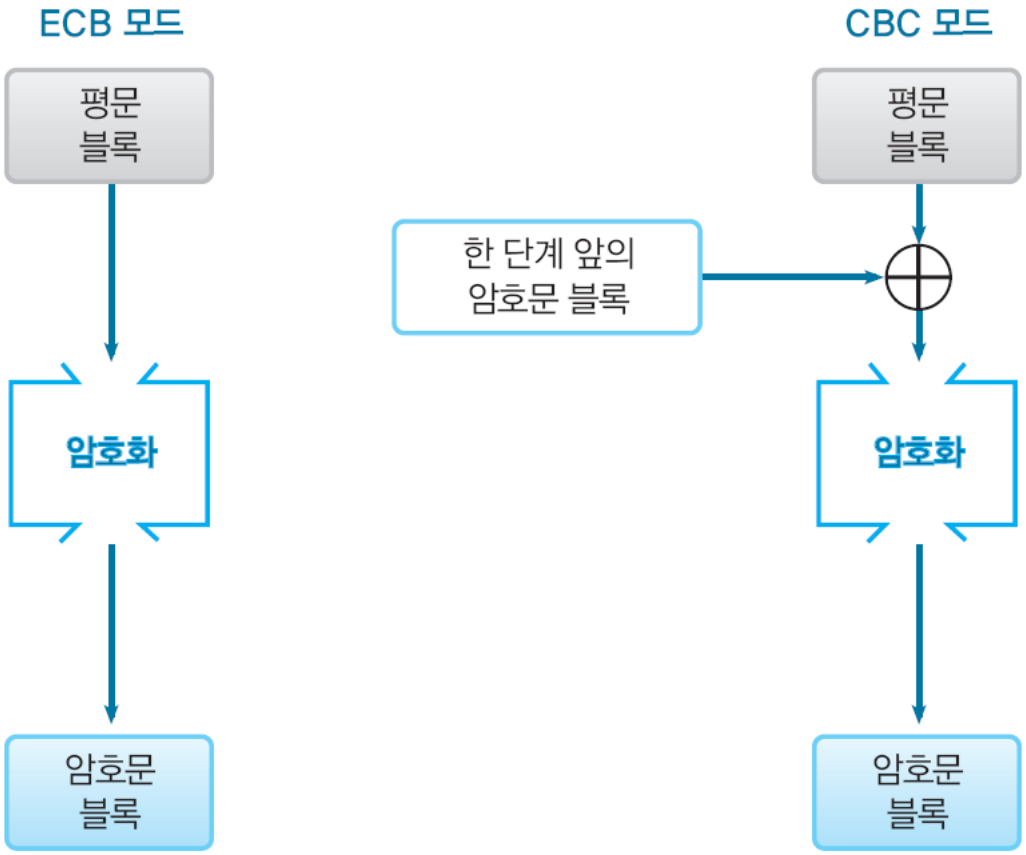


그림 5-4 • ECB 모드와 CBC 모드의 비교

깨진 암호문

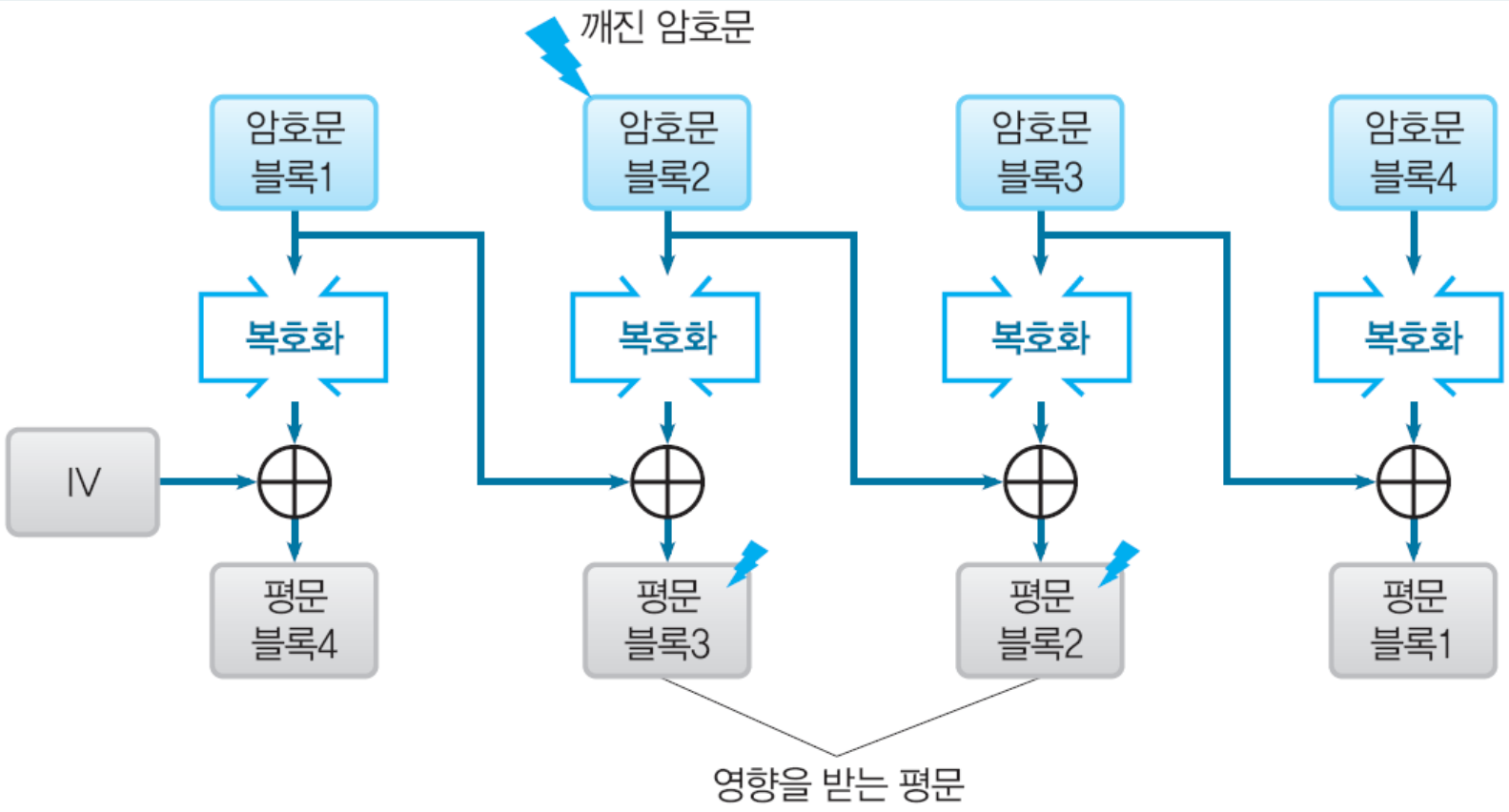


그림 5-5 • CBC 모드에서 암호문 블록이 파손되면 2개의 평문 블록에 영향을 미친다

암호문 블록에서 비트 누락

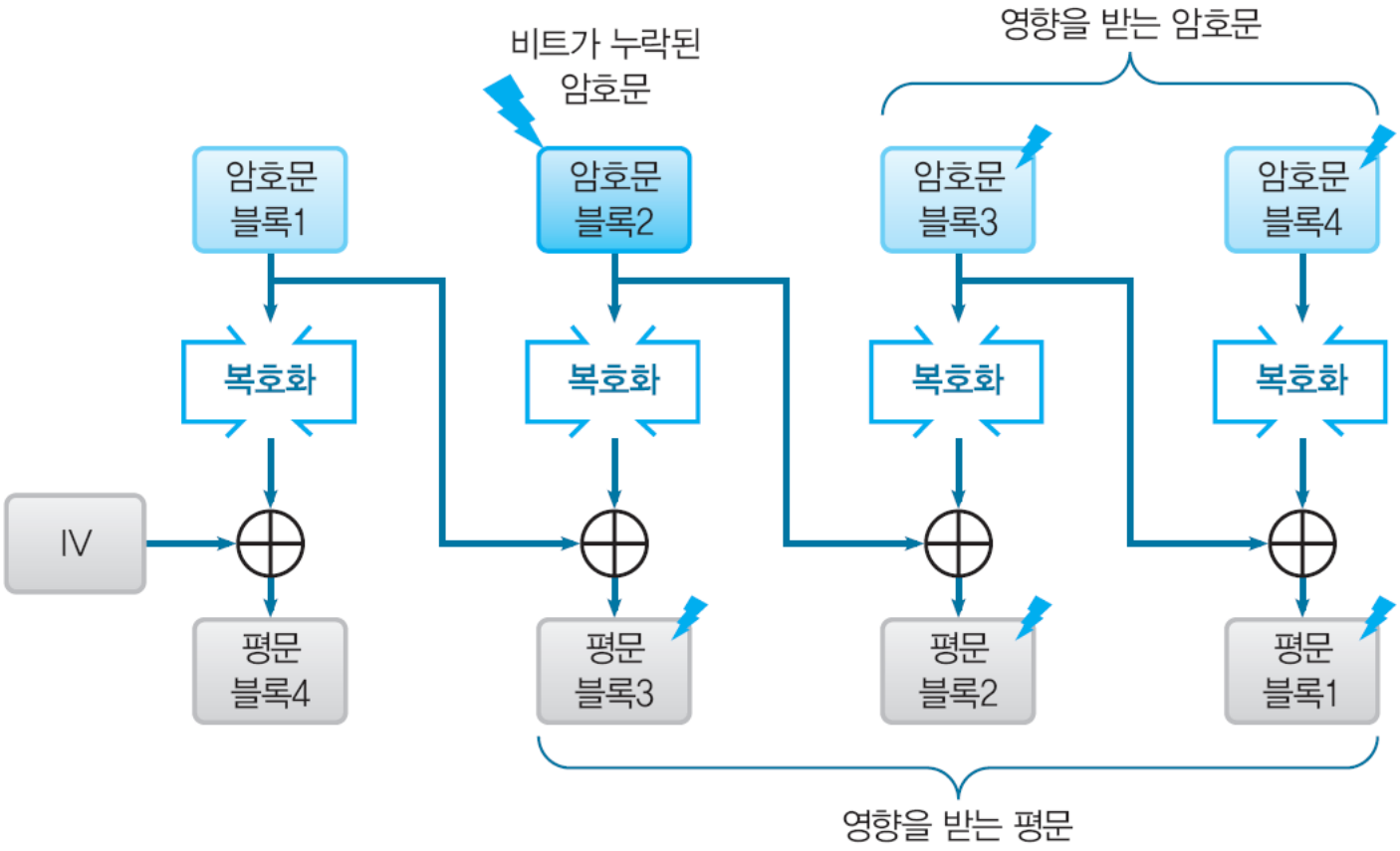


그림 5-6 • CBC 모드에서 암호문 블록에서 비트 누락이 생기면 그 이후의 평문 블록 전체에 영향을 미친다

3.4 CBC 모드에 대한 공격

- 초기화 벡터에 대한 공격
  - 맬로리가 초기화 벡터의 임의의 비트를 반전(1이라면 0, 0 이라면 1로)시킬 수 있다면, 암호블록1에 대응하는 평문 블록1(복호화되어 얻어지는 평문 블록)의 비트를 반전시킬 수 있다.

CBC 모드 초기화 벡터 비트반전

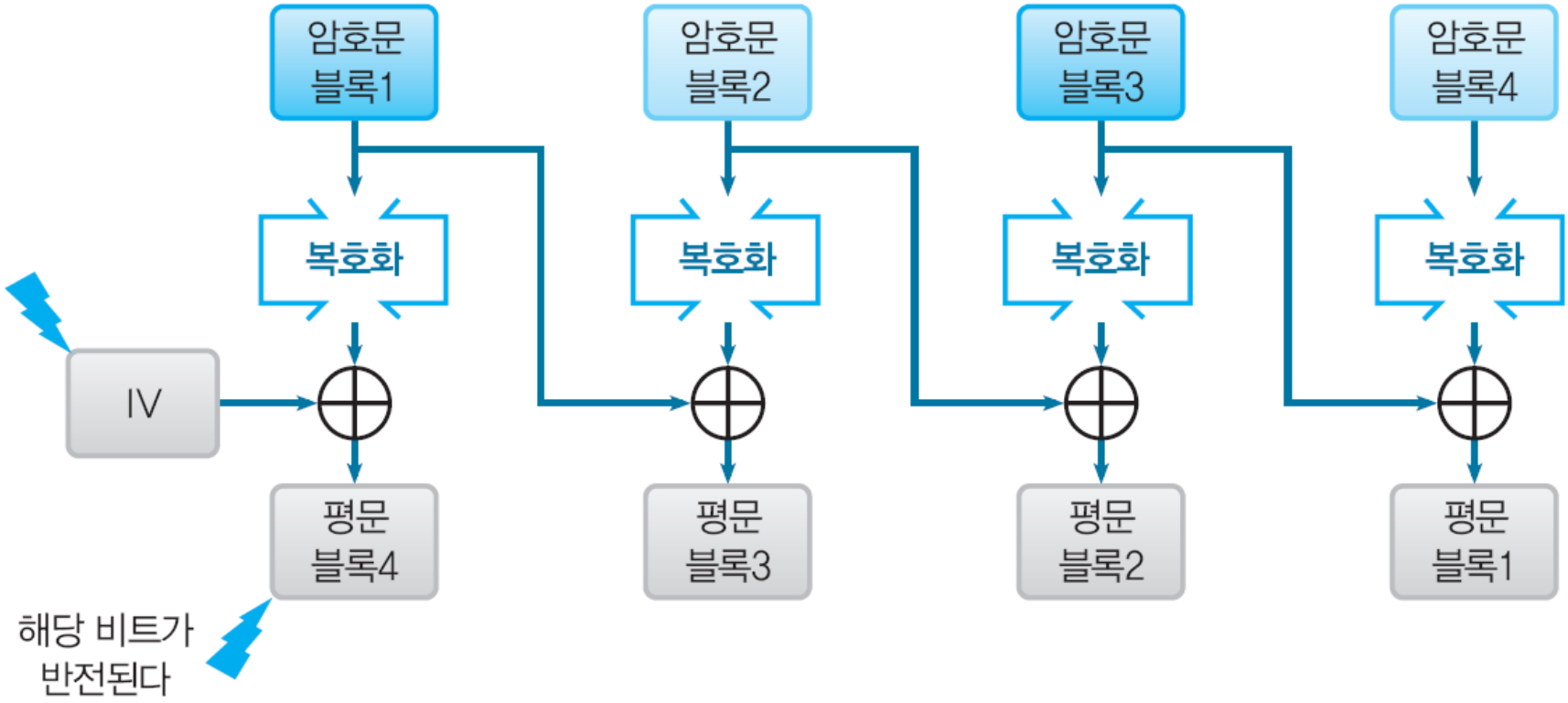


그림 5-7 • CBC 모드에 대한 공격(초기화 벡터의 비트 반전)

3.5 패딩 오라클 공격

- 블록 암호의 패딩을 이용한 공격
- 패딩 내용을 조금씩 변화시켜 암호문을 여러 차례 송신
- 수신자가 올바로 복호화 하지 못할 경우 오류를 관찰하여 평문 정보를 취득
- 패딩을 사용하는 모든 모드에 적용
- 2014 년 SSL3.0 에 대 한 POODLE(Padding Oracle on Downloaded Legacy Encryption) 공격

3.6 초기화 벡터(IV) 공격

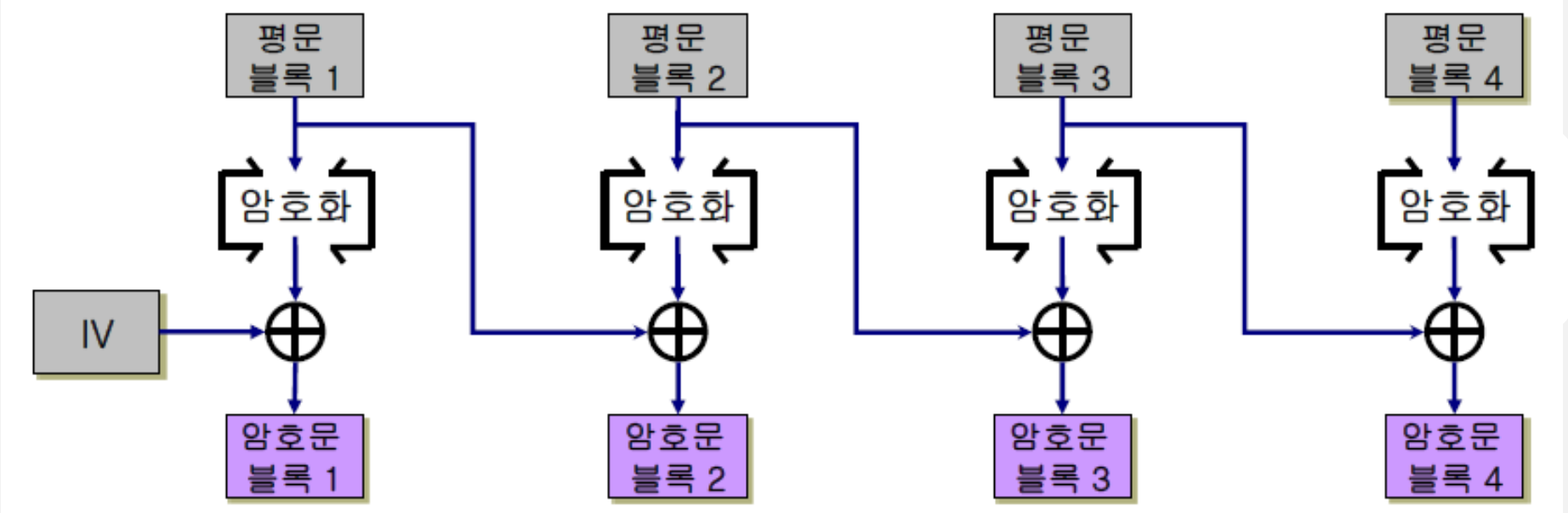
- 초기화 벡터는 난수(Random Number)로 부여
- SSL/TLS의 TLS 버전 1.0
  - 초기화 벡터를 이전 CBC 모드로 암호화한 마지막 블록을 사용
  - 문제점 발견 후 TLS 버전 1.1 부터는 초기화 벡터를 명시적으로 부여

3.7 CBC 모드 활용 예

- SSL/TLS:
  - 통신기밀성 보호
- 3DES-EDE-CBC
- AES-256-CBC:
  - 키 길이가 256비트인 경우

Quiz 4 CBC 모드 비슷한 것

CBC 모드 이야기를 들은 앨리스는 CBC모드와 아주 비슷한 모드를 생각해냈다. 이 모드는 어떤 성질을 가지고 있는가?



칼럼 (CTS 모드)

- CTS(Cipher Text Stealing) 모드
- 마지막 블록 한 단계 전의 암호화 블록을 패딩으로 대신 이용
- ECB나 CBC 모드와 조합해 사용
- 마지막 블록을 송신하는 순서를 변경하는 변형된 형태로도 운영
- CBC-CS1, CBC-CS2, CBC-CS3

CTS 모드 암호화

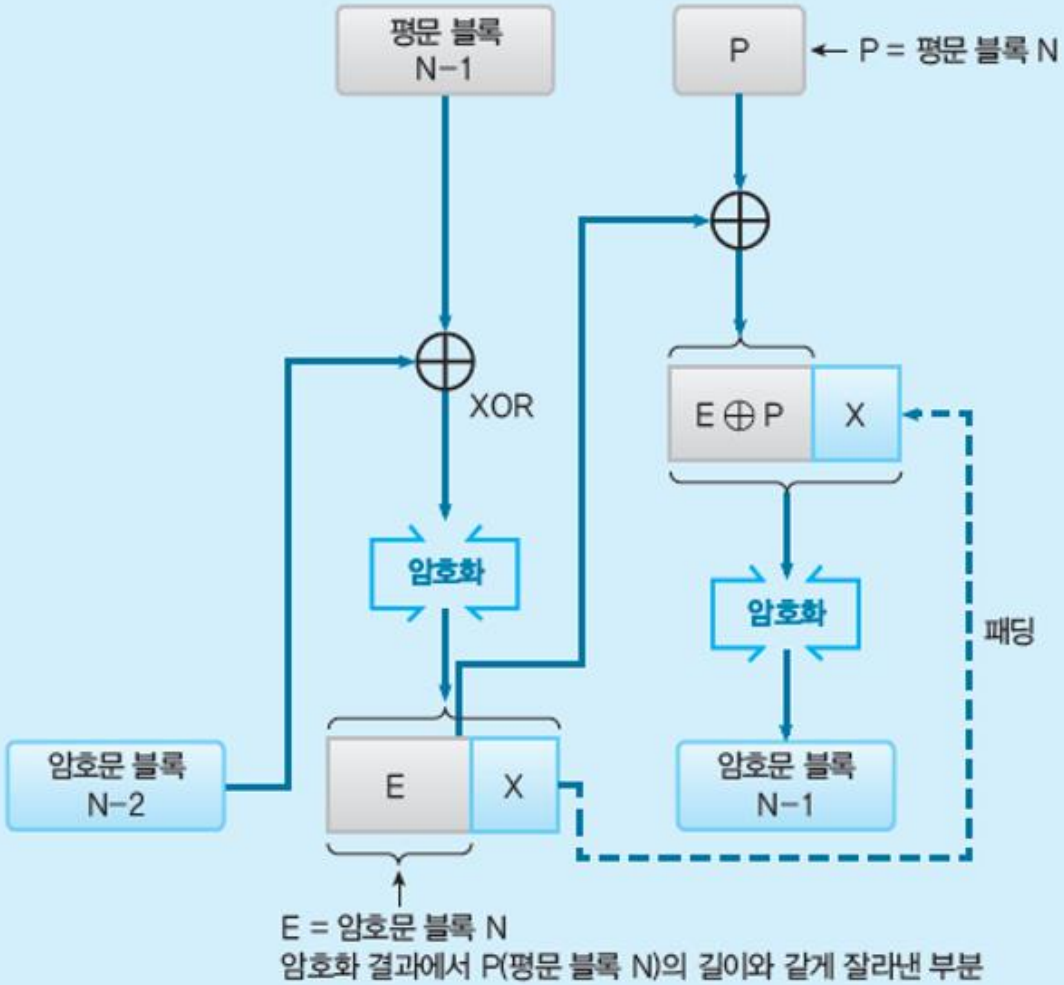


그림 5-C1 • CTS 모드 암호화

CTS 모드 복호화

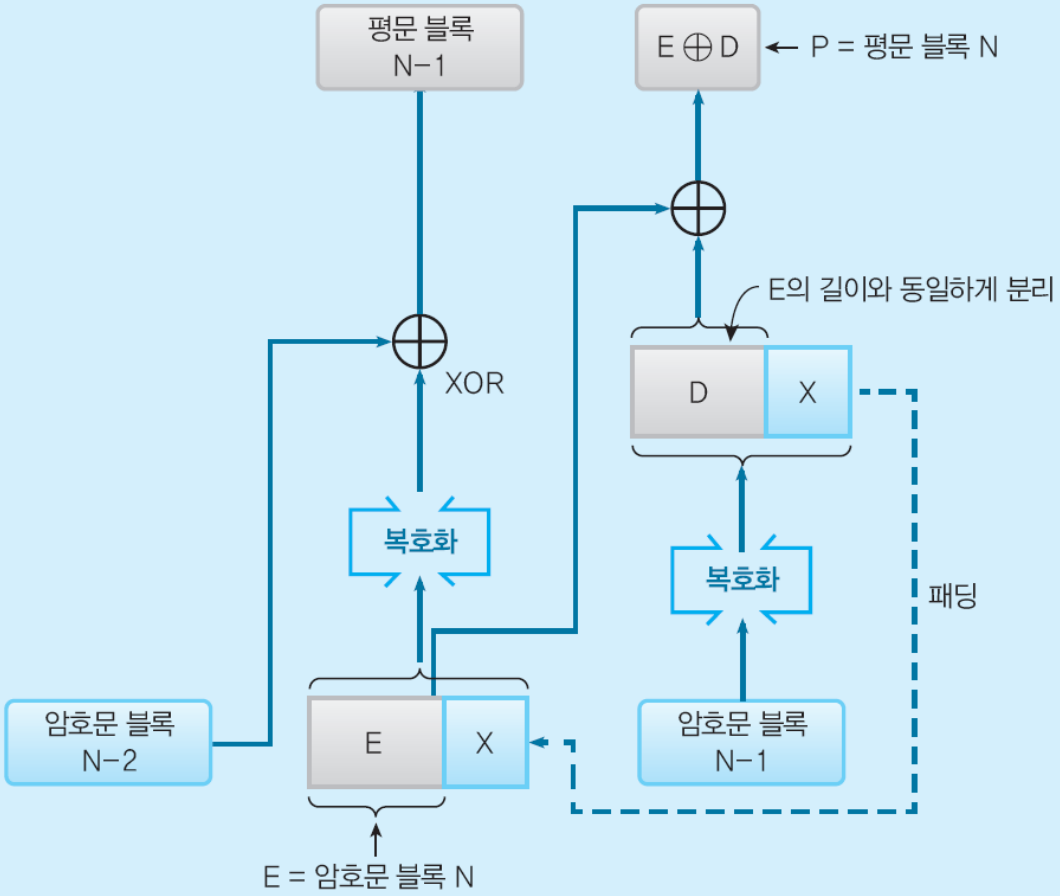


그림 5-C2 • CTS 모드 복호화

Section 04
CFB 모드

4.1 CFB 모드란?

4.2 초기화 벡터

4.3 CFB 모드와 스트림 암호

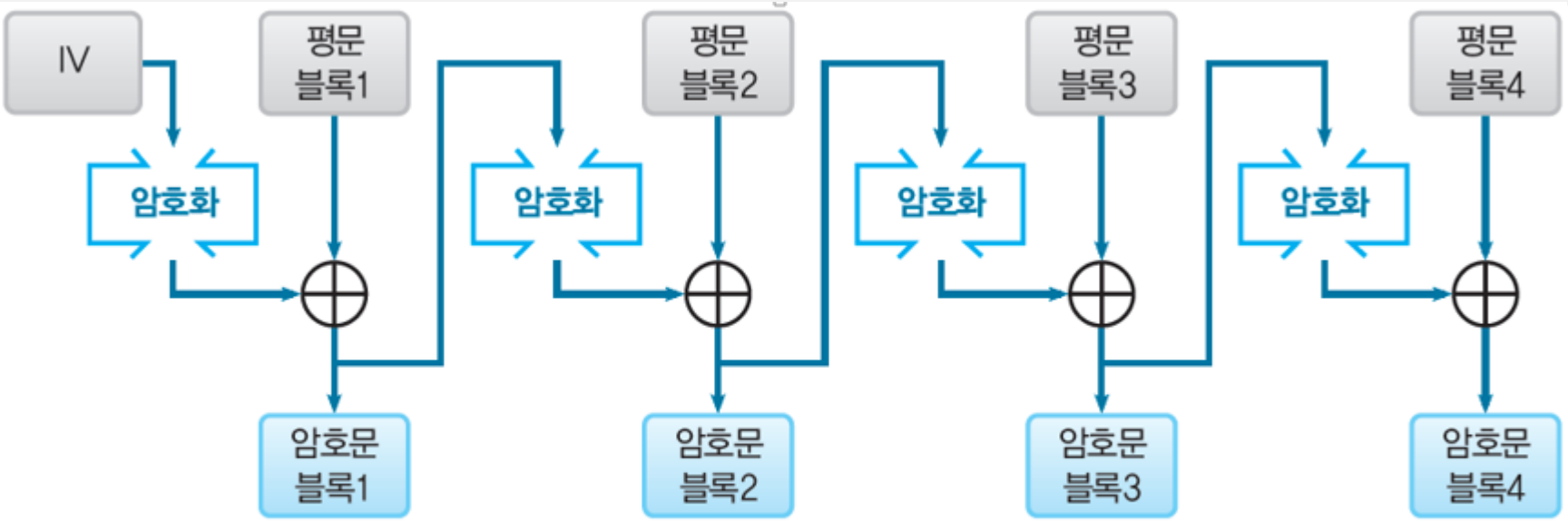
4.4 CFB 모드의 복호화

4.5 CFB 모드에 대한 공격

4.1 CFB 모드

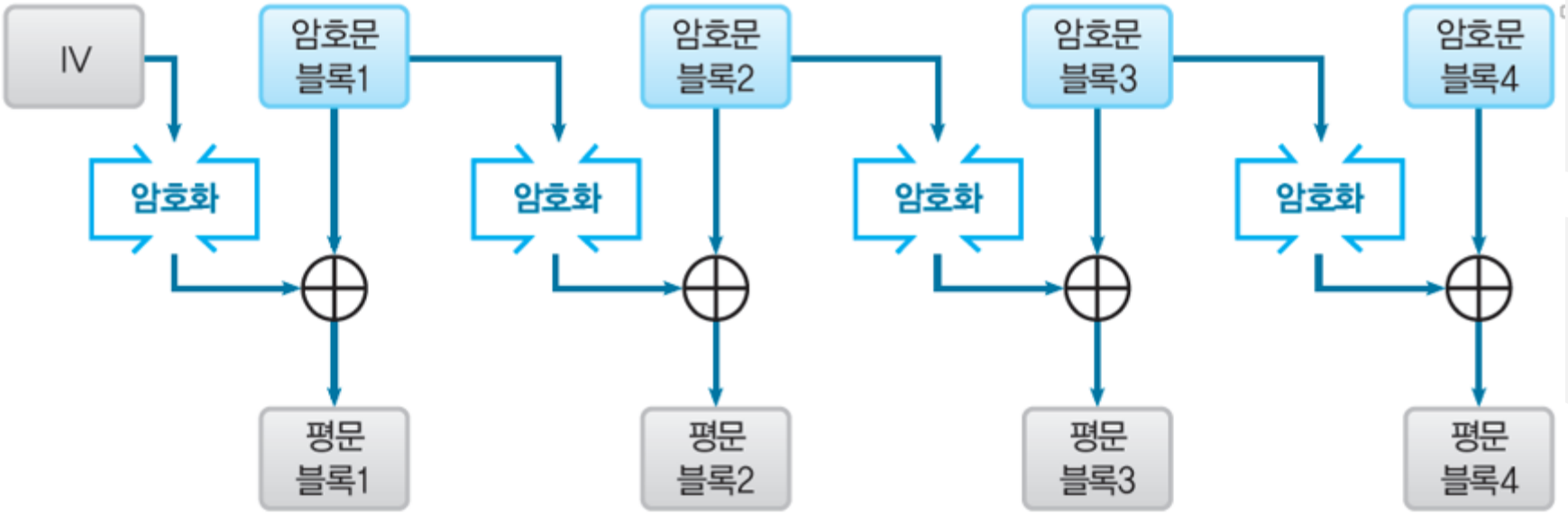
- **CFB 모드**
  - Cipher FeedBack 모드(**암호 피드백 모드**)의 약자
  - CFB 모드에서는 1 단계 앞의 암호문 블록을 암호 알고리즘의 입력으로 사용
  - 평문 블록을 암호 알고리즘에 직접 암호화 하지 않음
  - 평문과 암호문 블록 사이에 오직 XOR만 있음

CFB 모드의 암호화



(a) CFB 모드에 의한 암호화

CFB 모드의 복호화



(b) CFB 모드에 의한 복호화

그림 5-9 • CFB 모드(암호 피드백 모드)

CBC 모드와 CFB 모드 비교

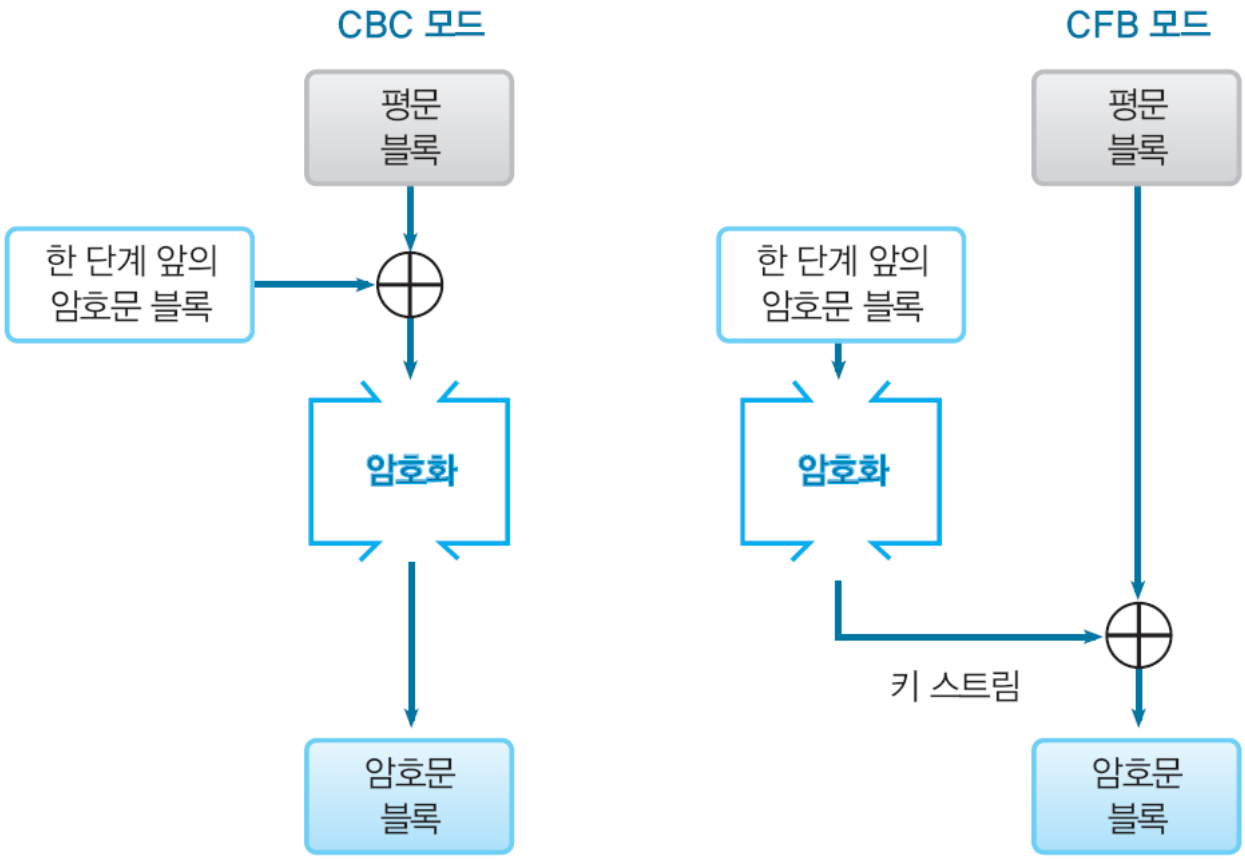


그림 5-10 • CBC 모드와 CFB 모드의 비교

4.2 초기화 벡터

- **초기화 벡터**(IV)
  - 최초의 암호문 블록을 만들어낼 때는 1 단계 앞의 출력이 존재하지 않으므로 대신에 IV를 사용
  - 암호화할 때 만다 다른 랜덤 비트열을 사용

4.3 CFB 모드와 스트림 암호

- **CFB 모드(Cipher FeedBack)**
  - 평문 블록과 암호 알고리즘의 출력을 XOR해서 암호 블록을 만듬
  - XOR로 암호화하는 것이 일회용 패드와 비슷함
- **키 스트림**(key stream)
  - CFB 모드에서 암호 알고리즘이 생성하는 비트열
  - 키 스트림을 생성하기 위한 의사난수 생성기로서 암호 알고리즘을 이용하는 것과 같음
  - 초기화 벡터는 의사난수 생성기의「seed(종자)」에 해당
- CFB 모드는 블록 암호를 써서 생성한 키를 이용하는 스트림 암호로 간주됨

4.4 CFB 모드의 복호화

- CFB 모드에서 복호화를 수행할 경우, 블록 암호 알고리즘 자체는 암호화를 수행하고 있다는 것에 주의
- 키 스트림은 암호화에 의해 생성

4.5 CFB 모드에 대한 공격

- **재전송 공격**(replay attack)
  - 앨리스가 밥에게 4개의 암호문 블록으로 이루어진 암호문 전송
  - 맬로리는 암호문 중 3개를 보존
  - 다음날 앨리스가 밥에게 또 다른 암호문 4개를 전송
  - 맬로리는 오늘 보내진 암호문 블록의 마지막 3개를 어제 보존해 놓은 암호문 블록으로 교체

재전송 공격(replay attack)

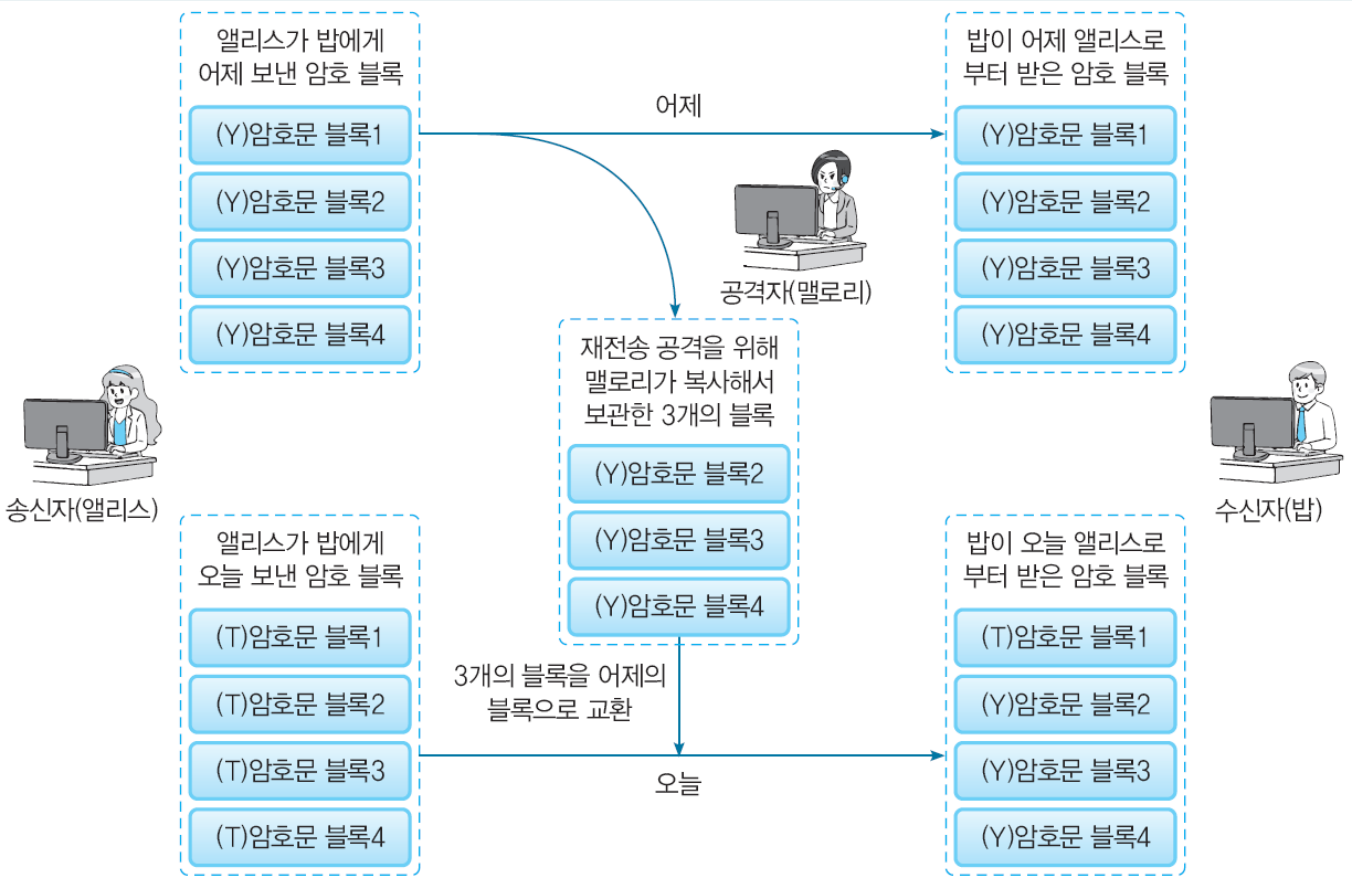


그림 5-11 • CFB 모드에 대한 재전송 공격

오늘 수신한 암호문의 복호화

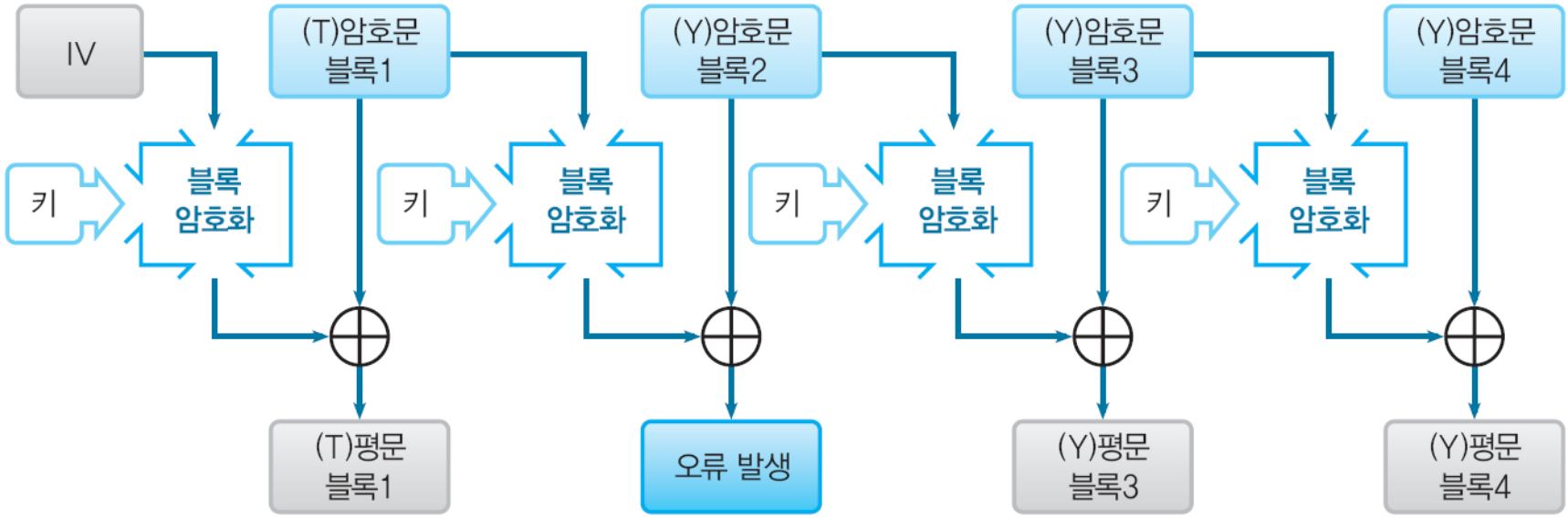


그림 5-12 • 오늘 수신한 암호문 블록을 복호화 한 결과

재전송 공격 결과

- 밥이 복호화를 수행하면 4개의 평문 중 첫번째는 바른 평문이 되고 두번째 부터 오류 발생
- 세번째 네번째 암호문은 맬로리가 바꾼 것임

Quiz 5

- CFB 모드의 그림 5-9를 가만히 보면서 앨리스는 이렇게 생각했다. 이 CFB 모드는 아무래도 납득이 안 간다. 왜냐하면 『CFB 모드의 암호화』그림을 잘 보면 평문 블록과 암호문 블록 사이에 『암호화』가 없지 않는가. 평문 블록을 암호화한 것이 암호문 블록일 텐데 어째서 그 사이에 『암호화』가 없는 것일까? 앨리스의 의문에 답하시오.

Section 05
OFB 모드

5.1 OFB 모드란?

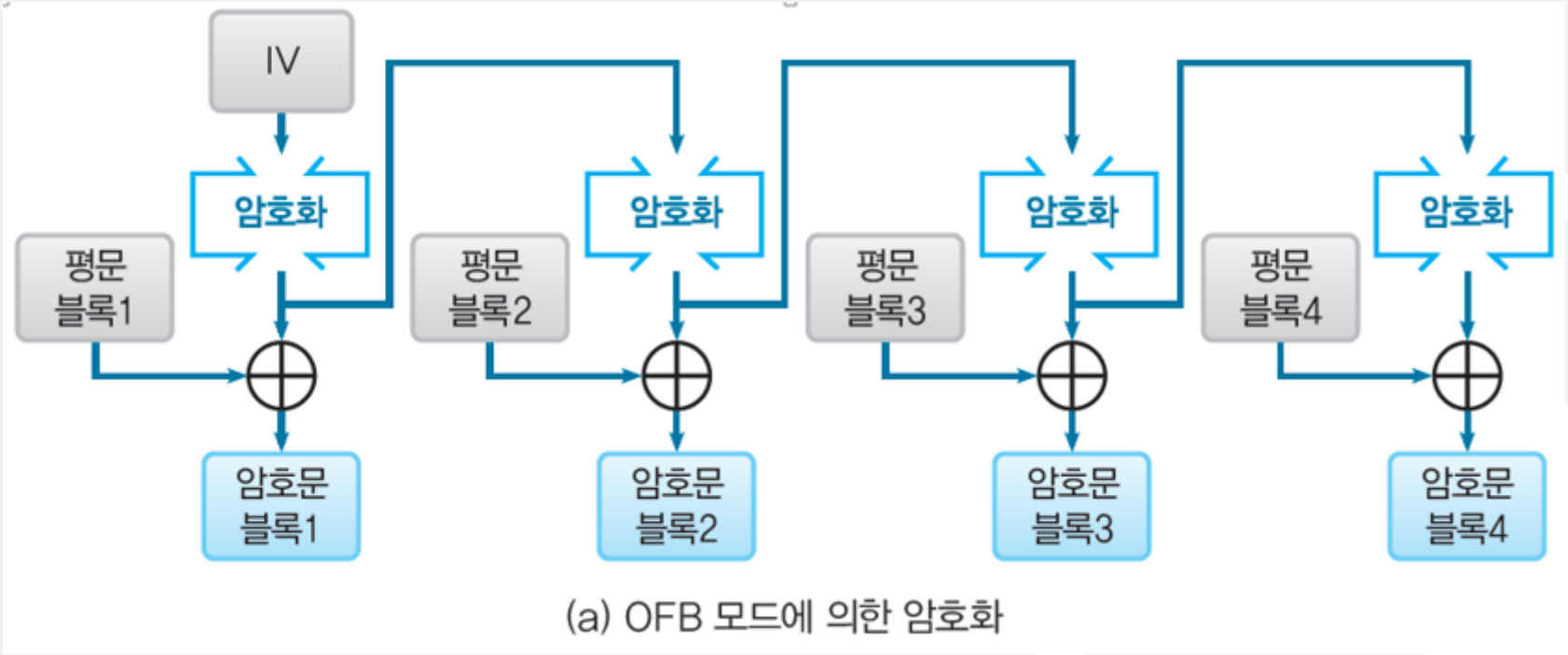
5.2 초기화 벡터

5.3 CFB 모드와 OFB 모드의 비교

5.1 OFB 모드란?

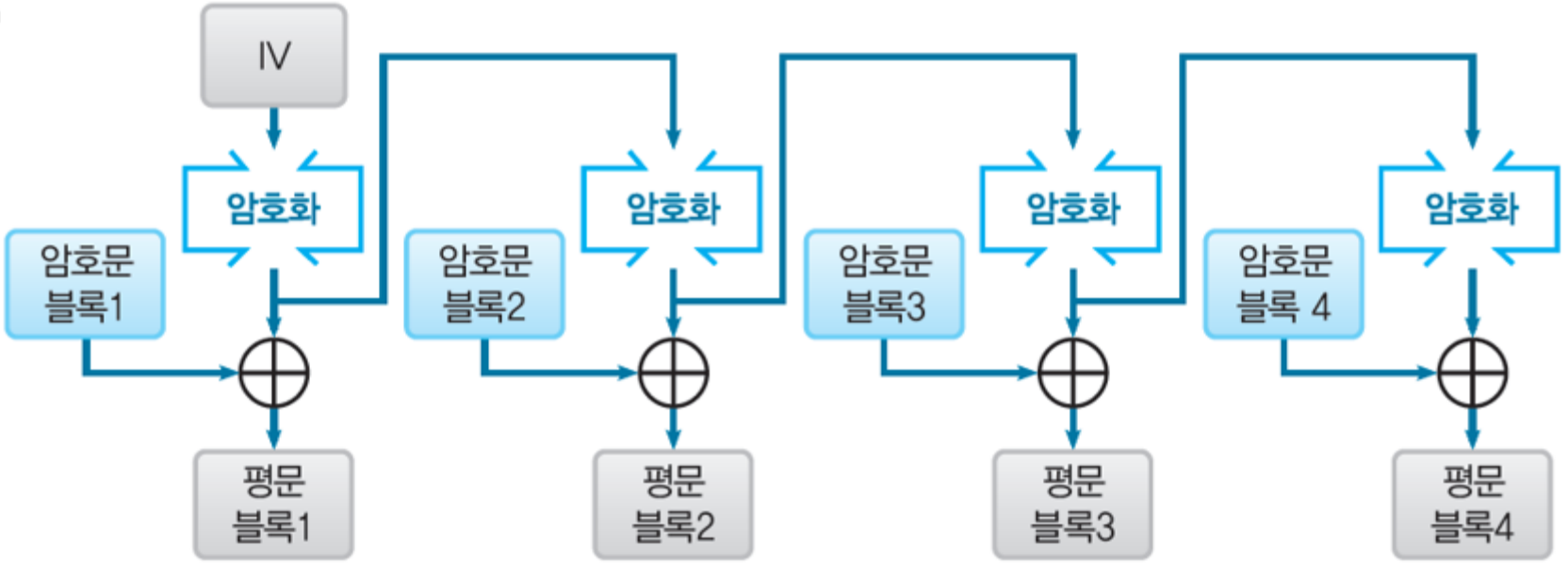
- **OFB 모드**
  - Output-FeedBack 모드(**출력 피드백 모드**)의 약자
  - OFB 모드에서는 암호 알고리즘의 출력을 암호 알고리즘의 입력으로 피드백
  - 평문 블록은 암호 알고리즘에 의해 직접 암호화되고 있는 것은 아님
  - 「평문 블록」과「암호 알고리즘의 출력」을 XOR해서「암호문 블록」을 만든다

OFB 모드에 의한 암호화



(a) OFB 모드에 의한 암호화

OFB 모드에 의한 복호화



(b) OFB 모드에 의한 복호화

그림 5-13 • OFB 모드(출력 피드백 모드)

5.2 초기화 벡터

- CBC 모드나 CFB 모드와 마찬가지로 **초기화 벡터**(IV)를 사용
- 초기화 벡터는 암호화 때마다 다른 랜덤 비트열을 이용

5.3 CFB 모드와 OFB 모드의 비교

- OFB 모드와 CFB 모드에서는 암호 알고리즘으로의 입력만이 다르다
- CFB 모드에서 암호문 블록을 피드백 했기 때문에 암호 피드백이라 함
- OFB 모드에서는 암호 알고리즘의 한단계 앞의 출력을 암호 알고리즘으로 피드백 했기 때문에 출력 피드백 모드라고 함

CFB 모드와 OFB 모드 비교

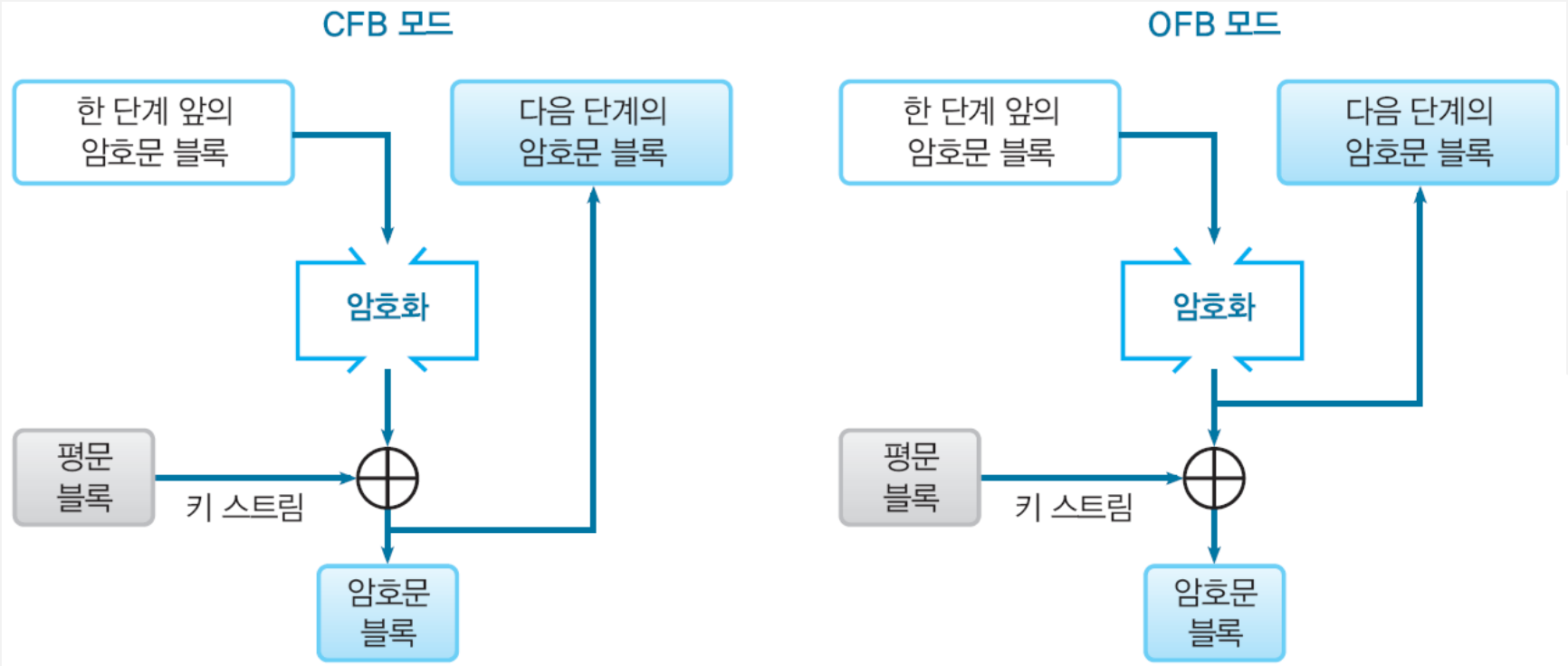


그림 5-14 • CFB 모드와 OFB 모드의 비교

5.3 CFB 모드와 OFB 모드의 비교

- CFB 모드
  - 암호문 블록을 피드백 하기 위해 최초의 평문 블록부터 순서대로 암호화해 가야 함
  - 평문 블록 1의 암호화를 수행하지 않고 건너 뛰어서 평문 블록2를 먼저 암호화 할 수 없음
- OFB 모드
  - 평문 블록과 관계 없이 암호 알고리즘을 빙빙 돌려 XOR하기 위한 비트열(키 스트림)을 준비해 둘 수 있음
  - 키 스트림을 미리 만들어 두면 암호화를 고속으로 수행할 수 있음

Section 06
CTR 모드

6.1 카운터 만드는 법

6.2 OFB 모드와 CTR 모드의 비교

6.3 CTR 모드의 특징

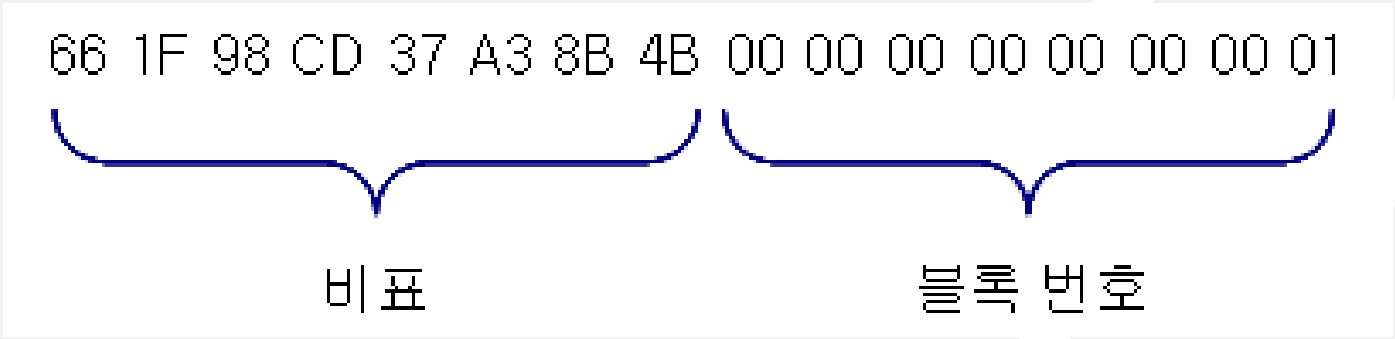
6.4 오류와 기밀성

CTR 모드

- **CTR 모드**
  - CounTeR 모드의 약자
  - **CTR 모드는 1씩 증가해 가는 카운터를 암호화해서 키 스트림을 만들어 내는 스트림 암호**
  - 블록을 암호화할 때마다 1씩 증가해 가는 카운터를 암호화해서 키 스트림을 만듬

6.1 카운터 만드는 법

- 카운터 초기값
  - 암호화 때마다 다른 값(nonce, 비표)을 기초로 해서 작성



6.1 카운터 만드는 법

- 평문 블록1용의 카운터(초기값)

66 1F 98 CD 37 A3 8B 4B 00 00 00 00 00 00 00 01

- 평문 블록2용의 카운터

66 1F 98 CD 37 A3 8B 4B 00 00 00 00 00 00 00 02

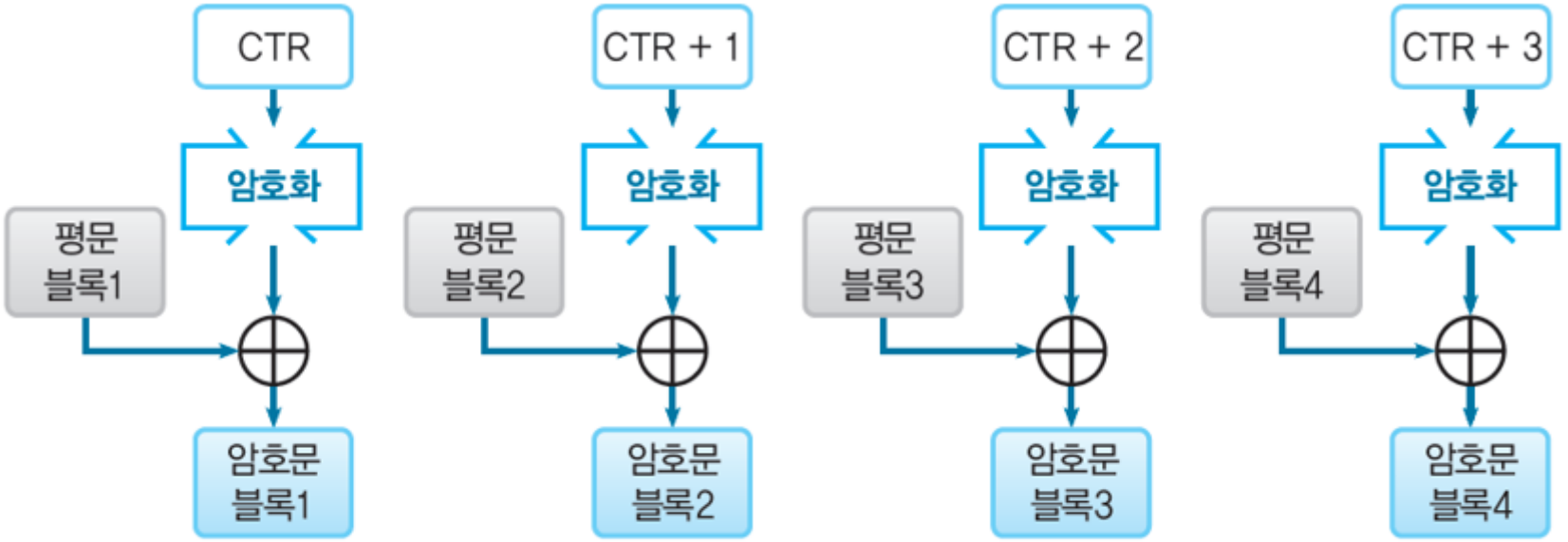
- 평문 블록3용의 카운터

66 1F 98 CD 37 A3 8B 4B 00 00 00 00 00 00 00 03

- 평문 블록4용의 카운터

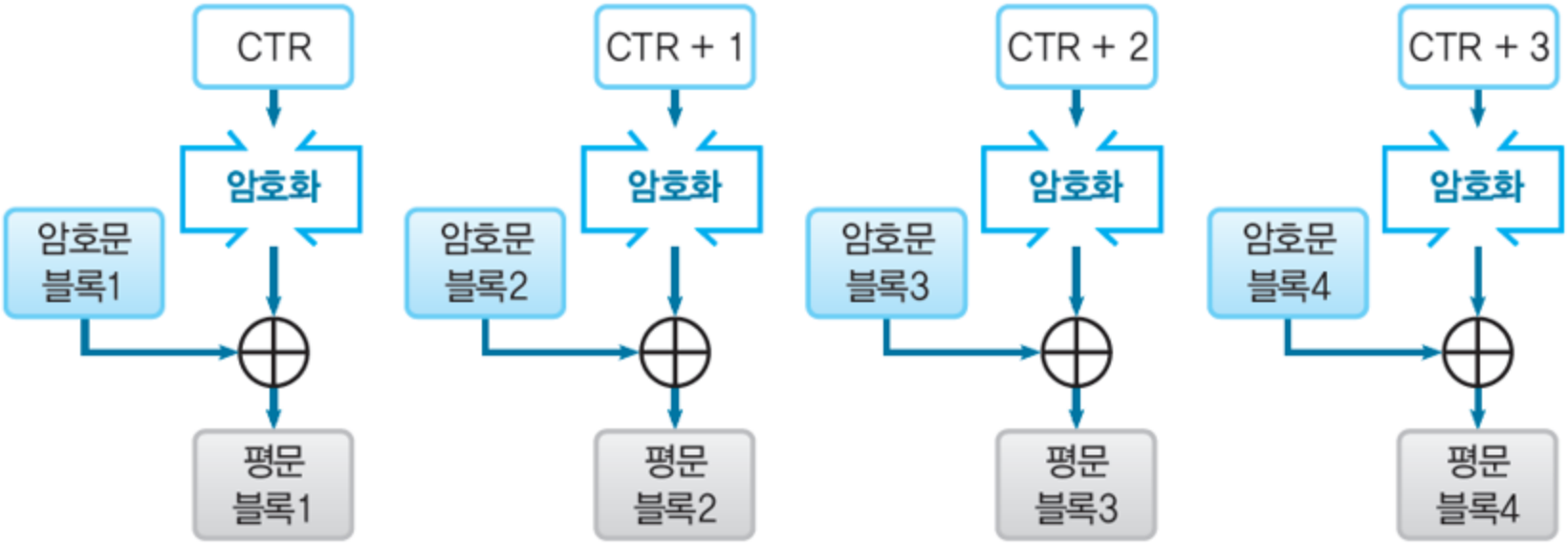
66 1F 98 CD 37 A3 8B 4B 00 00 00 00 00 00 00 04 ⋮ ⋮

CTR 모드 암호화



(a) CTR 모드에 의한 암호화

CTR 모드 복호화



(b) CTR 모드에 의한 복호화

그림 5-15 • CTR 모드(카운터 모드)

6.2 OFB 모드와 CTR 모드의 비교

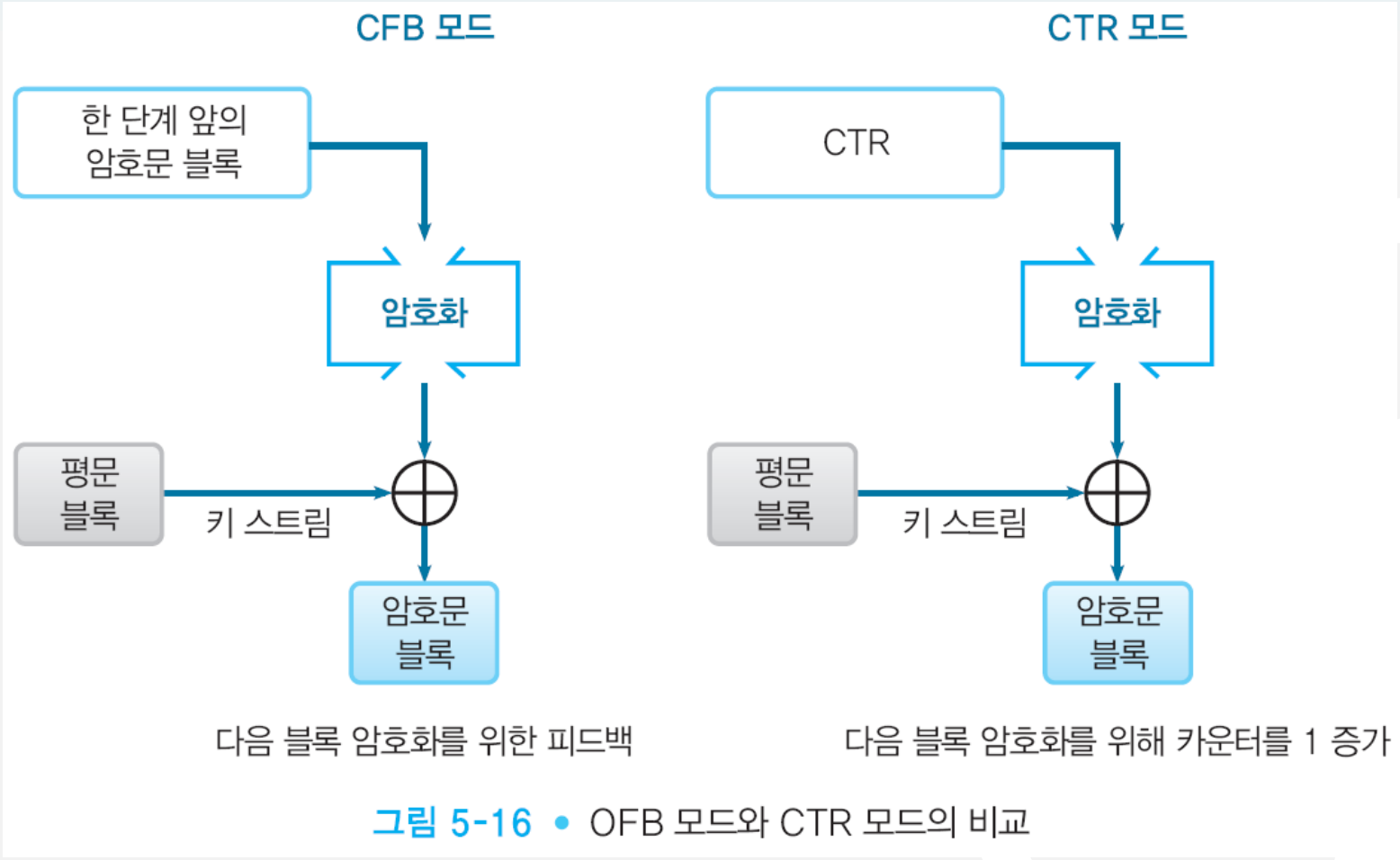


그림 5-16 • OFB 모드와 CTR 모드의 비교

6.3 CTR 모드의 특징

- CTR 모드의 암호화와 복호화는 완전히 같은 구조
- 프로그램으로 구현하는 것이 매우 간단
- OFB 모드와 같은 스트림 암호의 특징
- CTR 모드에서는 블록을 임의의 순서로 암호화·복호화할 수 있음
- 병렬 처리가 가능한 시스템에서는 CTR 모드를 이용하여 자료를 고속으로 처리

6.4 오류와 기밀성

- CTR 모드의 암호문 블록에서 1비트의 반전이 발생 가정
  - 복호화를 수행하면, 반전된 비트에 대응하는 평문 블록의 1비트만이 반전 되고, 오류는 확대되지 않는다.
- OFB 모드에서는 키 스트림의 1블록을 암호화한 결과가, 암호화 전의 결과와 우연히 같아졌다고 하면 그 이후 키 스트림은 완전히 같은 값의 반복이 된다.
  - CTR 모드에서는 그런 걱정은 없음

칼럼 (GCM 모드)

- GCM(Galois/Counter Mode)
- CTR 모드에 인증 기능을 추가한 모드
- CTR 모드로 암호문과 인증자를 생성
- 암호문 위조를 탐지할 수 있음

6.5 모드 선택

- 모드 비교
- 『Applied Cryptography』, Schneider,1996 참고
- 『Practical Cryptography』, Schneider,2003 CBC 모드와 CTR 모드 사용 권장

ECB 모드

	이름	장점	단점	비고
ECB 모드	Electric CodeBook 전자 부호표 모드	▪ 간단 ▪ 고속 ▪ 병렬 처리 가능(암호화. 복호화 양쪽)	▪ 평문 속의 반복이 암호문에 반영된다. ▪ 암호문 블록의 삭제나 교체에 의한 평문의 조작이 가능 ▪ 비트 단위의 에러가 있는 암호문을 복호화하면, 대응하는 블록이 에러가 된다. ▪ 재전송 공격이 가능	사용해서는 안 된다

CBC 모드

CBC 모드	Cipher Block Chaining 암호 블록 연쇄 모드	▪ 평문의 반복은 암호문에 반영되지 않는다. ▪ 병렬처리 가능(복호화만) ▪ 임의의 암호문 블록을 복호화할 수 있다.	▪ 비트 단위의 에러가 있는 암호문을 복호화하면, 1블록 전체와 다음 블록의 대응하는 비트가 에러가 된다. ▪ 암호화에서는 병렬처리를 할 수 없다.	Practical Cryptography 권장

CFB 모드

CFB 모드	Cipher-FeedBack 암호 피드백 모드	▪ 패딩이 필요 없다. ▪ 병렬처리 가능(복호화만) ▪ 임의의 암호문 블록을 복호화할 수 있다.	▪ 암호화에서는 병렬처리를 할 수 없다. ▪ 비트 단위의 에러가 있는 암호문을 복호화하면, 1블록 전체와 다음 블록의 대응하는 비트가 에러가 된다. ▪ 재전송 공격이 가능	현재는 사용 안 함 CTR 모드를 사용하는 편이 나음

OFB 모드

OFB 모드	Output-FeedBack 출력 피드백 모드	▪ 패딩이 필요 없다. ▪ 암호화. 복호화의 사전 준비를 할 수 있다. ▪ 암호화와 복호화가 같은 구조를 하고 있다. ▪ 비트 단위의 에러가 있는 암호문을 복호화하면, 평문의 대응하는 비트만 에러가 된다.	▪ 병렬 처리를 할 수 없다. ▪ 적극적 공격자가 암호문 블록을 비트 반전시키면, 대응하는 평문 블록이 비트 반전된다.	

CTR 모드

CTR 모드	CounTeR 카운터 모드	▪ 패딩이 필요 없다. ▪ 암호화. 복호화의 사전 준비를 할 수 있다. ▪ 암호화와 복호화가 같은 구조를 하고 있다. ▪ 비트 단위의 에러가 있는 암호문을 복호화하면, 평문의 대응하는 비트만 에러가 된다. ▪ 병렬 처리 가능(암호화. 복호화 양쪽)	▪ 적극적 공격자가 암호문 블록을 비트 반전시키면, 대응하는 평문 블록이 비트 반전된다.	Practical Cryptography 권장

Quiz 6 모드의 기초 지식

- 다음 문장 중 바른 것에는 O, 틀린 것에는 X를 표시하시오.
  1. ECB 모드의 암호화에서는 같은 내용의 평문 블록은 같은 내용의 암호문 블록으로 변환된다.
  2. CBC 모드의 복호화에서는 암호문 블록 3이 파손되어 있으면 암호문 블록 5를 바르게 복호화할 수 없다.
  3. CFB 모드의 암호화에서는 평문의 도중부터 암호화를 시작할 수 없다.
  4. OFB 모드로 복호화를 수행할 때 블록 암호 알고리즘 자체가 실제로 수행하는 처리는 암호화이다.