제 3 장 블록암호 와 DES

❑ 목 차

- ❖ 단순 **DES**
- ❖ 블록 암호 기법
- ❖ **DES**
- ❖ 블록 암호의 설계 원리
- ❖ 블록 암호의 운용 모드

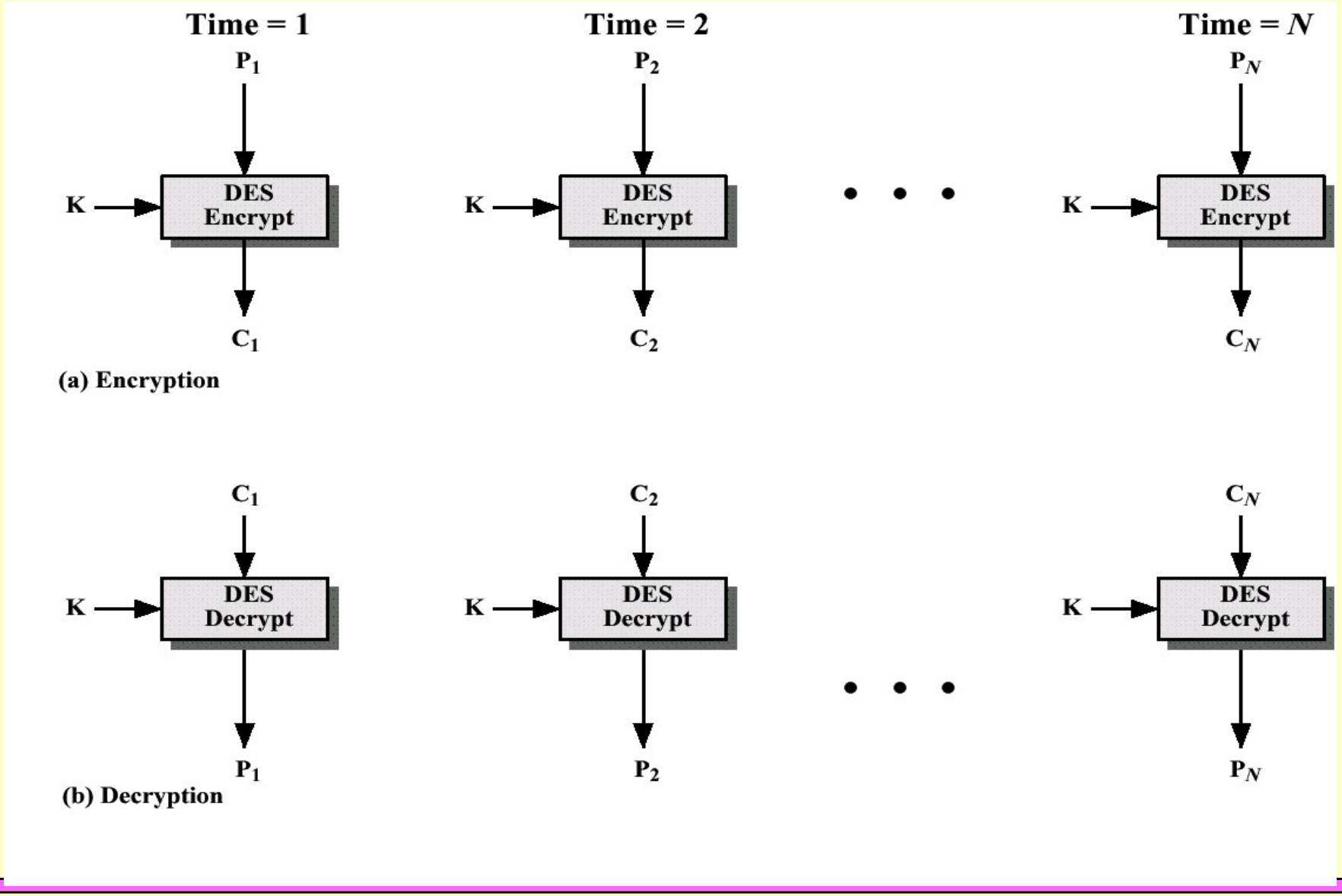
블록 암호의 운용 모드

운용 모드	설명	전형적인 응용
ECB	블록별 독립적으로 암호화 수행	짧은 자료전송 (예: 암호키)
CBC	선행 암호결과를 다음번 암호화할 평문 64 비트와 XOR 하여 암호화 수행	범용 블록형 전송 인증
CFB	한 번에 j 비트씩 선행 암호문과 평문을 XOR 하여 암호화 수행	범용 스트림형 전송 인증
OFB	CFB 와 유사한 방식이지만 한 번에 j 비트씩 암호문 이전의 DES 출력과 평문을 XOR 하여 암호화 수행	잡음있는 채널상의 스트림형 전송 (예: 위성통신)
CTR	평문의 각 블록을 암호화된 카운터와 XOR, 각 단계마다 카운터 증가	일반 용도의 블록형 전송 ATM, IPSec 보안 고속응용

전자 코드북(ECB; Electronic Codebook)

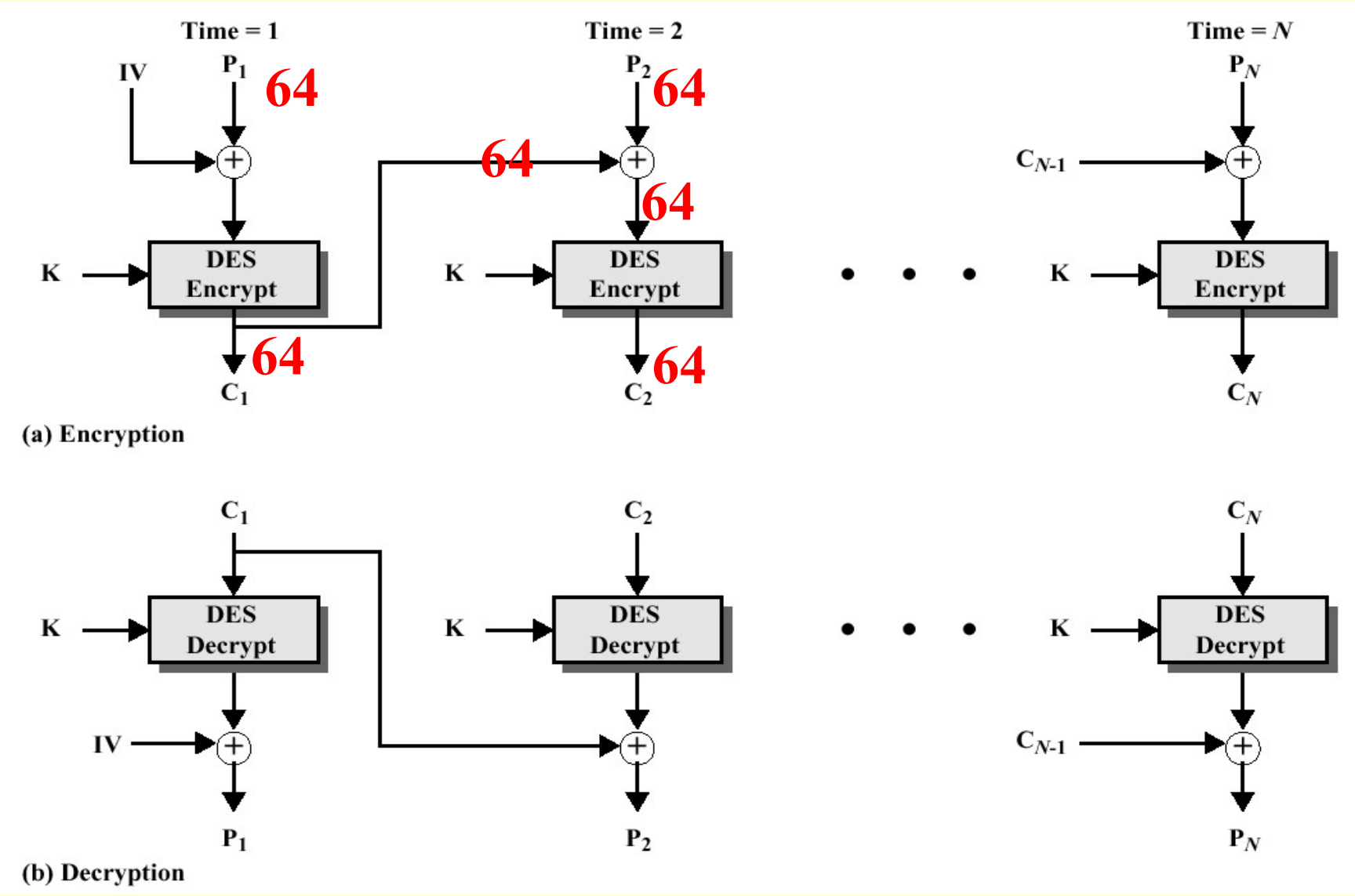
- 하나의 64비트 평문 단위로 처리
  - 각 64비트 평문에 대응하는 64비트 암호문→ 코드 북 유사
- 마지막 비트가 64비트 미만이면 나머지 비트를 채운 후 진행
- 동일한 블록이 입력되면 암호문도 동일
  - 안전성 저해 요소
  - 메시지가 긴 경우는 동일한 블록이 출현할 확률 증가
  - 메시지가 항상 정규화 된 어떤 필드로 시작되는 경우는 해독위험

ECB (Electronic Codebook) 모드



암호 블록 연결(CBC; Cipher Block Chaining)

- 선행 단계의 암호문 출력이 다음 암호단계의 입력에 XOR 반영됨



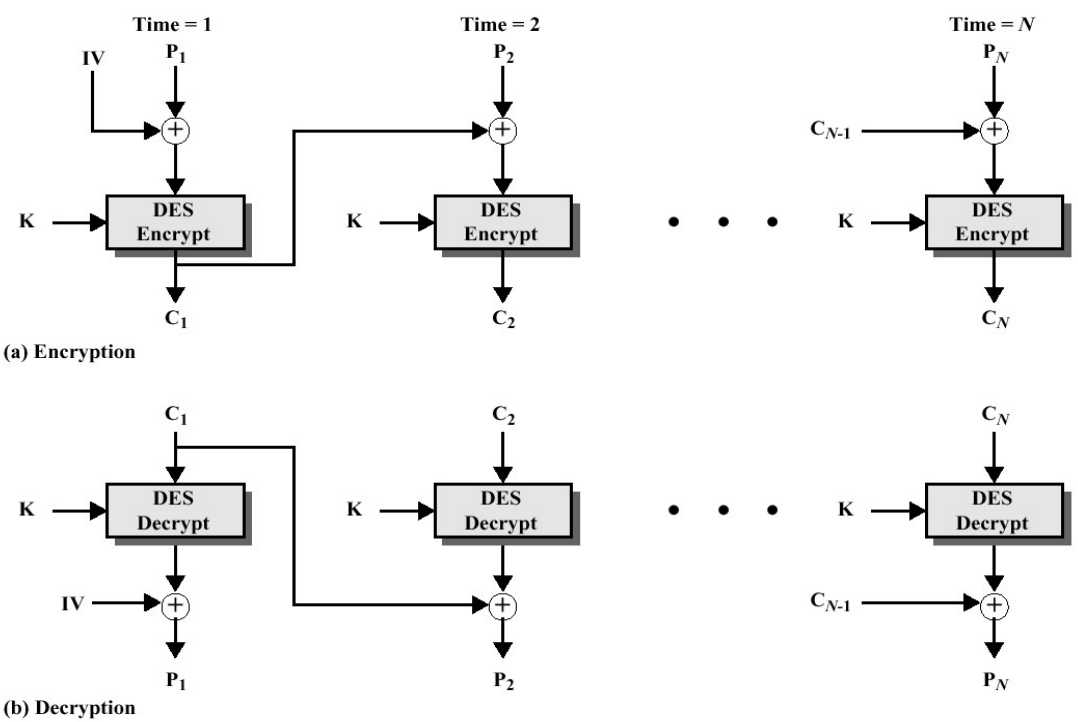
암호 블록 연결(CBC; Cipher Block Chaining)

- 선행 단계의 암호문 출력이 다음 암호단계의 입력에 XOR 반영됨
  - 동일한 평문 블록이 입력되어도 상이한 암호문 생성효과
  - 암호문 : $C_n = E_k (C_{n-1} \oplus P_n)$ $C_2 = E_k (C_1 \oplus P_2)$
  - 복호화 :

$$D_k (C_n) = D_k [E_k (C_{n-1} \oplus P_n)]$$
$$= (C_{n-1} \oplus P_n)$$
$$D_k (C_2) = D_k [E_k (C_1 \oplus P_2)]$$
$$= (C_1 \oplus P_2)$$

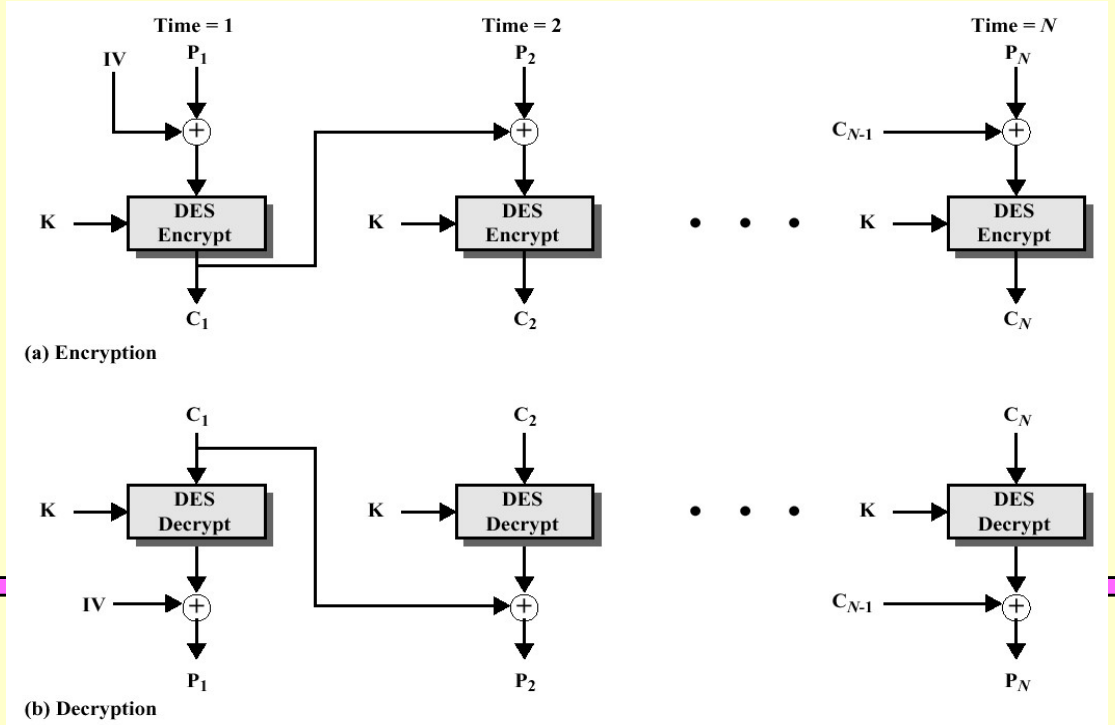
  - $P_n = C_{n-1} \oplus D_k (C_n)$

$$= C_{n-1} \oplus (C_{n-1} \oplus P_n) = P_n$$



암호 블록 연결(CBC; Cipher Block Chaining)

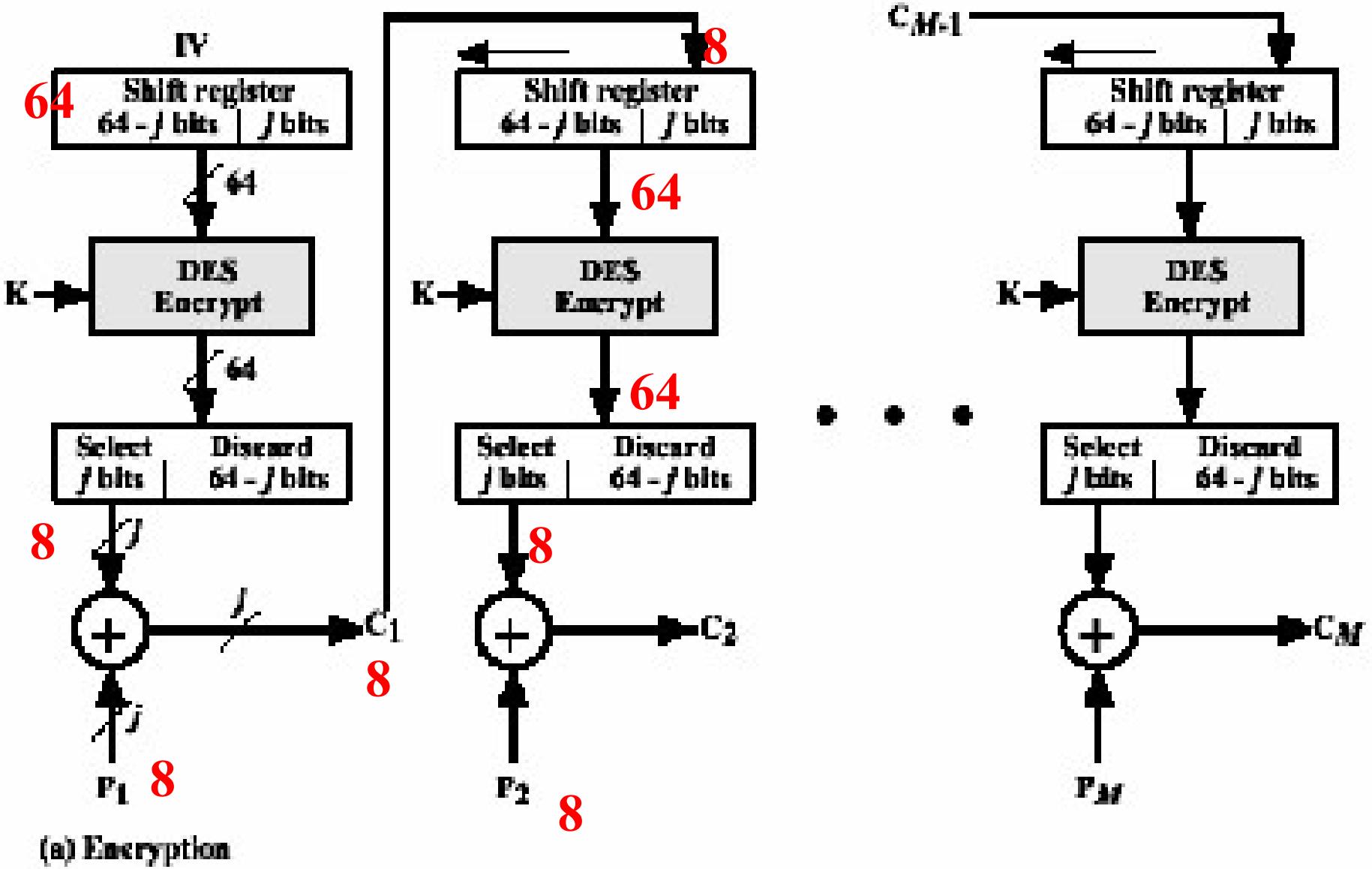
- 첫번째 암호화에 적용할 IV 값은 송수신자가 미리 인지 필요
  - IV는 키와 동등하게 보호
    - 시작에 ECB 방식으로 암호화하여 전송가능
- 기밀성 외에 인증목적으로 활용가능
- 전송상에서 암호문의 결함은 복호화 과정에 오류 발생



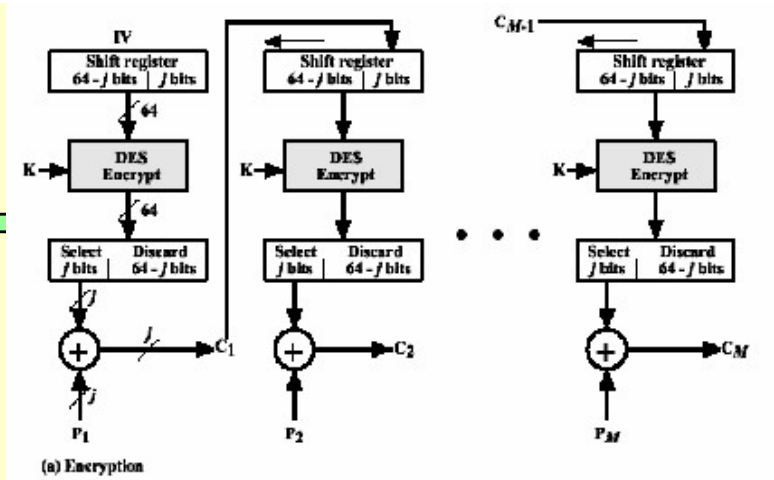
암호 피드백(CFB; Cipher FeedBack mode)

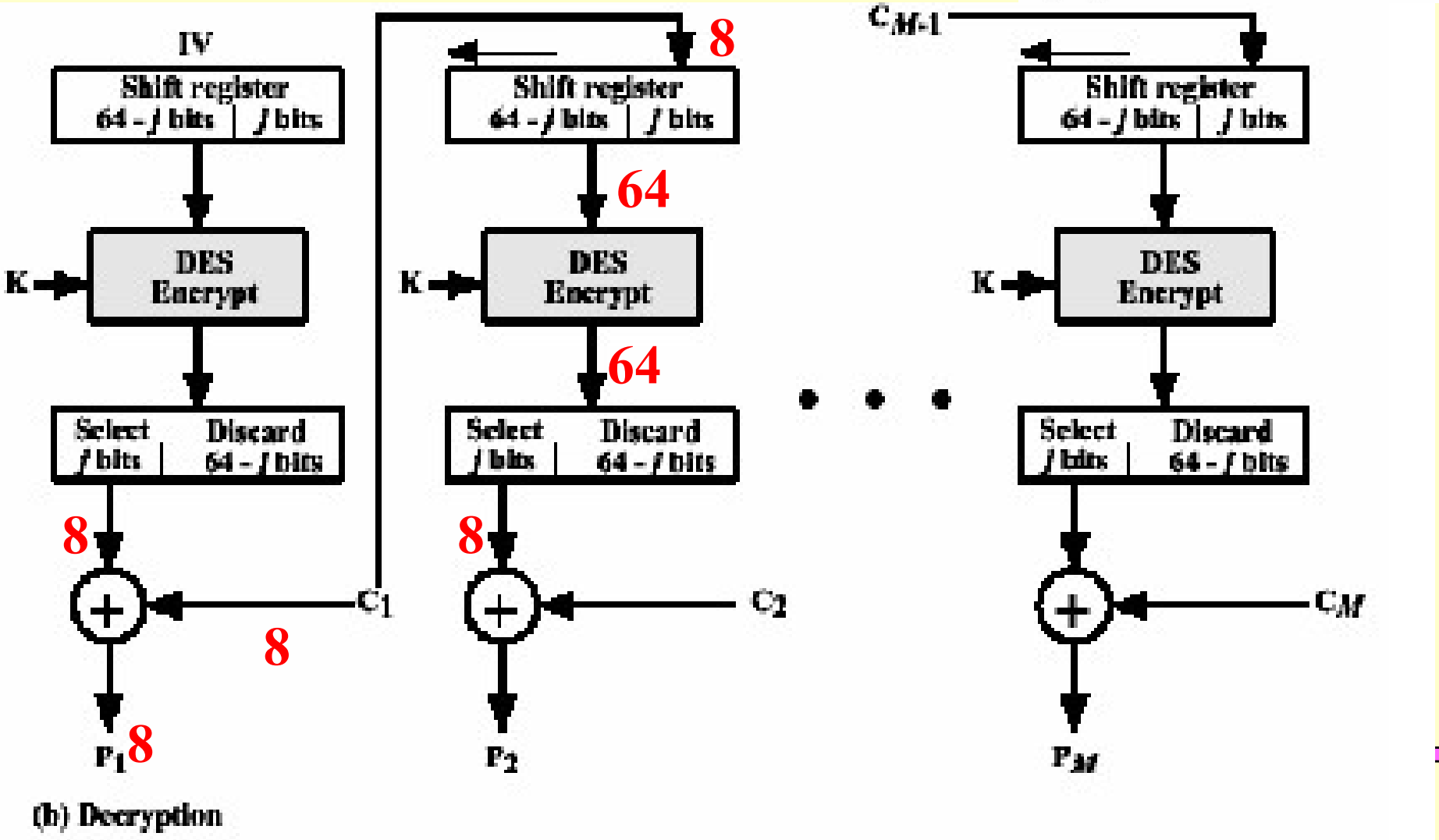
- DES는 본질적으로 블록 암호 방식
  - CFB 또는 OFB모드를 사용하여 스트림 암호방식 전환가능
- 스트림 암호방식은 블록이 64비트 정수배가 되도록 패딩 불필요
- CFB는 문자지향 스트림 암호화 형식으로 실시간 작동가능
  - 8-비트 문자 전송경우 8비트 단위로 암호화 전송
- 암호화 과정(전송단위를 j비트로 가정, 일반적으로 8)
  - 첫번째 암호과정 입력 : IV로 초기화된 64비트 이동 레지스터
  - 키를 적용하여 64비트 전체 암호화
  - 좌측 j 비트를 평문의 첫 단위 P_1 과 XOR 한 결과가 암호문 C_1
  - 암호문 C_1 은 다음 단계의 암호화를 위하여 레지스터의 우측에 J비트 입력
- 전송중의 비트 오류가 전체적으로 전파

J비트 암호 피드백(CFB) 모드



CFB 모드

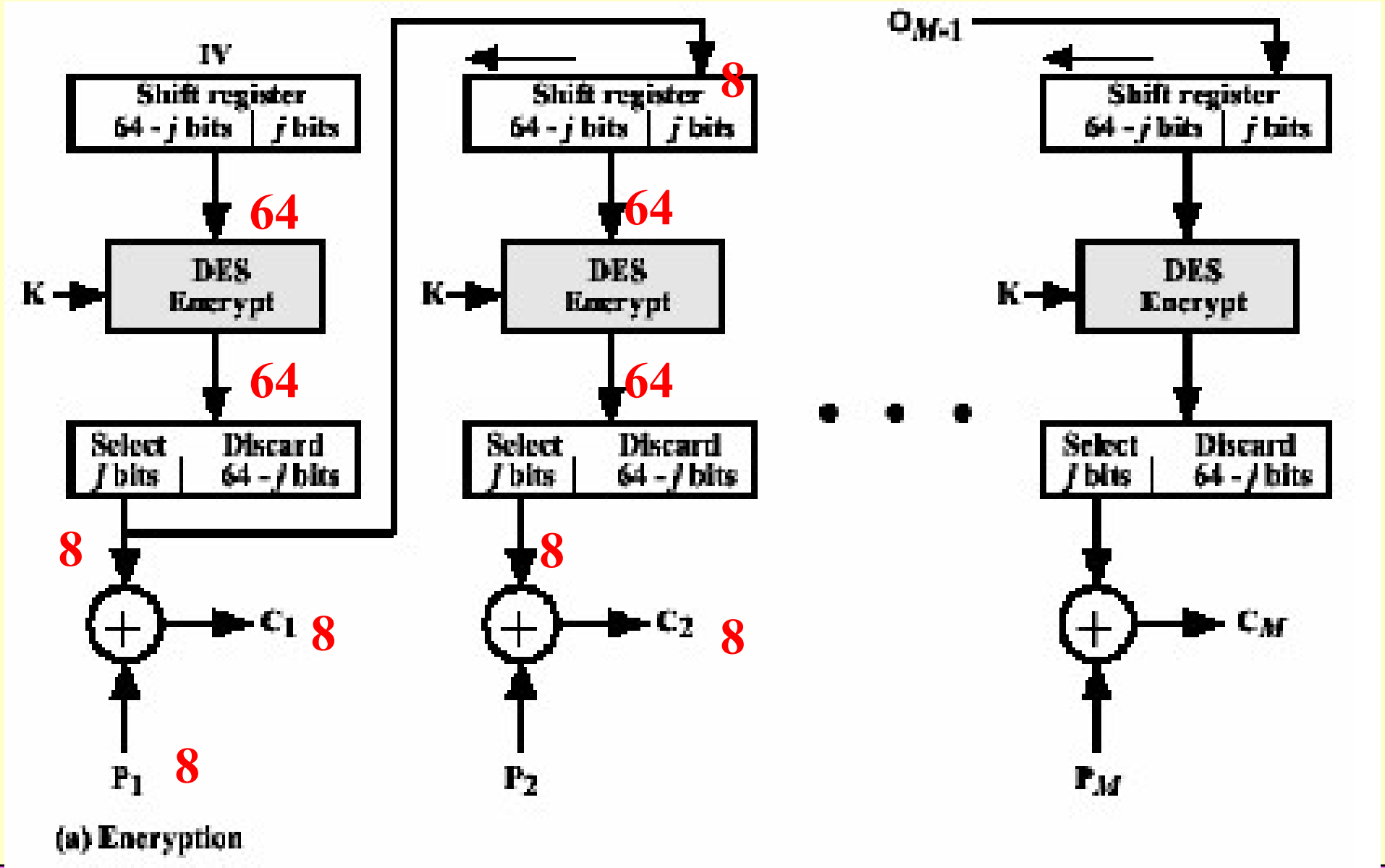

IV
Shift register
64 - j bits
j bits
64
DES
Encrypt
K
Select
j bits
Discard
64 - j bits
C1
C2
CM
P1
P2
PM
CM-1
(a) Encryption

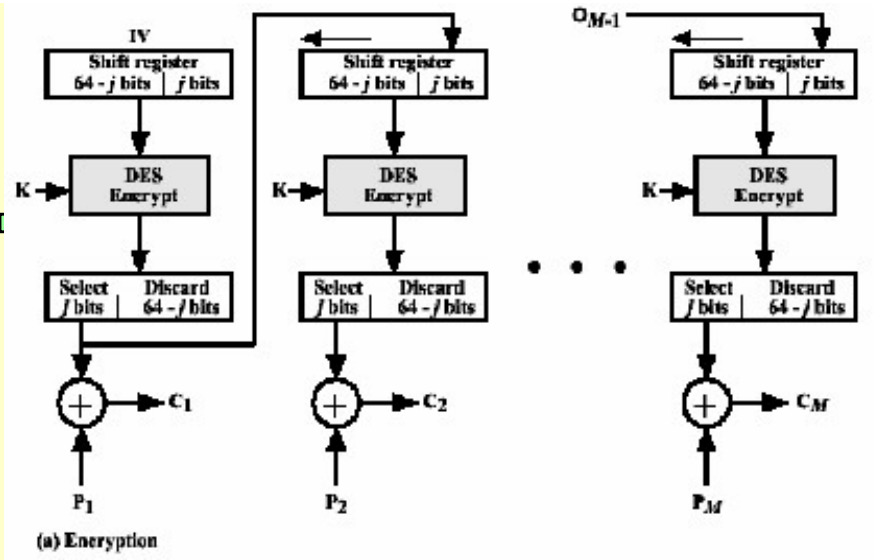

IV
Shift register
64 - j bits
j bits
8
64
DES
Encrypt
K
Select
j bits
Discard
64 - j bits
C1
C2
CM
CM-1
P1
P2
PM
(b) Decryption

출력 피드백(OFB; Output-FeedBack mode)

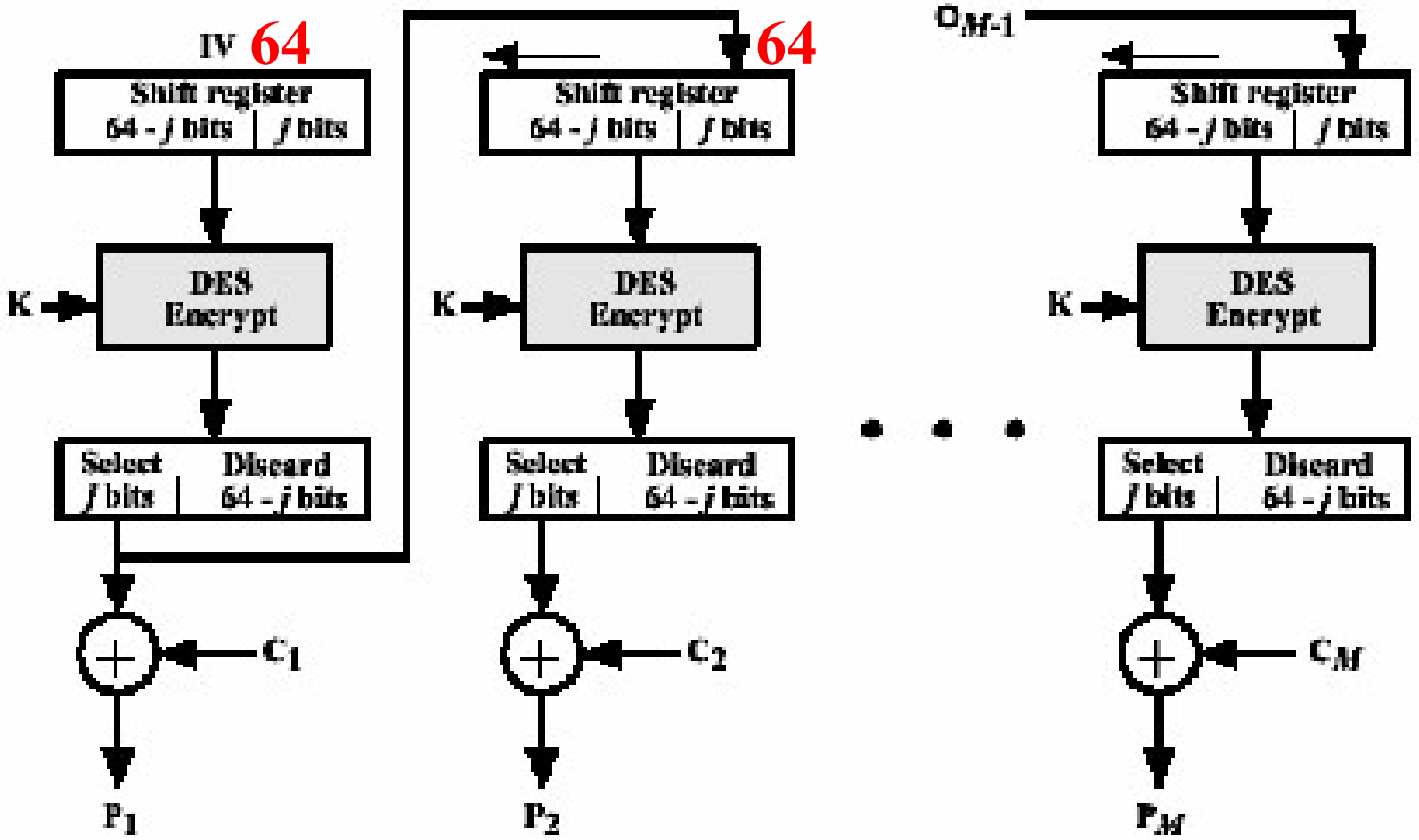
- 전송중의 비트 오류는 해당 암호단위 하나에 제한
- CFB보다 메시지 스트림 변조공격에 취약
  - 암호문의 연계성 부족원인
  - 암호문 변조와 오류 검출부를 동시 조작가능
- 키 스트림: 주기성이 있음
- Feedback의 출발 위치를 제외하고는 CFB와 유사

J비트 출력 피드백(OFB)모드



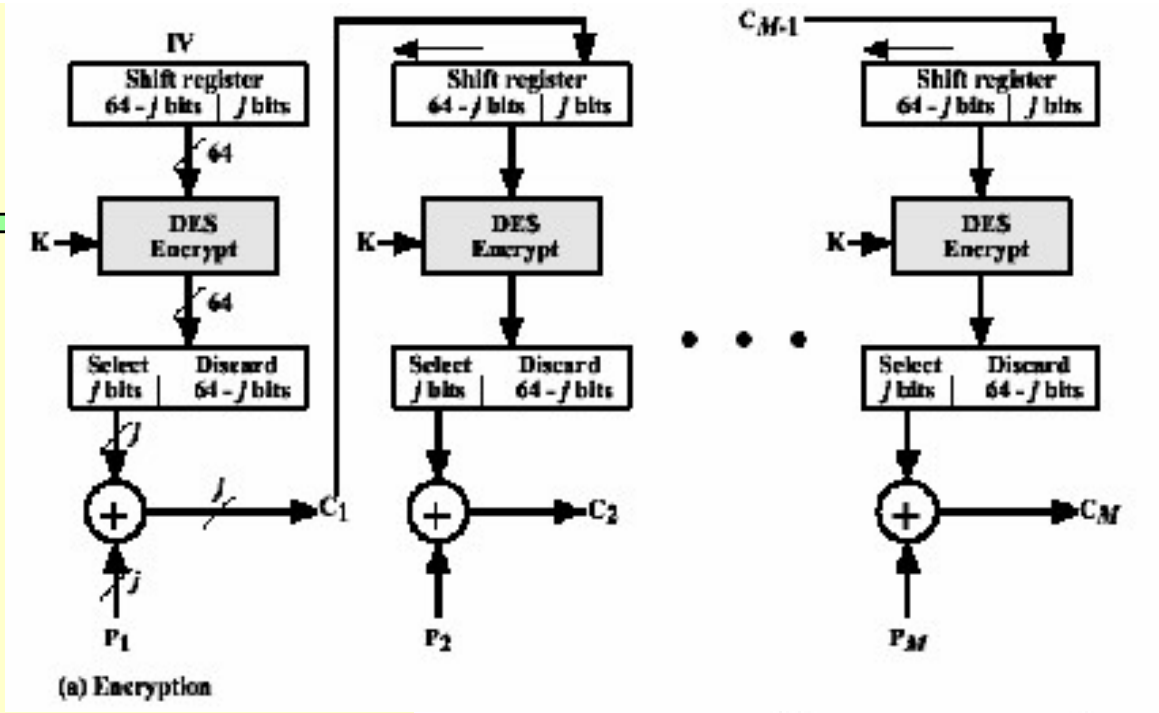


(a) Encryption

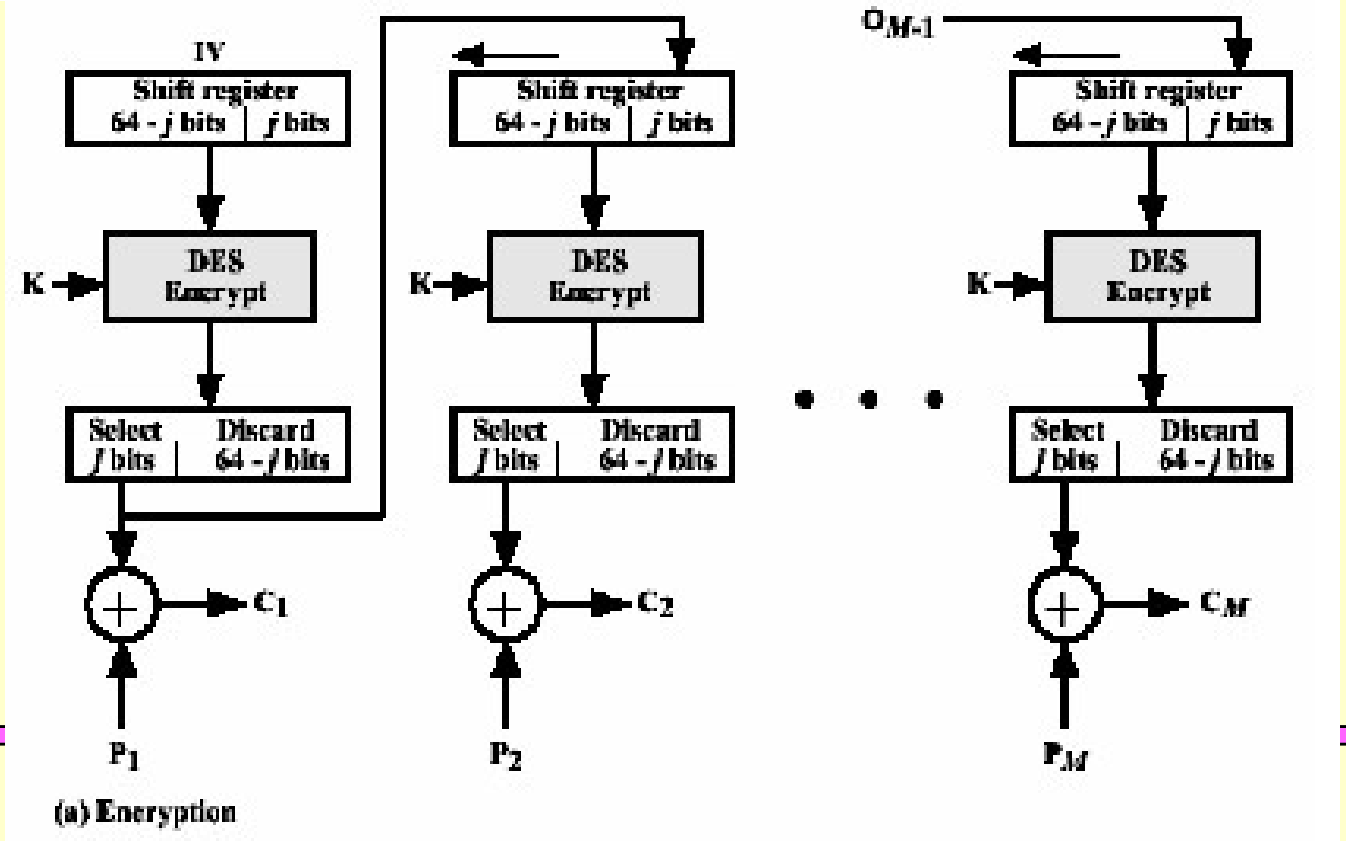


(b) Decryption

CFB

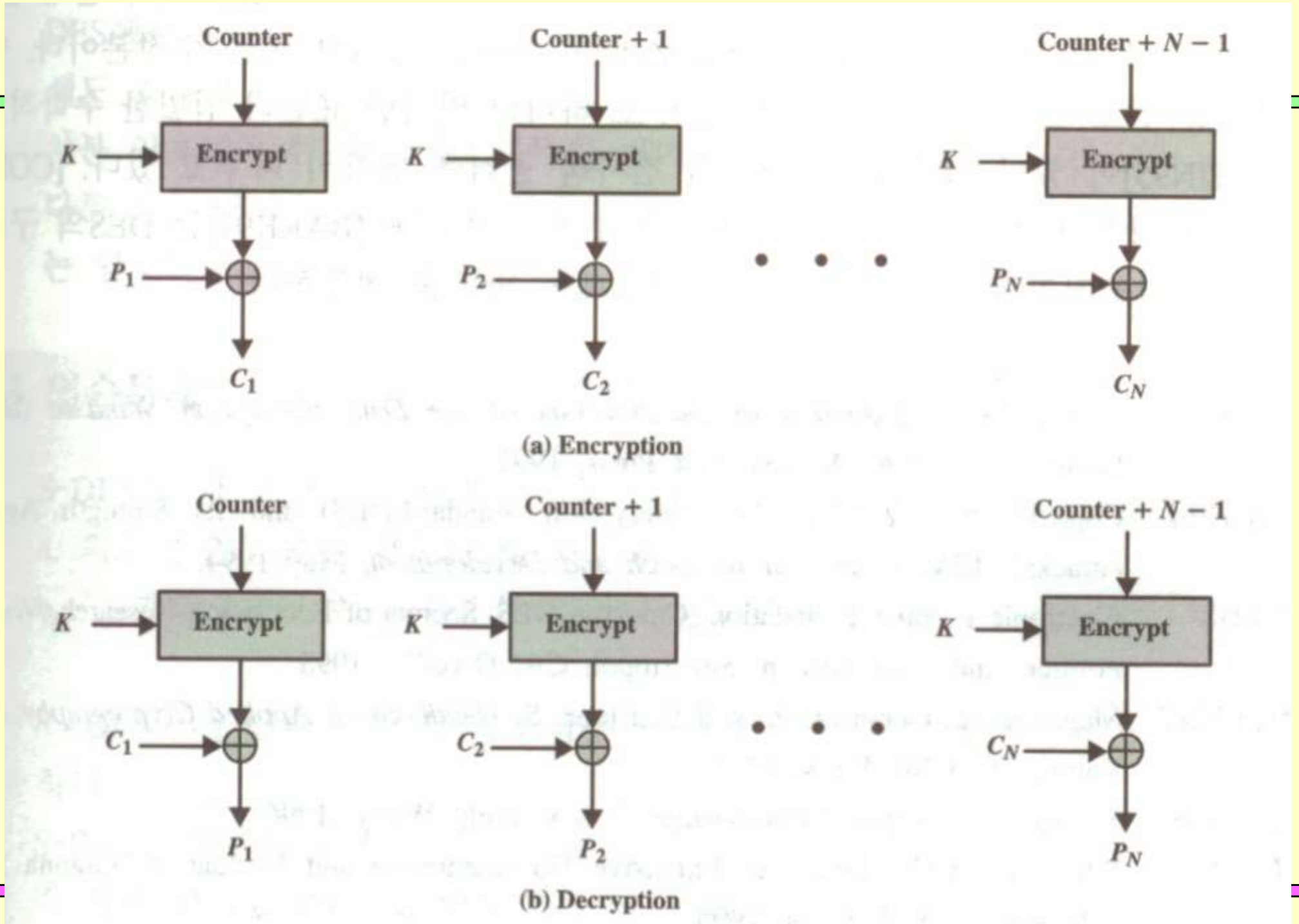

IV
Shift register
64 - j bits
j bits
64
DES
Encrypt
K
64
Select
j bits
Discard
64 - j bits
j
P1
C1
P2
C2
CM-1
PM
CM
(a) Encryption

OFB


IV
Shift register
64 - j bits
j bits
DES
Encrypt
K
Select
j bits
Discard
64 - j bits
P1
C1
P2
C2
OM-1
PM
CM
(a) Encryption

CTR 모드 (Counter)

- ATM 통신망보안 및 IP 보안
- 계수기 값이 암호화 되는 각 평문 블록마다 달라야 함
- 계수기는 어떤값으로 초기화된 다음 매블럭마다 1씩 증가
- 장점
  - 카운터 하드웨어의 효율성 : 암호화가 병렬 처리 가능
  - 소프트웨어 효율성 : 파이프라이닝 등의 병렬 처리
  - 전처리 : 암호문 입력과 별개로 처리, 유일한 연산은 XOR
  - 임의 접근이 가능
  - 안전성의 증명
  - 단순성 : 암호화 알고리즘의 구현만 필요


Counter
Counter + 1
Counter + N − 1
K
Encrypt
P_1
P_2
P_N
C_1
C_2
C_N
(a) Encryption
Counter
Counter + 1
Counter + N − 1
K
Encrypt
C_1
C_2
C_N
P_1
P_2
P_N
(b) Decryption

< 에러 파급 >

- 전송 중 1비트 에러에 대한 복호시 에러 파급
  - **ECB 모드 :**
  - **CBC 모드 :**
  - **CFB 모드 :**
  - **OFB 모드 :**

❑ ECB 모드 : 비트

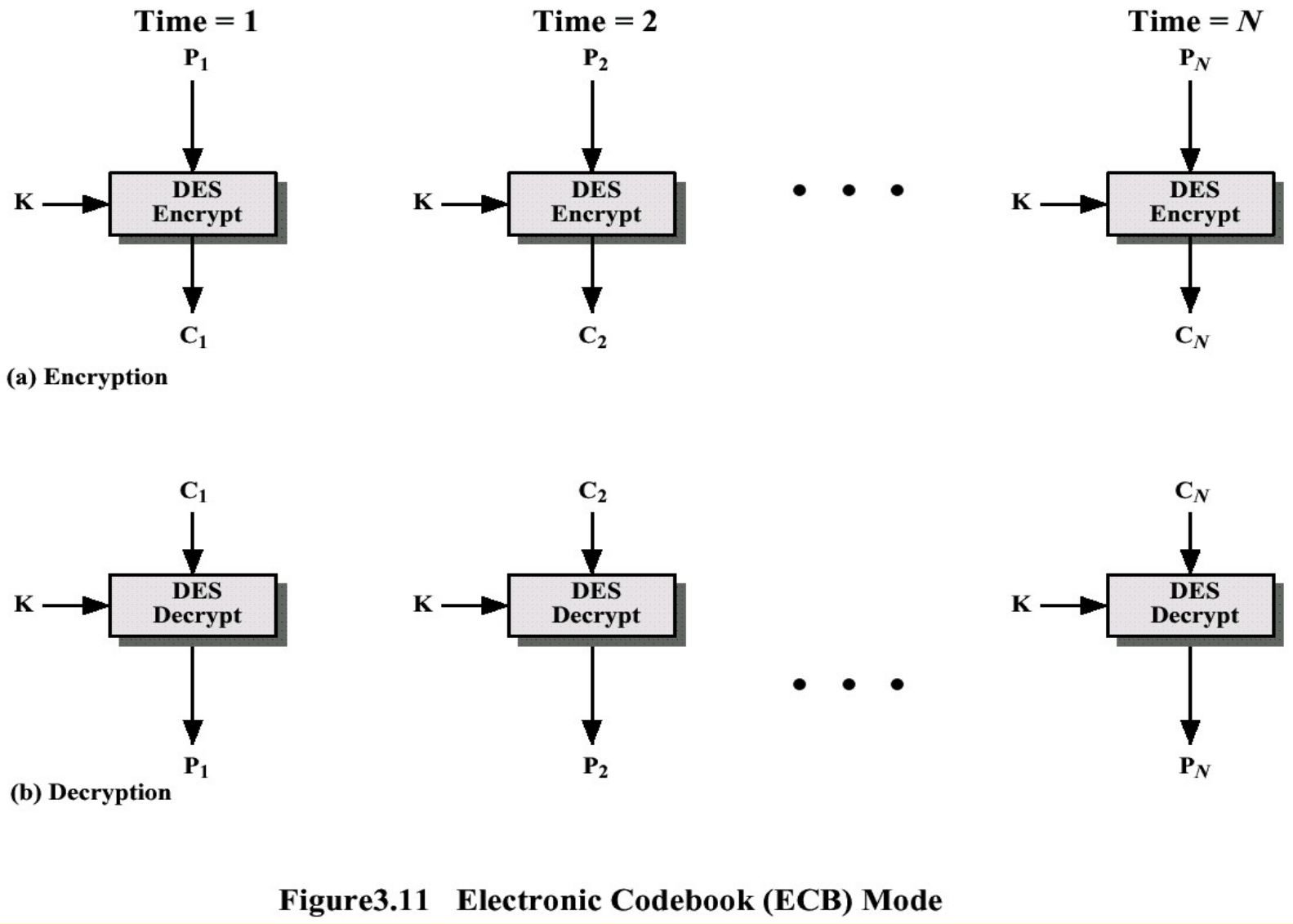
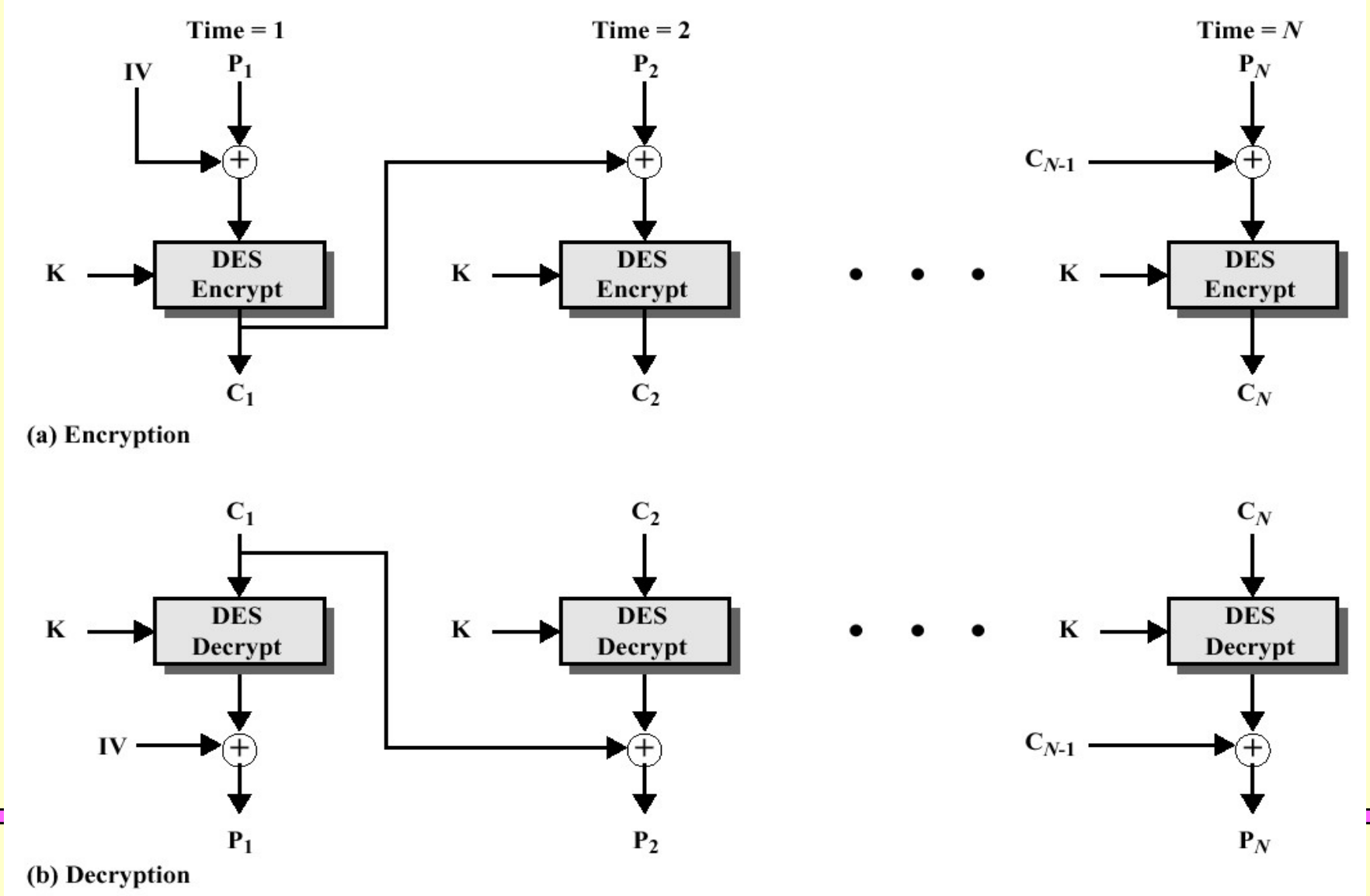


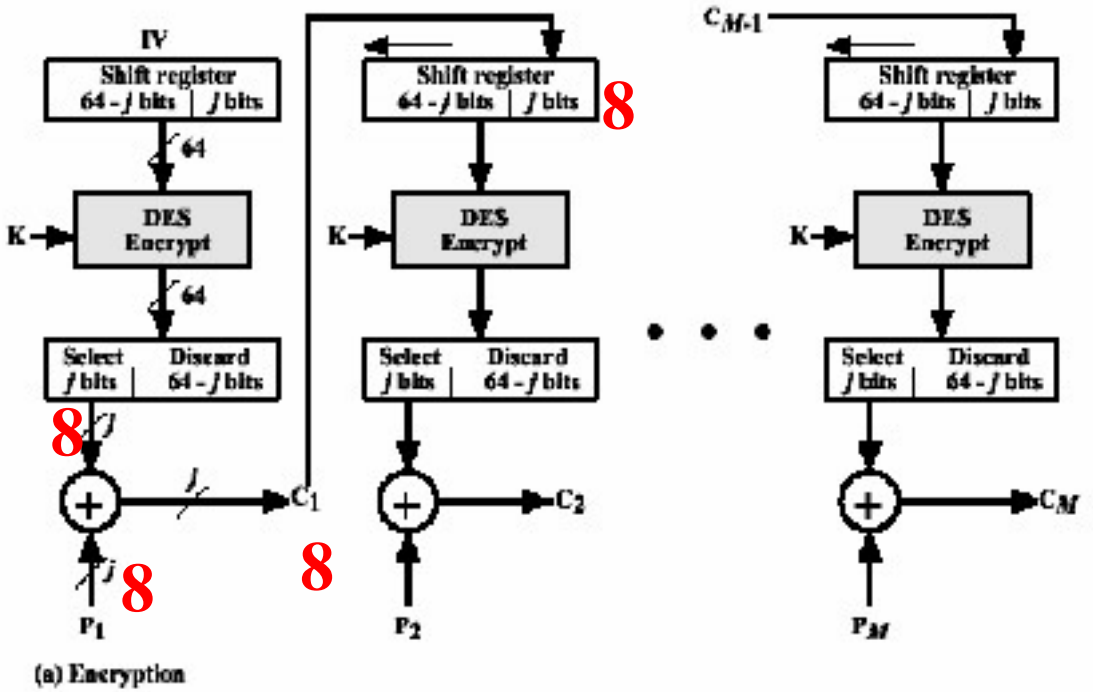
Figure3.11 Electronic Codebook (ECB) Mode

❑ CBC 모드 : 비트

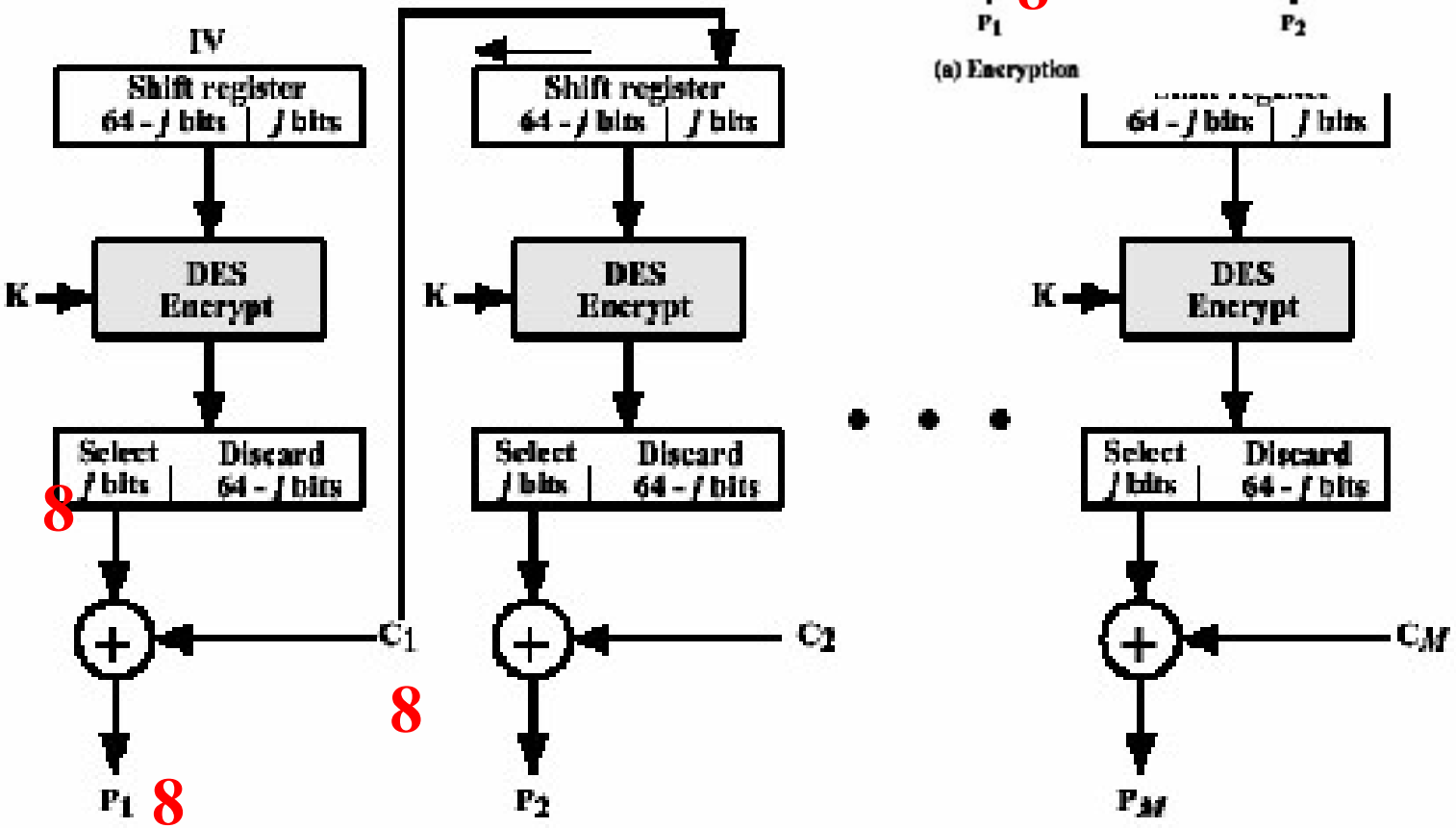

Time = 1
Time = 2
Time = N
IV
P_1
P_2
P_N
C_{N-1}
K
DES Encrypt
C_1
C_2
C_N
(a) Encryption
DES Decrypt
(b) Decryption

CFB 모드

CFC 모드 : 비트

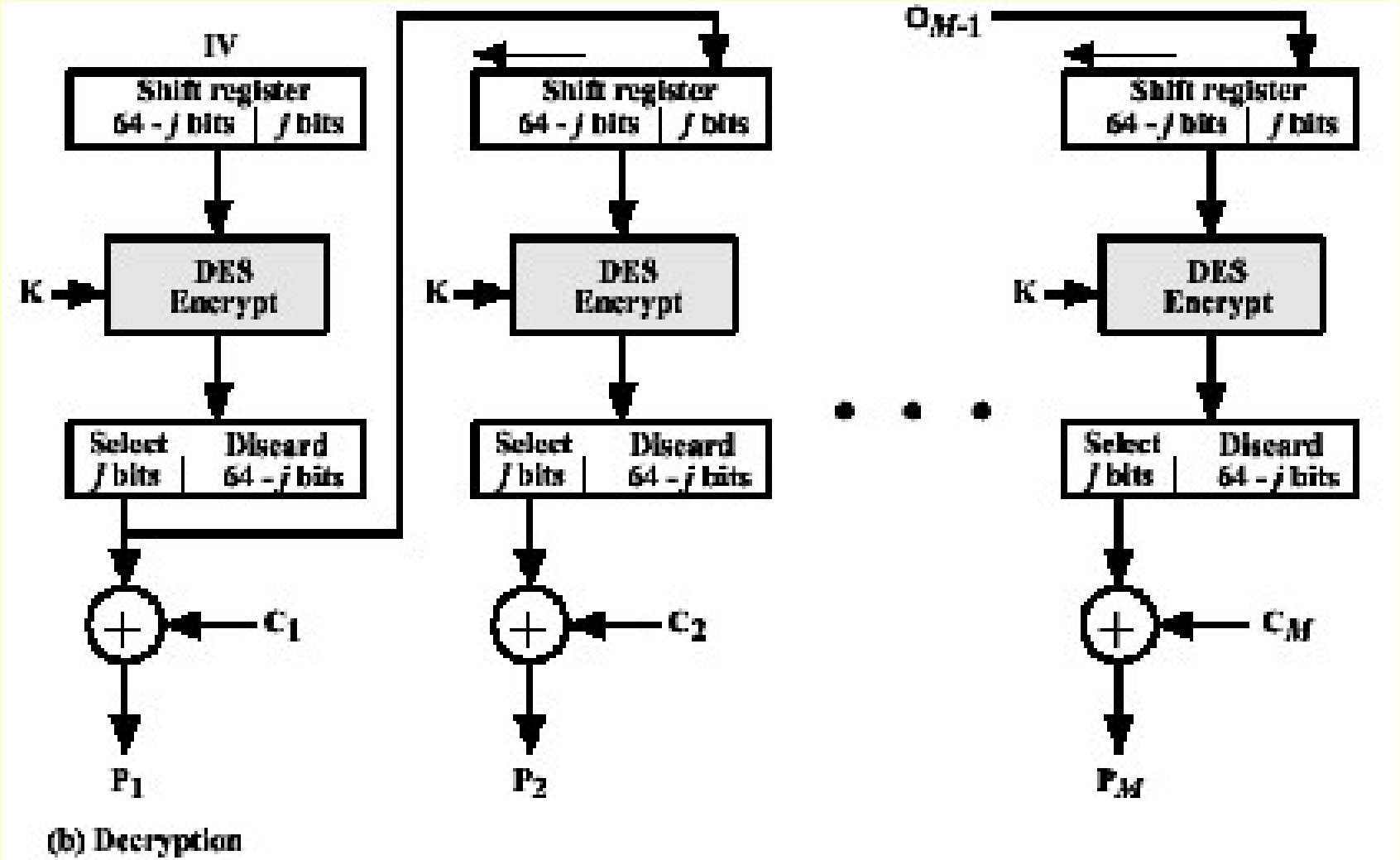


(a) Encryption



(b) Decryption

❑ OFB 모드 : 　　비트



(b) Decryption

< 에러 파급 >

- 전송 중 1비트 에러에 대한 복호시 에러 파급
  - **ECB 모드 : 64비트**
  - **CBC 모드 : 65비트**
  - **CFB 모드 : 65비트**
  - **OFB 모드 : 1비트**

블록 암호의 운용 모드

운용 모드	설명	전형적인 응용
ECB	블록별 독립적으로 암호화 수행	짧은 자료전송 (예: 암호키)
CBC	선행 암호결과를 다음번 암호화할 평문 64 비트와 XOR 하여 암호화 수행	범용 블록형 전송 인증
CFB	한 번에 j 비트씩 선행 암호문과 평문을 XOR 하여 암호화 수행	범용 스트림형 전송 인증
OFB	CFB 와 유사한 방식이지만 한 번에 j 비트씩 암호문 이전의 DES 출력과 평문을 XOR 하여 암호화 수행	잡음있는 채널상의 스트림형 전송 (예: 위성통신)
CTR	평문의 각 블록을 암호화된 카운터와 XOR, 각 단계마다 카운터 증가	일반 용도의 블록형 전송 ATM, IPSec 보안 고속응용