# 암호인재 인력양성 2차 교육

정보컴퓨터공학과 권혁동

한성대학교 HANSUNG UNIVERSITY

CryptoCraft LAB
https://crypto.modoo.at

# Contents



CryptoCraft LAB

# 블록 암호 안전성

- 일반적인 블록 암호의 경우
  - 기밀성 제공 외에도 다양한 용도로 사용
    - MAC, 난수 발생기, 키 유도 함수
  - **따라서 최대한의 안전성을 보장해야 함**
- 일부 블록 암호 (특히 경량 암호)
  - 열악한 구현 환경
  - 구현 환경 상, 일부 공격은 효과적이지 않으므로 **모든 공격을 고려하지 않음**

# 블록 암호 안전성

- 이론적 안전성 (가정)
  - 키가 고정된 블록 암호는 랜덤 함수와 구별이 어려워야 함
  - 블록 길이와 키 길이가 같은 블록 암호들 중에서 랜덤하게 선택됨
- 실용적 안전성 (실제)
  - **키 전수 조사보다 효과적인 공격이 성립하지 않아야 함**
  - 블록 암호를 대상으로 하는 각종 공격에 대한 안전성 제공
    - 차분 공격, 선형 공격, Intgegral 공격, 연관키 공격 등..

# 블록 암호 안전성

- 공격 분류 기준 1: 공격자의 데이터 수집 능력
  - 암호문 단독 공격(ciphertext only): 암호문 만을 사용한 공격
  - 알려진 평문 공격(known plaintext): 주어진 평문과 그에 관한 암호문으로 공격
  - 선택 평문/암호문 공격(chosen plaintext/ciphertext): 공격자가 선택한 평문과 그에 관한 암호문으로 공격
  - 능동 선택 평문/암호문 공격(adaptive chosen plaintext/ciphertext): 공격자가 선택한 평문에 대한 암호문을 획득

# 블록 암호 안전성

- 공격 분류 기준 2: 공격자의 공격 목표
  - 구별 공격(distinguishing): 주어진 값이 공격 대상 블록 암호인지 무작위 수열 인지 구별하는 공격
  - 키 복구 공격(key recovery): 공격자가 보유한 평문/암호문 쌍을 생성하는데 사용된 비밀키를 찾아내는 공격
  - 평문 복구 공격(plaintext recovery): 암호문에 대한 평문을 찾아내는 공격

# 블록 암호 안전성

- 공격 분류 기준 3: 키에 대한 가정
  - 비밀키 공격(secret-key): 키를 비밀 요소로 가정한 공격
    - 단일키 공격(single-key): 하나의 키에서 얻은 평문/암호문을 사용
    - 연관키 공격(related-key): 둘 이상의 연관된 키를 사용하여 획득한 평문/암호문을 이용한 공격
  - 알려진 키 공격(known-key): 공격자가 키를 알고 있다고 가정한 공격
  - 선택 키 공격(chosen-key): 공격자가 키를 선택하여 공격

# 블록 암호 안전성

- 공격 분류 기준 4: 공격에 이용되는 특성
  - 차분을 이용한 공격
    - **차분공격**, 부정차분공격, 불능차분공격, 고계차분공격, 포화공격, 부메랑공격 등
  - 선형근차를 이용한 공격
    - **선형공격**, 다중선형공격, 제로 상관관계 공격, 차분-선형공격 등
  - 기타 특성을 이용한 공격
    - 로테이션 공격, 슬라이드 공격, 대수적 공격, 큐브 공격, 중간일치공격, 바이클릭 공격
  - 특성의 확률 분포
    - 0과 1사이의 확률을 가지는 특성 활용
    - 0 또는 1의 확률을 가지는 특성 활용

# 블록 암호 안전성

- 공격 복잡도
  - 시간 복잡도
    - 공격에 소요되는 **공격자의 계산량**
    - 알고리즘의 가동에 소요되는 시간은 제외
  - 데이터 복잡도
    - 공격에 필요한 **평문/암호문 쌍의 수**
    - 알고리즘 가동 횟수와 동일
  - 메모리 복잡도
    - 공격에 필요한 **메모리의 양**

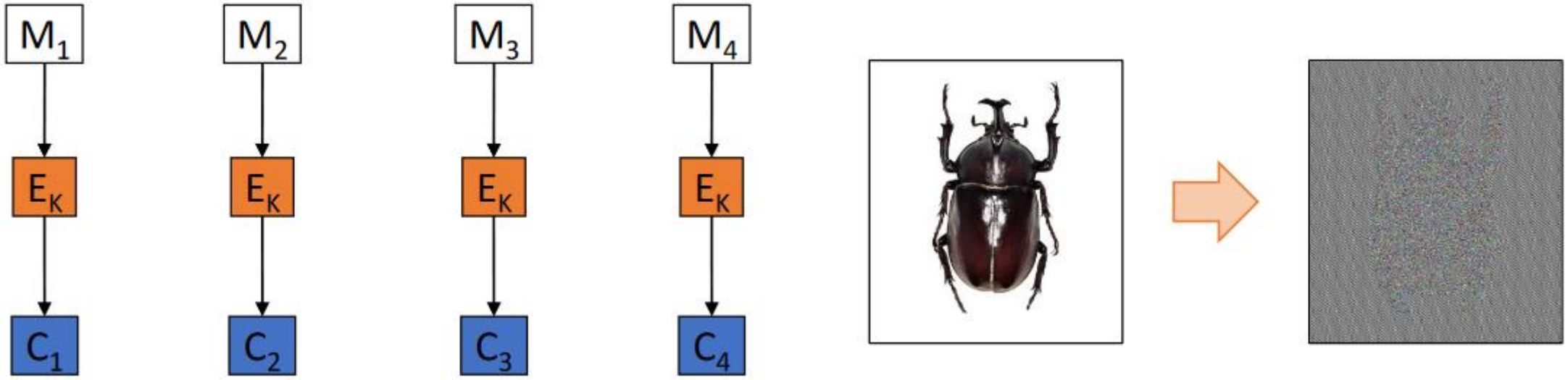
# 블록 암호 운용모드

- 운용모드(Mode of Operation)
  - 블록 암호를 사용하여 **임의 길이의 평문을 암호화하기 위해 필요**
  - 부가기능
    - 메시지 무결성을 제공할 수 있는 운용모드(CBC-MAC)
    - 인증과 암호화를 동시에 제공하는 운용모드(OCB, GCM)
- 운용모드 사용 원칙
  - 블록 암호를 이용할 때, 평문, **IV**, 비밀키가 필요
  - **같은 평문에서 같은 암호문이 생성되지 않아야 함**
    - 동일한 키를 사용한다면, 다른 IV를 사용하도록 설계
    - 비밀키는 수시로 변경되어야 함

# 블록 암호 운용모드

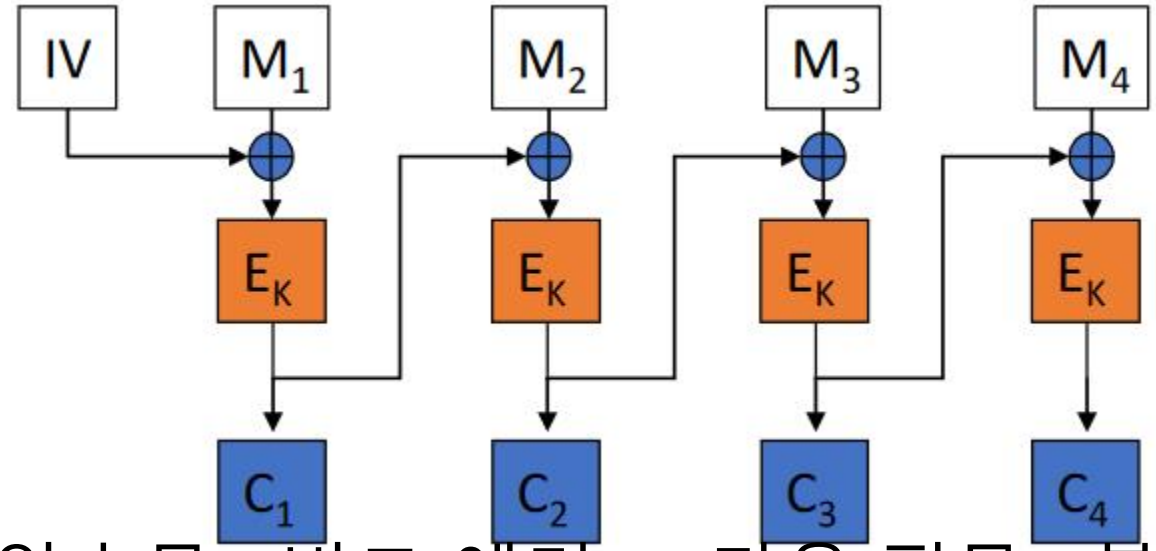
- 5대 기밀성 운용 모드
  - ECB, CBC, CFB, OFB, CTR
- 인증암호화 운용 모드
  - OCB 1.0/2.0/3.0, GCM, CCM
- 저장매체 암호화 모드
  - LRW, XEX, CMC, EME, XTS
- 키랩 운용 모드
  - AES-KW, AES-SIV
- 형태보존 암호화 운용 모드
  - FF1, FF3

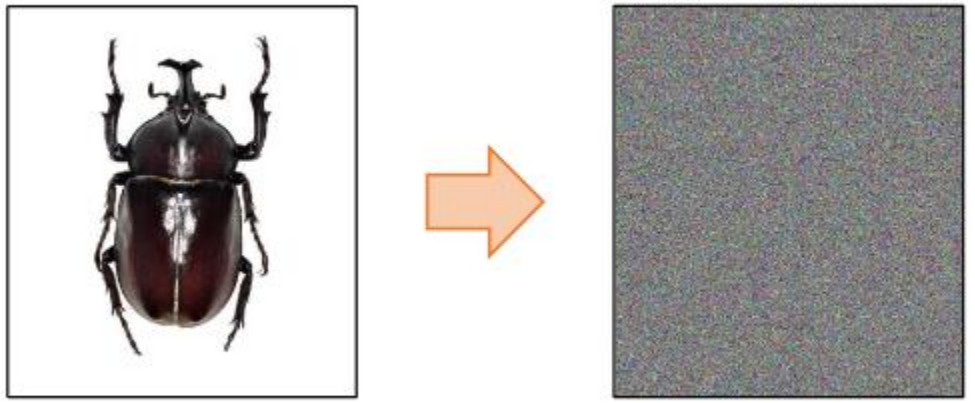
# 블록 암호 운용모드: ECB 모드




- 같은 키를 사용한다면, 같은 평문은 같은 암호문으로 변환
- 암호문 오류가 전파되지 않음
- **평문 크기가 1블록 크기 보다 큰 경우 -> 평문 패턴 노출 위험**
  - 따라서, 일반적인 경우는 ECB를 사용하지 않음
- 1블록으로 표현 가능한 평문 -> ECB 사용 가능

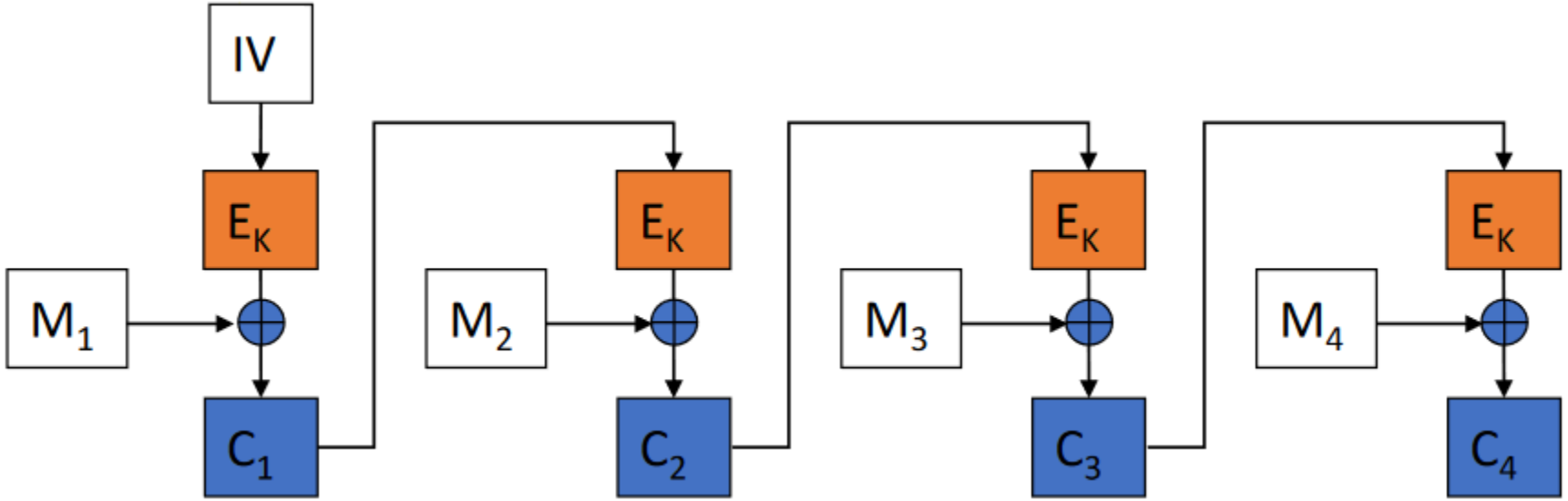
# 블록 암호 운용모드: CBC 모드



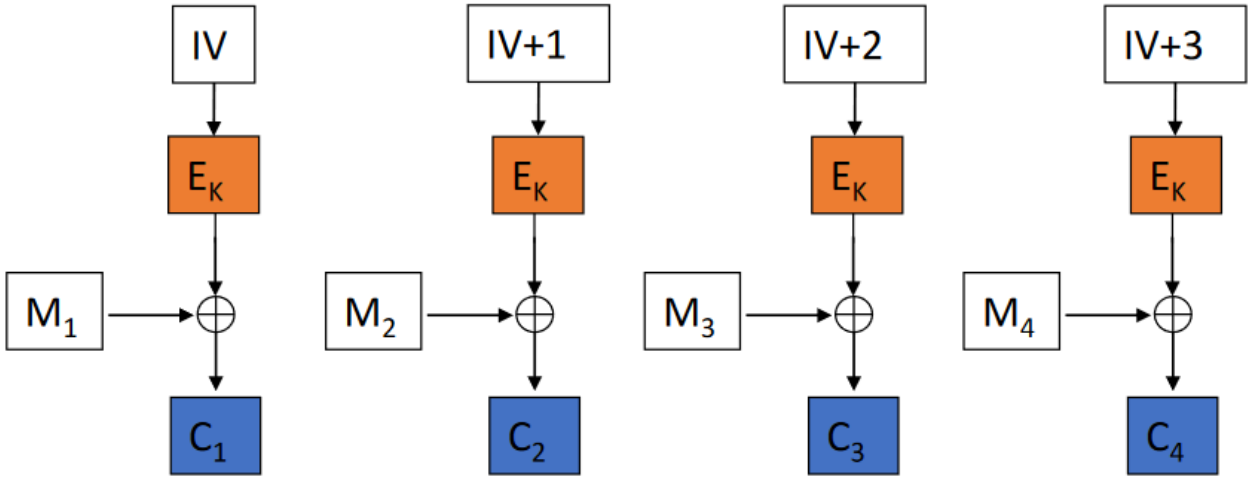
- 암호문 1비트 에러 -> 다음 평문 1블록 에러 전파
- IV 사용에 주의
  - **재사용 시, 평문 정보 일부 노출**
  - IV 조작 = M1 조작
- 암호화에는 병렬처리가 안되지만, **복호화 때는 병렬처리 가능**
- **파일 암호화**에 주로 사용

# 블록 암호 운용모드: CFB 모드



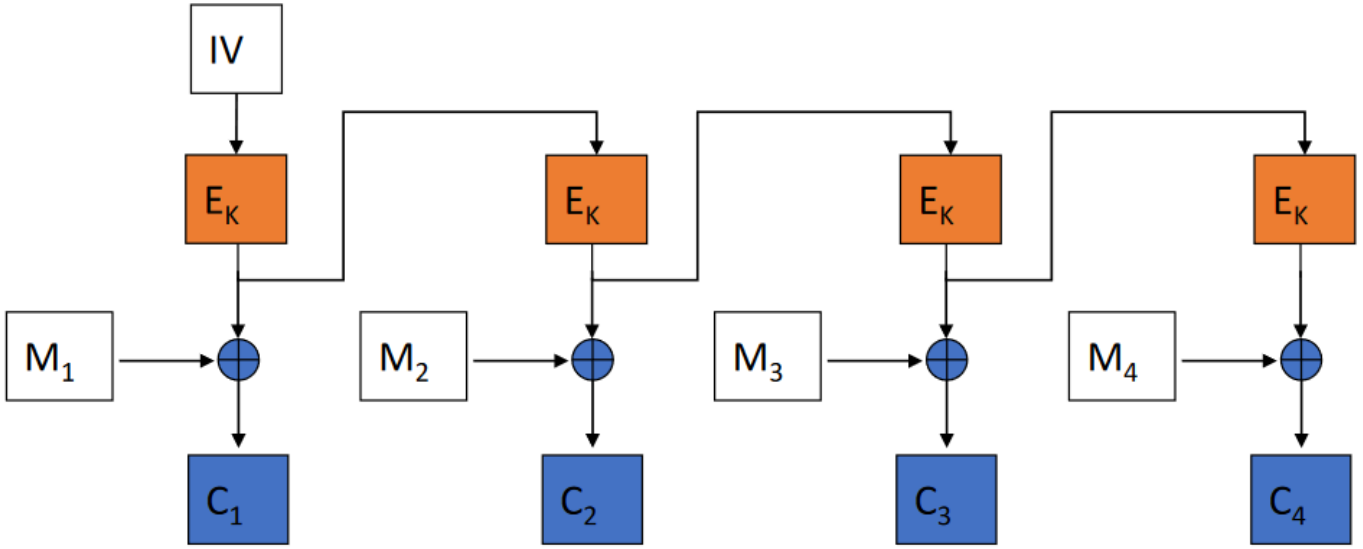

- 스트림모드, 복호화만 병렬화 가능
- IV 재사용시 평문 정보 일부 노출
- 자가동기 기능
  - 암호문 블록이 소실 되어도, **2번째 이후 평문 블록 복구 가능**
- **데이터 유실** 등 동기 이탈이 발생할 가능성이 높을 때 사용

# 블록 암호 운용모드: CTR 모드




- 스트림모드, 병렬화 가능, 사전연산 가능
- **IV 재사용시, 동일한 키 수열이 재사용되므로 매우 위험**
  - IV를 매번 바꿔주어야 함
- **암호화, 복호화 모두 병렬처리 가능**

# 블록 암호 운용모드: OFB 모드




- 스트림모드
- IV 재사용시 동일한 난수열 발생
  - IV를 매번 다른 값으로 사용해야 함
- **암호화, 복호화 모두 병렬화 불가능**

# 블록 암호 운용모드

| 모드 | MB / sec | Cycles / Byte |
|---|---|---|
| AES-ECB | 99 | 17.7 |
| AES-CTR | 96 | 18.1 |
| AES-OFB | 83 | 21.1 |
| AES-CFB | 69 | 25.3 |
| AES-CBC | 84 | 20.9 |

- Crypto++ 5.5 벤치마크
  - Intel Core 2 1.83 Ghz processor
  - 128비트 키