2010-1학기 현대암호학

제 6장. 하이브리드 암호 시스템

박 종 혁

Tel: 970-6702
Email: jhpark1@snut.ac.kr

목차

- 하이브리드 암호 시스템
- 강한 하이브리드 암호 시스템
- 암호 기술의 조합

6.0 주요 내용

- 하이브리드 암호 시스템
  - 대칭 암호의 장점인 빠른 처리속도
  - 비대칭 암호의 장점인 키 배송문제의 편리함
  - 평문을 대칭 암호로 암호화
  - 평문을 암호화 할 때 사용했던 대칭 암호 키를 공개 키 암호로 암호화

- 하이브리드 암호 시스템을 통해, 대칭 암호와 공개 키 암호의 장점을 조합한 통신수행이 가능

6.1 하이브리드 암호 시스템

6.1.1 대칭 암호와 공개 키 암호

- 대칭 암호를 사용하면 기밀성을 유지한 통신이 가능
  - 대칭 암호를 실제로 운용하기 위해서는 키 배송 문제를 해결할 필요가 있음

- 공개 키 암호를 사용하면
  - 복호화에 사용할 키를 배송할 필요가 없어지기 때문에 대칭 암호가 근본적으로 가지고 있는 키 배송 문제를 해결할 수 있음

공개 키 암호의 2가지 큰 문제

(1) 공개 키 암호는 대칭 암호에 비해 처리 속도가 훨씬 느림

(2) 공개 키 암호는 중간자(man-in-the-middle) 공격에 취약

- 하이브리드 암호 시스템 ➔ (1)의 문제를 해결
- (2)의 문제를 해결 ➔ 공개 키에 대한 「인증」 필요 (제 10장에서 소개)

6.1.2 하이브리드 암호 시스템

- 기밀성을 위해 메시지를 일단 고속의 대칭 암호로 암호화

- 대칭 암호 키의 기밀성을 지키것이 필요

  ➔ 공개 키 암호를 사용

  - 메시지를 암호화할 때에 사용한 대칭 암호 키를 데이터로 간주하여 공개 키 암호로 암호화함
  - 메시지의 길이에 비해 일반적으로 대칭 암호 키의 길이는 짧기 때문에 이처럼 짧은 데이터를 암호화 하는데 공개 키 암호의 속도가 느린 것은 별 문제가 되지 않음

하이브리드 암호 시스템의 구조

- 메시지: 대칭 암호로 암호화

- 대칭 암호의 암호화에서 사용한 세션 키
  ➔ 의사난수 생성기로 생성
  - 세션 키는 공개 키 암호로 암호화

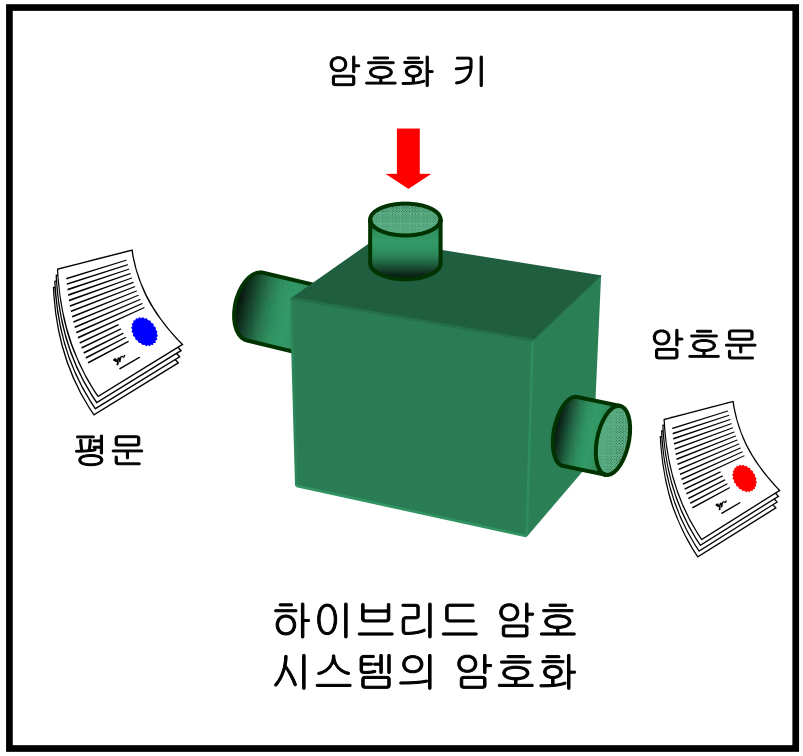
- 공개키 암호의 암호화에서 사용하는 키
  ➔ 하이브리드 암호 시스템의 외부로부터 부여

하이브리드 암호 시스템에 사용되는 3 가지 암호 기술

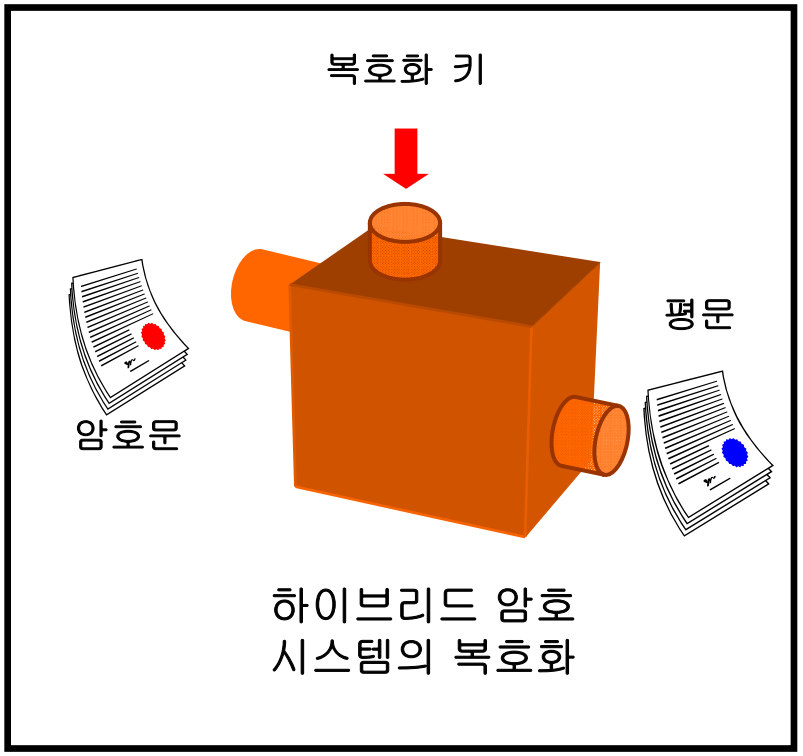
- 하이브리드 암호 시스템의 3가지 암호기술
  - 의사난수 생성기
  - 대칭 암호
  - 공개키 암호

- 하이브리드 암호 시스템
  - 이 3개의 암호 기술을 조합, 대칭 암호와 공개 키 암호의 장점을 갖춘 새로운 암호를 만듦

하이브리드 암호 시스템의 암호화와 복호화



하이브리드 암호
시스템의 암호화

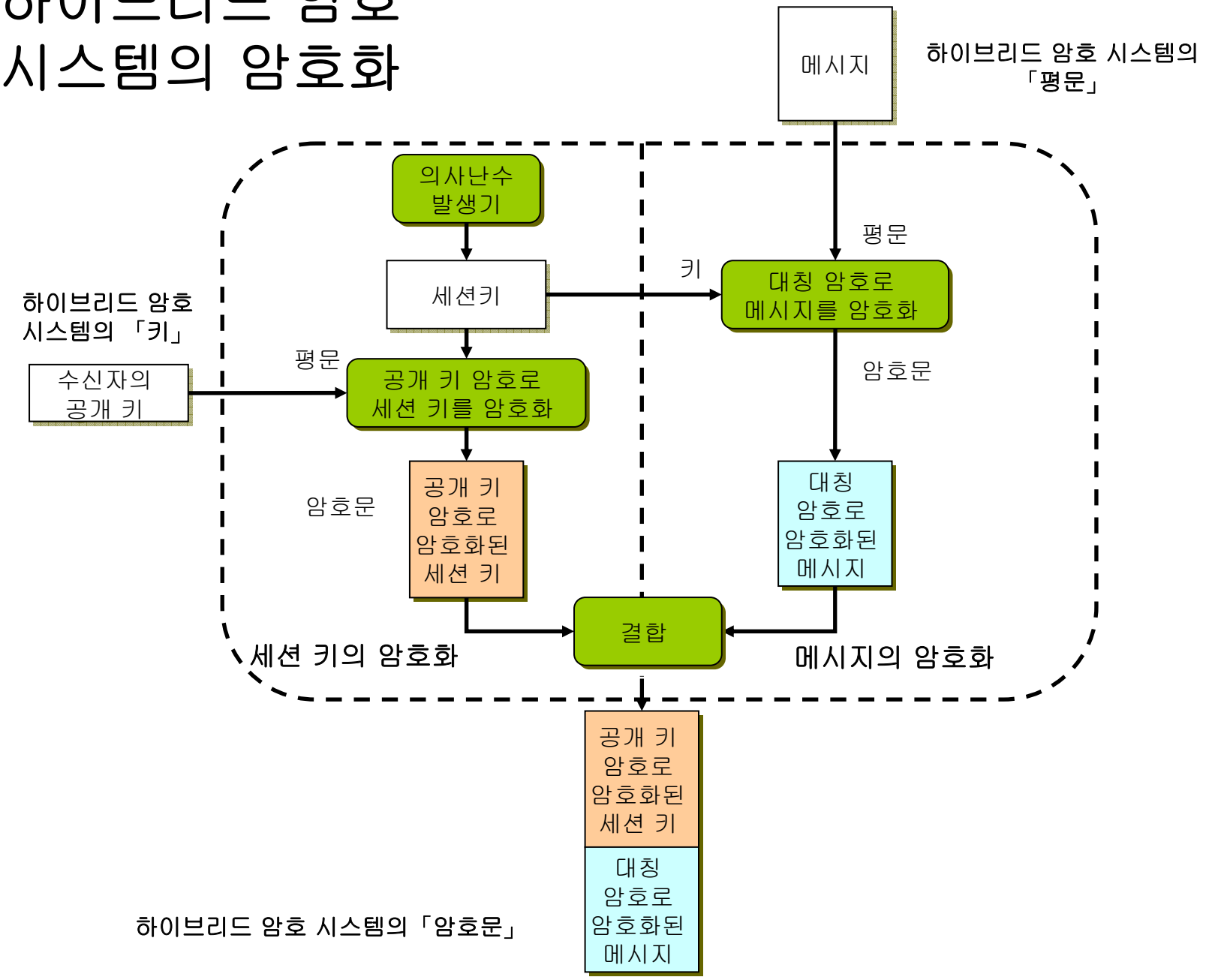


하이브리드 암호
시스템의 복호화

6.1.3 암호화

- 평문・키・암호문
- 메시지의 암호화
- 세션 키의 암호화
- 결합

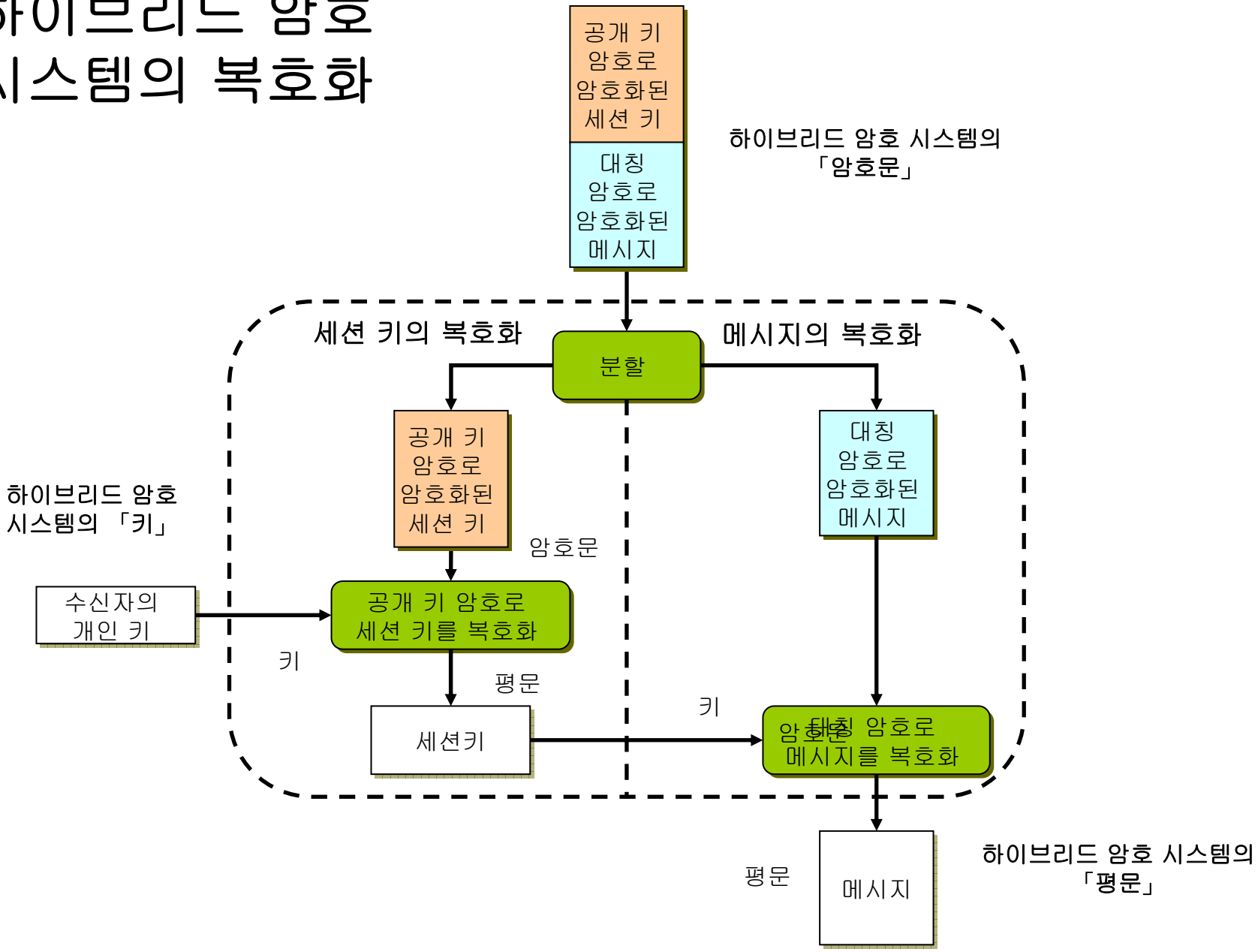
하이브리드 암호 시스템의 암호화



6.1.4 복호화

- 분할
- 세션 키의 복호화
- 메시지의 복호화

하이브리드 암호 시스템의 복호화



6.1.5 하이브리드 암호 시스템의 장점

- 기밀성

- 비대칭 암호 한 가지만 사용해도 기밀성을 보장할 수 있지 않은가?
  - 대칭 암호만 사용하여 기밀성을 보장받기 위해서는
    ➔ 통신을 하는 쌍방이 메시지 암호화에 사용할 세션 키를 사전에 공유해야 함 (세션키 배송의 문제)

  - 하이브리드 암호 시스템
    ➔세션 키를 안전하게 수신자에게 전달하는 역할: 공개키 암호 시스템 부분이 해결

기밀성 뿐만 아니라 속도도 고려

- 처음부터 공개키 암호 한 가지만 사용해도 기밀성을 보장할 수 있지 않은가?
  - 공개키로 암호화를 할 경우
  - 메시지를 복호화 하는 시간이 대칭 암호를 이용할 때보다 적게는 수십 배 많게는 수백 배의 시간이 걸림 (비효율적임)

기밀성 뿐만 아니라 속도도 고려

- 두 컴퓨터나 라우터 등의 경우에는 수신된 암호화된 데이터를 빠른 시간 내에 복호화 할 함
  - 만약 처리 속도가 늦게 되면,

    트래픽이 지체되어 서버나 인터넷 등의 속도가 느려짐

    ➔ 암/복호화 속도 문제도 심각한 문제가 될 수 있음

- 라우터나 기타 대량의 데이터를 처리해야 하는 노드 → 대부분 대칭 암호 시스템을 사용

6.1.6 하이브리드 암호 시스템의 예

- 하이브리드 암호 시스템에서는
  - 공개 키 암호의 처리속도가 느린 것을 대칭 암호로 해결
  - 대칭 암호의 키 배송 문제를 공개 키 암호로 해결
- Web의 암호 통신에서 사용되고 있는 SSL/TLS
- 유명한 암호 소프트웨어인 PGP
- PGP의 처리에서는,
  - 하이브리드 암호 시스템에 추가해서 디지털 서명/서명의 검증, 개인키의 관리라는 처리도 연관됨

6.2 강한 하이브리드 암호 시스템

- 하이브리드 암호 시스템이 의사난수 생성기, 대칭 암호, 공개 키 암호를 조합시킨 것이기 때문
  - ➔ 하이브리드 암호 시스템이 강한 보안성을 갖기 위해 각각의 기술 요소가 강한 보안성을 갖아야함

- 또한 강도의 밸런스도 중요함

6.2.1 의사난수 생성기

- 하이브리드 암호 시스템에서는 세션 키를 만들어 내는 데 의사난수 생성기를 사용

- 의사난수 생성기의 품질이 나쁘면
  - 만들어지는 세션 키를 공격자가 추측하게 될 위험성이 존재
- 의사난수 생성기의 품질이 나쁘다는 의미는 생성되는 의사난수가 진성난수의 특성인 무작위성이나 비주기성 등이 약한 경우를 의미

난수의 생성(1)

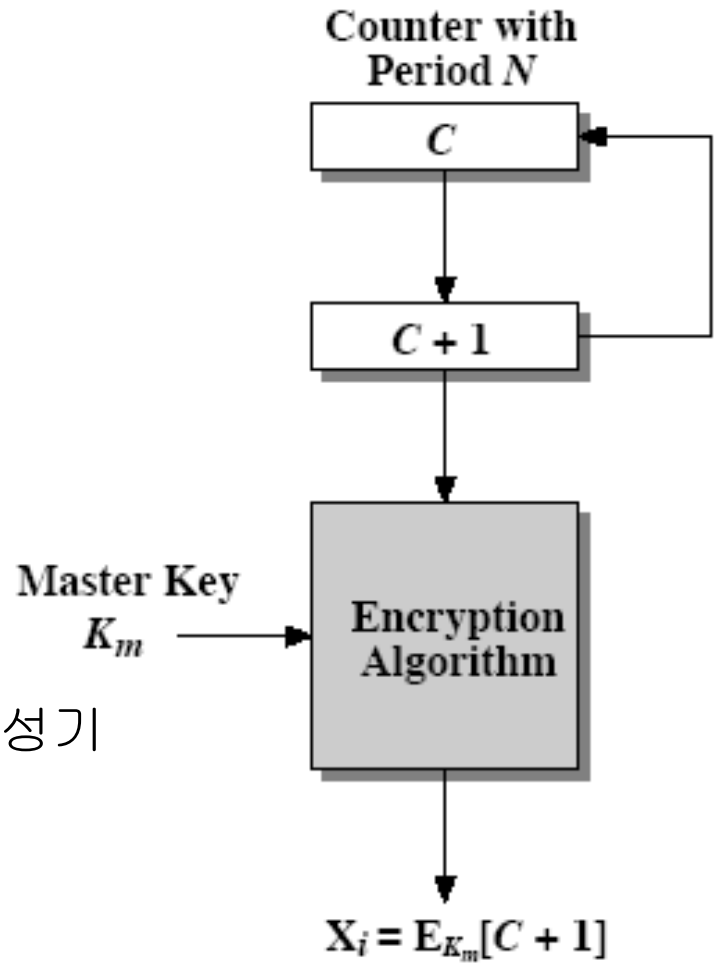
- 암호화의 사용에 중요한 역할
- 난수를 키분배에서 비표로 사용

- 임의성 (Rondomness)
  - 균일 분포
    - 순서상으로 수의 분포가 균일해야 함, 각 수의 출현 빈도가 거의 동일해야 함
  - 독립성
    - 순서상 어떤 값도 다른 값으로부터 추론될 수 없음
- 비예측성 (Unpredictability)
  - 임의적 순서를 갖는 각 수는 다른 수와 통계적으로 독립적이고, 비예측적임

- 난수의 생성
  - 물리적 잡음 생성기 (가스방출 튜브, 누전 축전지 등)
    → 임의성과 정확도에 문제
  - 의사난수(pseudo random number) 사용
    - 통계적으로 임의적이 아닌 일련의 수를 생성
      → 임의성 시험 통과된 수

난수를 생성하는 방법

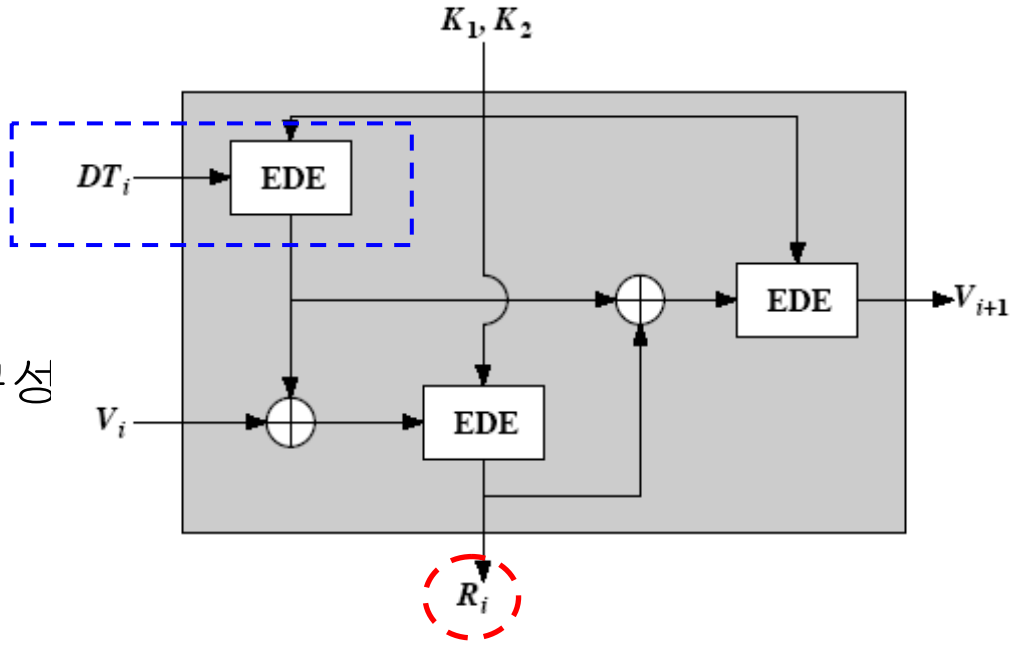
- 순환 암호 방식
  - 주기가 N인 카운터를 암호장치의 입력으로 사용
- DES의 OFB 모드
  - 스트림 암호화 , 키생성에 사용
- ANSI X9.17 의사난수 생성기
  - 암호학적으로 가장 강력한 난수생성기
- Blum Blum Shub 생성기



[카운터를 이용한 의사난수 생성]

ANSI X9.17 의사 난수 생성기

- 입력
  - 두 개의 의사 난수 값이 생성기를 구동
    - 현재의 날짜와 시간을 나타내는 64비트 값 (난수 생성 마다 갱신)
    - Seed 값 (임의의 값으로 초기화되며 생성과정 중 갱신)
- 키
  - 생성기는 3개의 3중 DES 모듈을 사용
- 출력
  - 64비트 의사 난수와 64-비트 seed값으로 구성



6.2.2 대칭 암호

- 하이브리드 암호 시스템에서는 메시지를 암호화할 때 대칭 암호를 사용
- 강한 대칭 암호 알고리즘을 사용하고, 키 길이도 충분히 길게 할 필요가 있음
- 적절한 블록 암호 모드를 사용할 필요가 있음

6.2.3 공개 키 암호

- 하이브리드 암호 시스템에서는 세션 키를 암호화할 때 공개키 암호를 사용
- 강한 공개 키 암호 알고리즘을 사용하고, 키 길이도 충분히 길게 할 필요가 있음

6.2.4 키 길이의 밸런스

- 하이브리드 암호 시스템에서는 대칭 암호와 공개 키 암호 두 가지가 모두 사용
- 어느 쪽인가 한 쪽의 키 길이가 극단적으로 짧으면, 공격이 그쪽으로 집중될 가능성이 있음
- 대칭 암호와 공개 키 암호의 키 길이는 양쪽이 같은 정도의 강도가 되도록 길이를 맞추는 것이 바람직함 (키 길이의 밸런스 중요함)

6.3 암호 기술의 조합

- 하이브리드 암호 시스템에서는 대칭 암호와 공개 키 암호를 조합 ➔ 양쪽의 장점을 살리는 시스템을 구축

- 암호 기술을 조합해서 보다 유용한 시스템을 구축한다는 것은 자주 사용되는 기법

- 3DES는 DES를 3개 조합해서 DES보다도 긴 키 길이를 갖는 대칭 암호를 만듦

암호기술 조합의 예

- 디지털 서명: 일방향 해시 함수 + 공개 키 암호
- 인증서: 공개 키 + 디지털 서명
- 메시지 인증 코드:
  - 일방향 해시 함수+ 키
  - 대칭 암호로부터 만드는 경우
- 의사난수 생성기:
  - 대칭 암호, 일방향 해시 함수, 혹은 공개 키를 사용

Q & A

Thanks