7장. 관용 암호 방식을 이용한 기밀성

박 종 혁

(jhpark1@snut.ackr)

http://www.parkjonghyuk.net

❑ 목 차

1.암호화 함수의 배치

❑ 암호화 함수의 배치

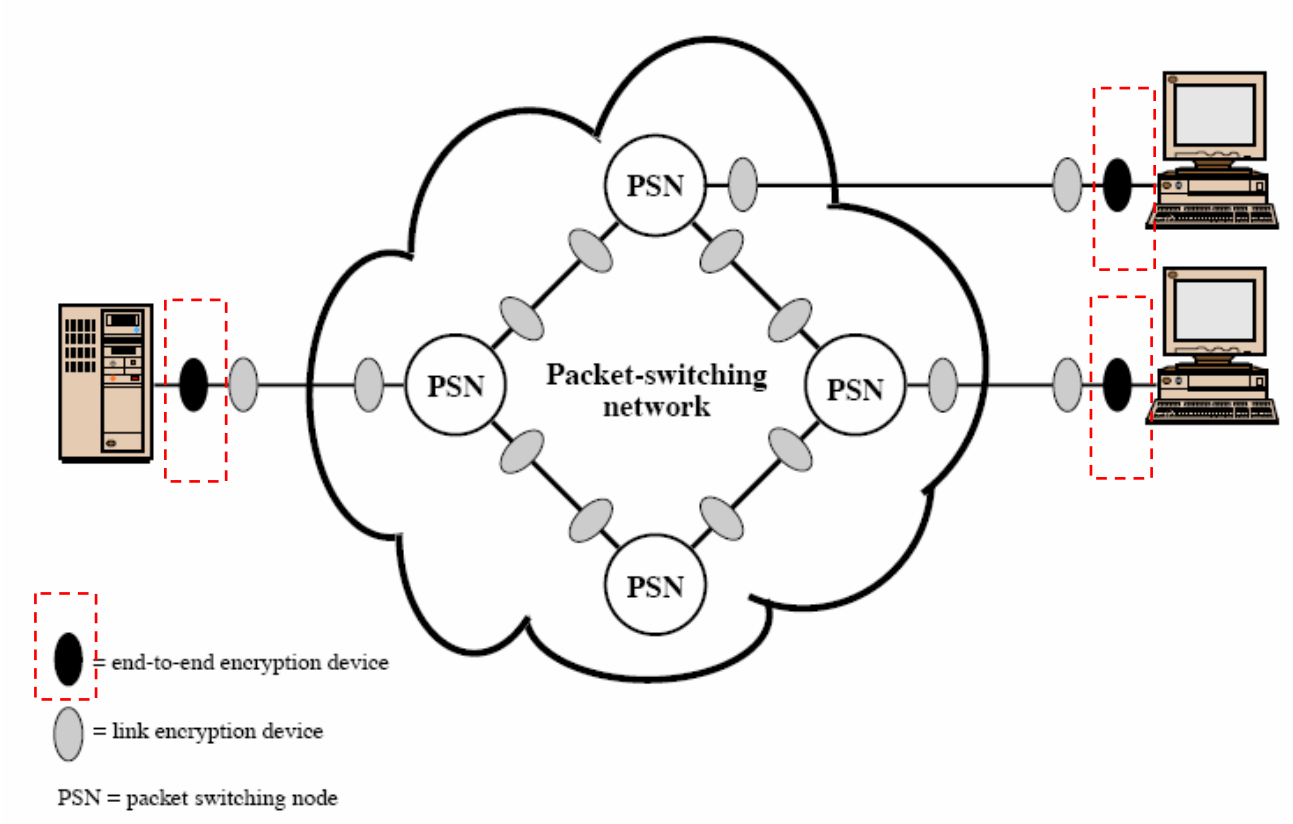
- ❖ 사용자는 LAN이나 또는 브리지와 라우터에 연결된 동일 건물 내 혹은 외부의 서버와 접촉 가능함
- ❖ 배선함 전체는 공격당하기 쉬움
  - ➢ 데이터 전송되는 회선을 찾아 각 선을 도청 가능
- ❖ 무선 통신은 도청의 가능성이 높음
  - ➢ 공격은 소극적 및 적극적 공격이 가능함

❑ 링크 암호화 대 단대단 암호화

- ❖ 링크 암호화 (Link Encryption)
  - ➢ 취약한 통신 링크에 암호화 장치를 양 단 모두에 설치
  - ➢ 모든 통신 링크 상의 모든 트래픽을 보호
    - ▪ 단점 : 패킷 교환기의 복호화에 공격 가능함
- ❖ 단대단 암호화 (End-to-End Encryption)
  - ➢ 암호화 과정은 두 종단 시스템에서 수행
  - ➢ 데이터는 암호화된 형식으로 네트워크를 통하여 목적지 터미널이나 호스트로 변경 없이 전송
  - ➢ 인증기능 제공

❑ 패킷 교환망의 암호화

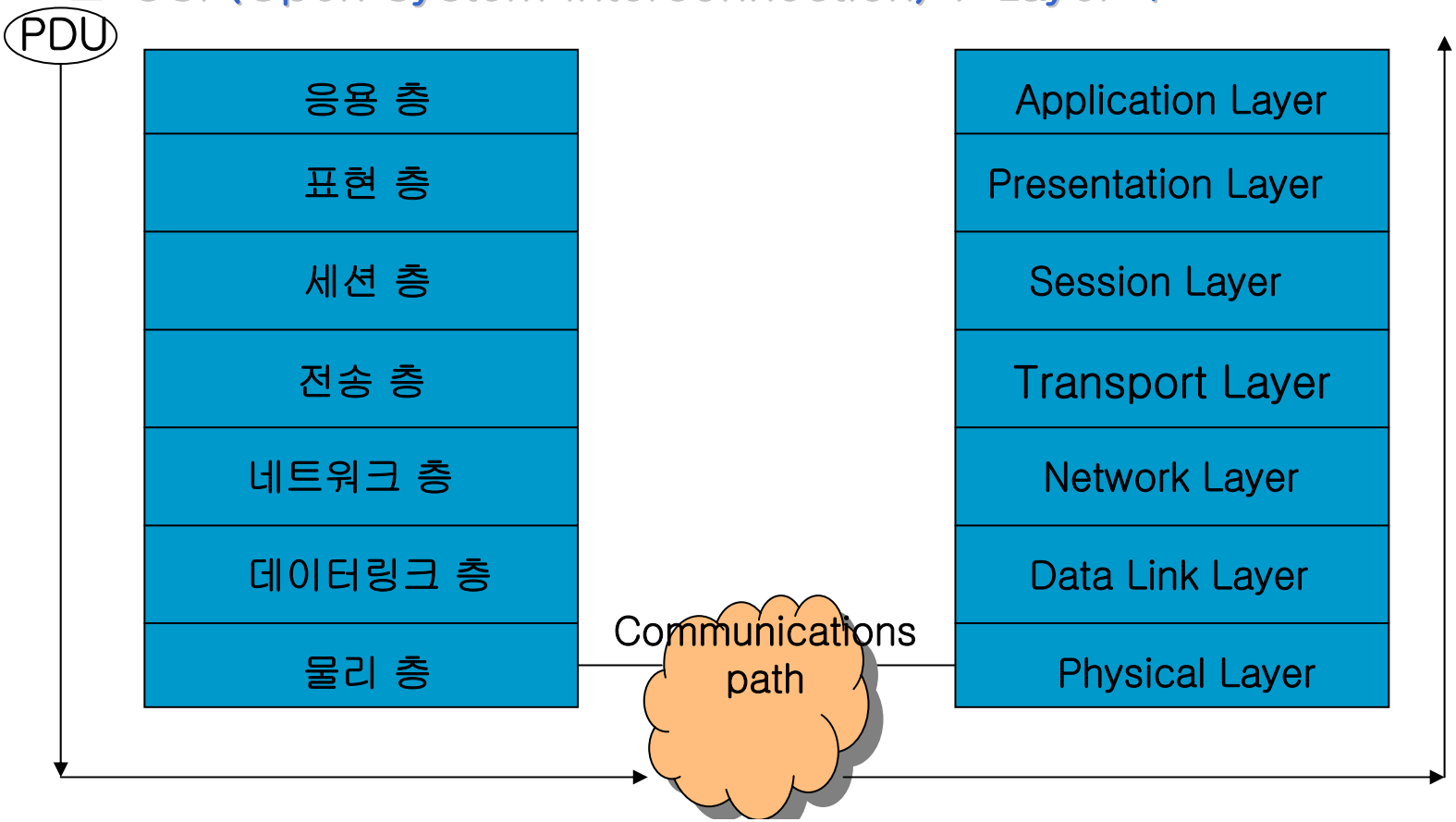
❖ 링크 암호화 및 단대단 암호화



❑ 링크 암호화 및 단대단 암호화의 특징

링크 암호화	단대단 암호화
종단 시스템(ES) 및 중간 시스템(IS) 내의 보안	
송신 호스트에 노출된 메시지	송신 호스트에 암호화된 메시지
중간 노드에 노출된 메시지	중간 노드에 암호화된 메시지
사용자의 역할	
송신 호스트에 의해 적용	송신 프로세스에 의해 적용
사용자에 투명	사용자가 암호화 적용
호스트가 암호화 설비 유지	사용자가 알고리즘 결정
모든 사용자를 위한 하나의 설비	사용자가 암호 기법 선정
하드웨어 내에서 암호화 가능	소프트웨어 구현
전체 메시지의 암호화 또는 아무 메시지도 암호화 안함	각 메시지에 대해 사용자가 암호화 여부 선택
적용상의 고려 사항	
ES_IS 및 IS_IS쌍당 하나의 키 필요	사용자 쌍당 하나의 키 필요
호스트 인증 제공	사용자 인증 제공

❑ OSI (Open System Interconnection) 7 Layer 구조

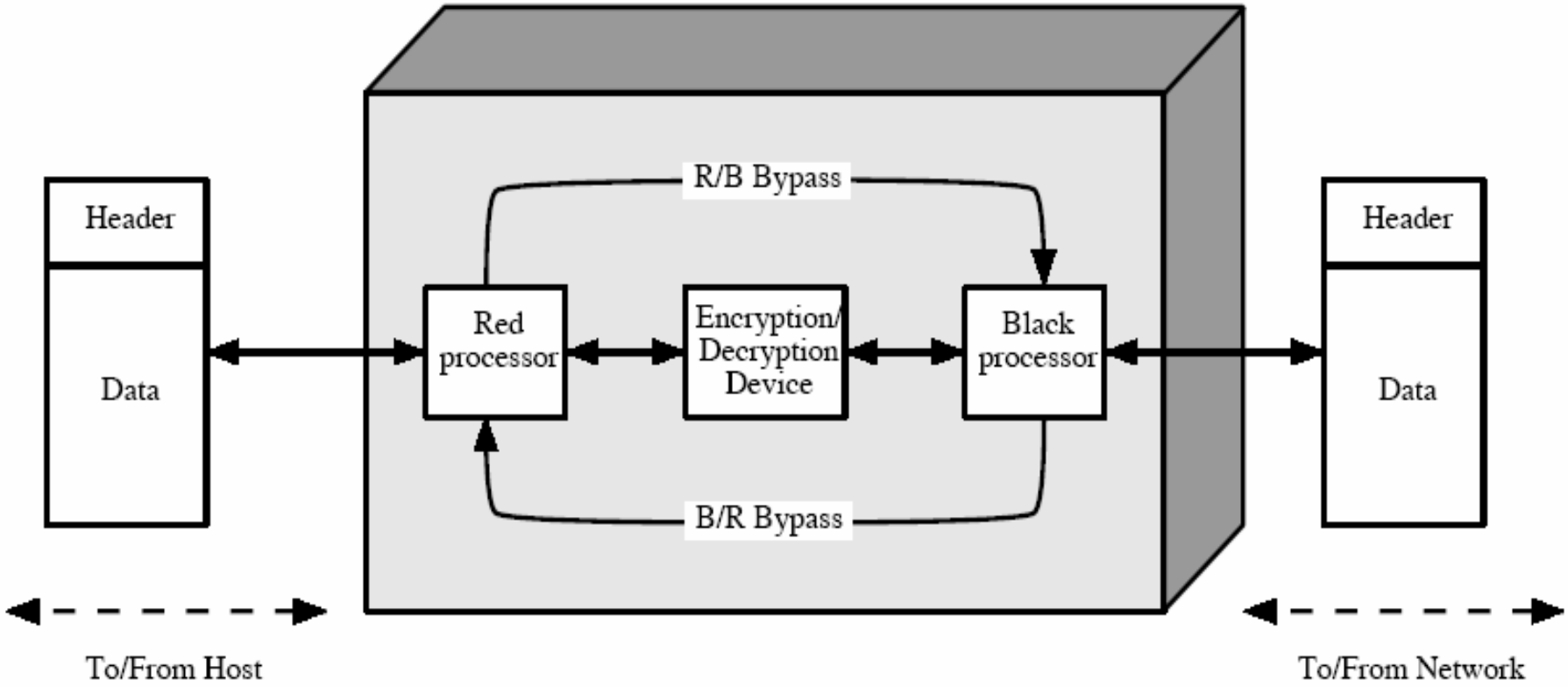


데이터 단위

- PDU (protocol data unit):동등 계층 사이에 주고받는 데이터 형식
  - SDU (service data unit) :상,하위 계층간 서비스 요청시 주어진 데이터 형식
  - PCI (protocol control information):프로토콜의 제어정보

❑ 전위 처리기(Front-End Process : FEP)의 암호화 기능

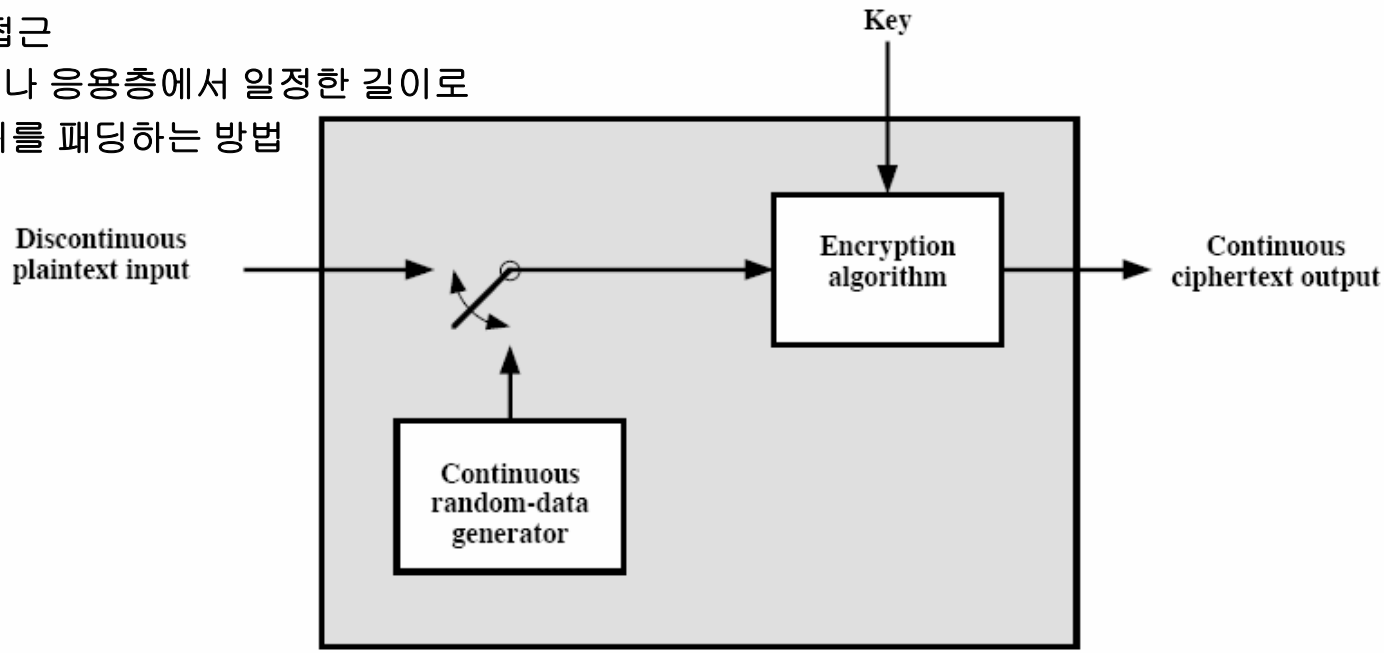
- ❖ 패킷의 헤더는 암호화되지 않는 반면 그 패킷의 사용자 데이터 부분은 암호화
- ❖ 적과 흑이라는 용어로 적색 데이터는 암호화 되지 않는 기밀 또는 비밀 데이터이며, 흑색 데이터는 암호화된 데이터 임



2. 트래픽 기밀성

❑ 트래픽 기밀성

- ❖ 트래픽 분석 공격으로 얻을 수 있는 정보
  - ➢ 파트너들의 신원
  - ➢ 파트너들의 통신 빈도
  - ➢ 중요한 정보가 교환되고 있음을 제시해 주는 메시지 패턴, 메시지 길이 또는 메시지 양
  - ➢ 특정 파트너 사이의 특별한 대화와 관련된 사건
- ❖ 링크 암호화 접근
  - ➢ 네트워크 계층의 헤더 (프레임 / 셀헤더)를 암호화
  - ➢ 공격자의 트래픽 양 관찰의 위험이 여전히 남아있음 → 효과적대처방안: 트래픽 패딩
- ❖ 단대단 암호화 접근
  - ➢ 트랜스포트나 응용층에서 일정한 길이로 데이터 단위를 패딩하는 방법



[트래픽 패딩 암호화 장치]

3. 키의 분배

❑ 키의 분배 기술의 정의

- ❖ 데이터를 교환하고자 하는 양측에 침입자들이 알지 못하도록 키를 전달하는 방법

❑ 관용 암호방식의 키 요구사항

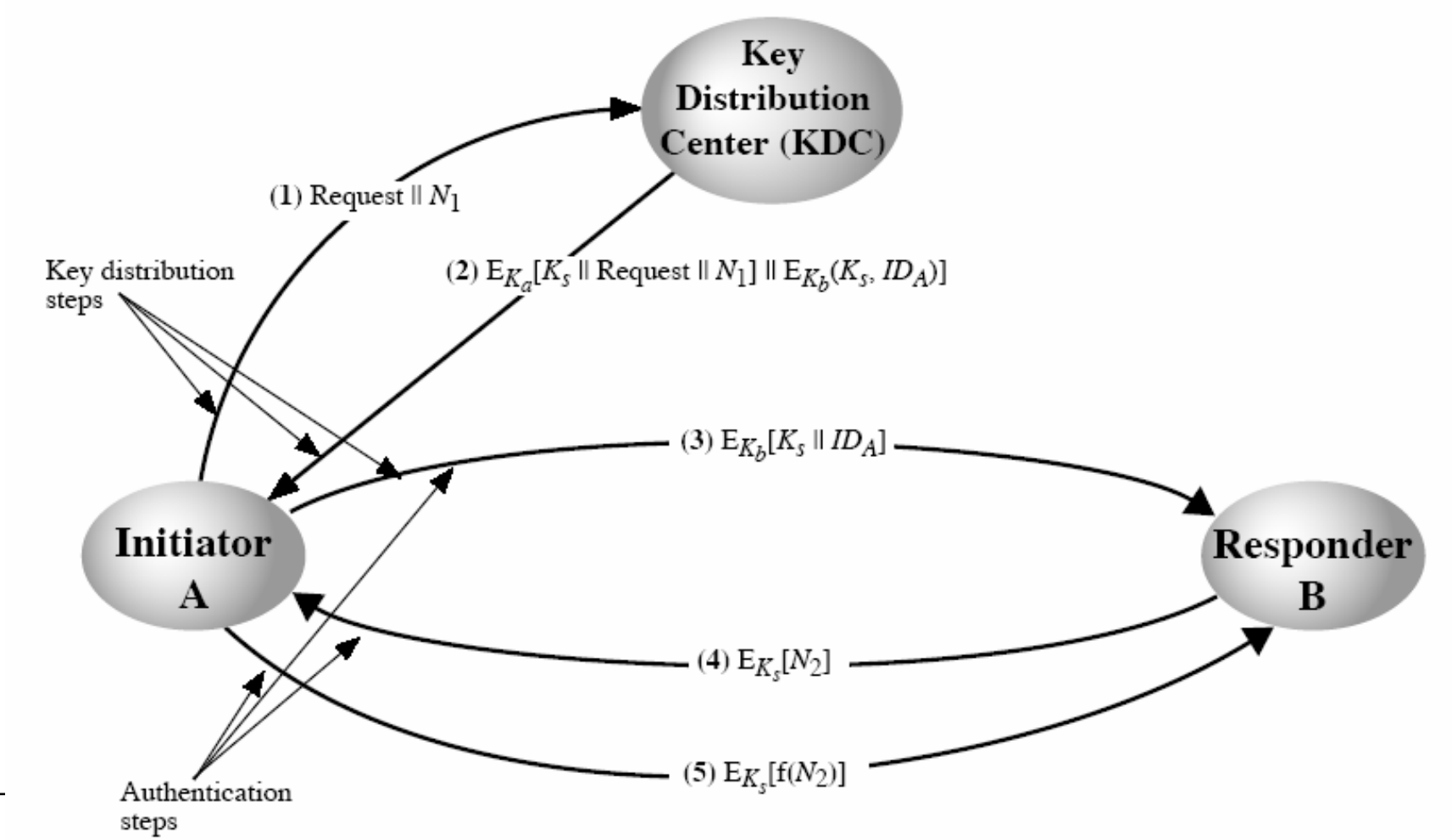
- ❖ 양측이 동일한 비밀키를 공유할 것
- ❖ 키를 제3자가 모르게 보호할 것
- ❖ 키를 적당한 주기로 변경할 것
  - ➢ 공격 당한 키의 손상범위를 제한
- ❖ 효과적인 키 전달 기술을 강구할 것

❑ 키 분배의 여러가지 방법

- ❖ A가 키를 선택하여 물리적으로 B에게 전달
- ❖ 제 3자가 키를 선택하여 물리적으로 A와 B에 전달
- ❖ A와 B가 최근에 사용한 키로 새로운 키를 암호화하여 전송
- ❖ A와 B가 각각 제 3자 C에 암호화된 연결을 갖고 있으면,
  C는 키를 그 암호화된 연결을 통해서 A와 B에게 전달 (가장 일반적으로 사용)

❑ 키 분배 시나리오

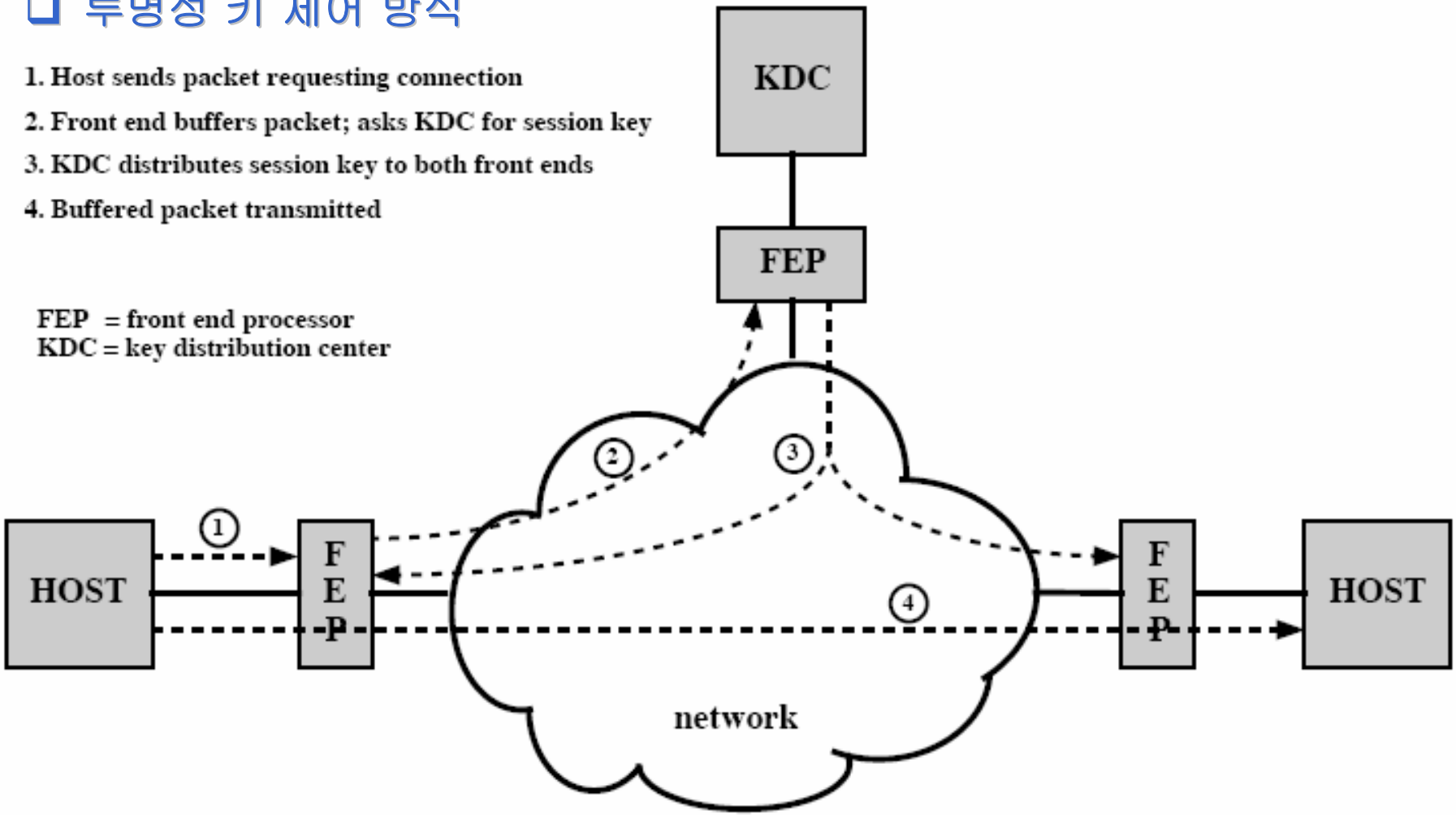
❖ 각 사용자는 키 분배 센터와 유일한 마스터 키를 공유 함



❑ 투명성 키 제어 방식

1. Host sends packet requesting connection
2. Front end buffers packet; asks KDC for session key
3. KDC distributes session key to both front ends
4. Buffered packet transmitted

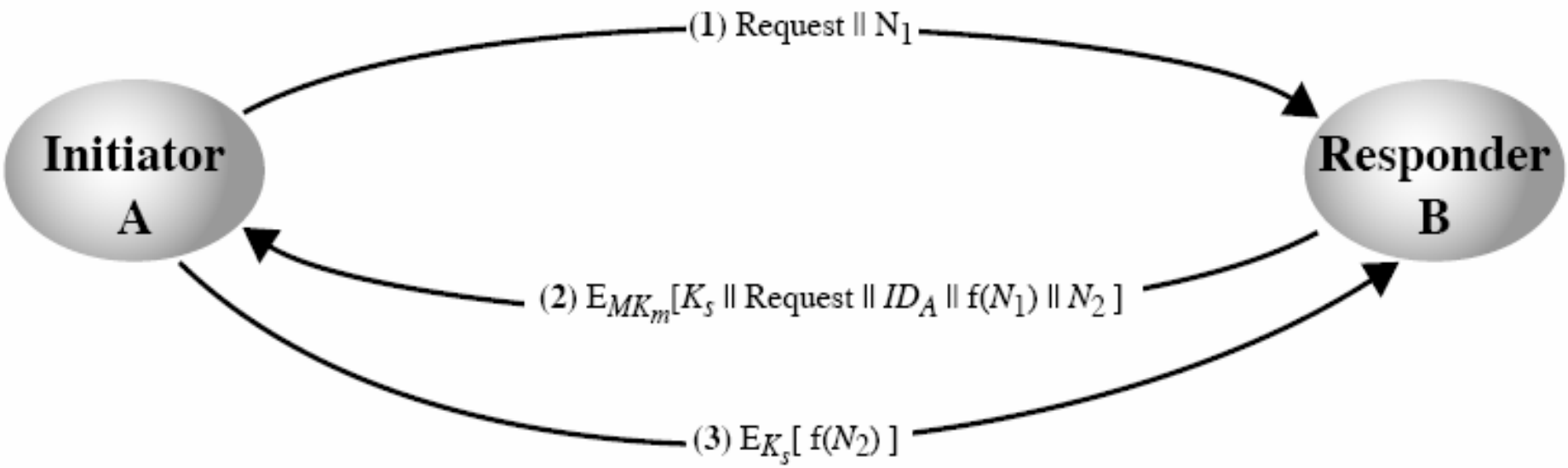
FEP = front end processor
KDC = key distribution center



[연결형 프로토콜을 위한 자동 키분배]

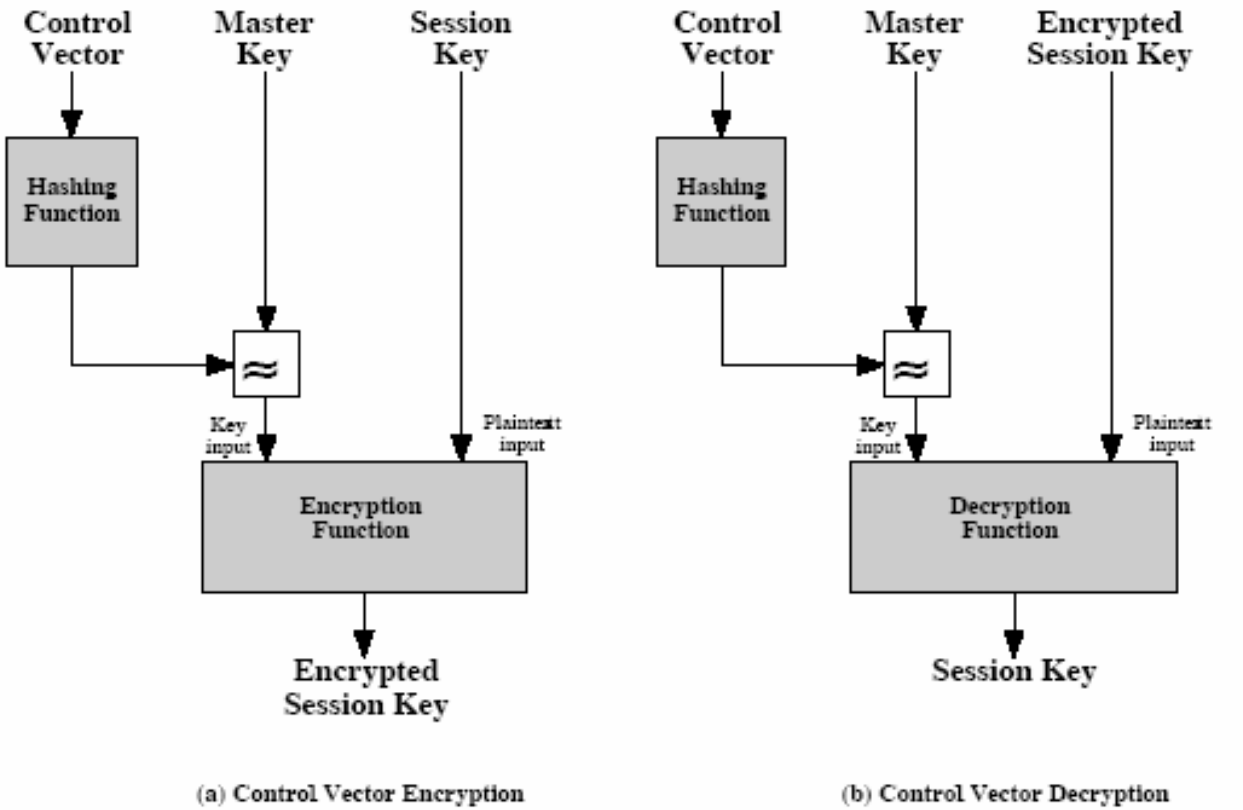
❑ 분산 키 제어

❖ 분산 키 방법은 지역 네트워크 환경에서 유용한 방법



❑ 키 사용에 대한 제어

- ❖ 세션키와 마스터키의 분리
- ❖ 키의 특성에 따라 키의 사용방법을 제한하는 제어방식이 바람직함
  - ➢ 예) **DES**키의 추가 **8**비트
- ❖ 제어벡터를 이용한 키사용



(a) Control Vector Encryption (b) Control Vector Decryption

≈ : XOR

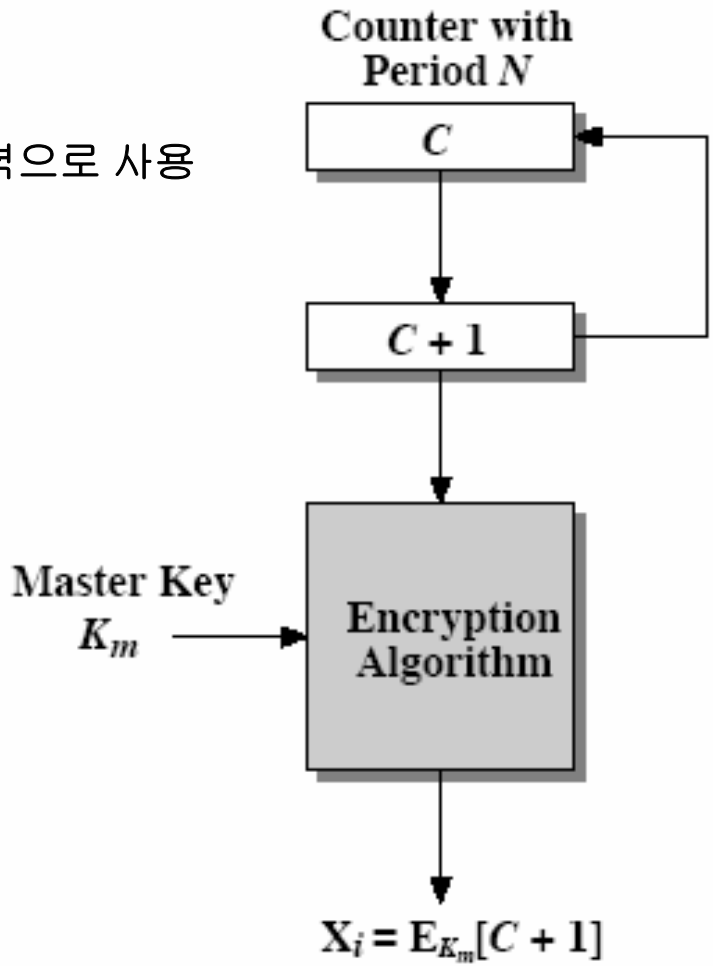
4. 난수의 생성

❑ 난수의 생성

- ❖ 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

❑ 암호학적으로 생성된 난수

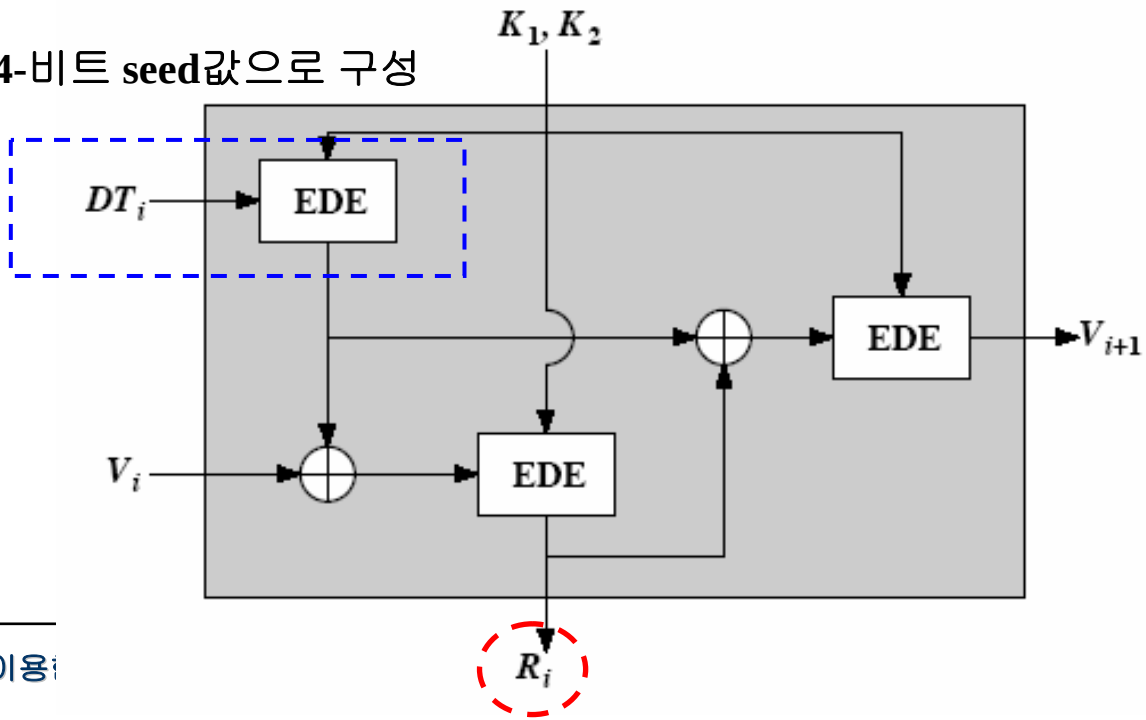
- ❖ 순환 암호 방식
  - ➢ 주기가 N인 카운터를 암호장치의 입력으로 사용
- ❖ DES의 OFB 모드
  - ➢ 스트림 앙호화 , 키생성에 사용
- ❖ ANSI X9.17 의사난수 생성기
  - ➢ 암호학적으로 가장 강력한 난수생성기
- ❖ Blum Blum Shub 생성기



[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



Thanks

Q & A