# 암호기술 개요

NOTE 01



한국기술교육대학교 컴퓨터공학부 김상진

sangjin@koreatech.ac.kr
www.facebook.com/sangjin.kim.koreatech

## 교육목표

- 정보보호 서비스와 암호기술
  - 비밀성, 무결성, 인증, 부인방지, 프라이버시
- 통신계층과 암호기술
- 암호기술 관련 기본 용어
- 암호기술의 한계

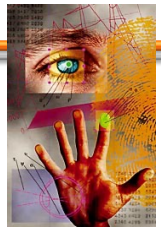
- 정보보호 서비스는 응용의 보안 요구사항을 말함
- 이 교과에서 고려하는 응용은 주로 통신 프로토콜을 이용하여 이루어짐
- 통신 프로토콜은 원격에 있는 참여자 간의 메시지 교환을 통해 진행되는 프로토콜을 말함

# 보안 목적 (1/4)

- 비밀성(confidentiality, secrecy, privacy): 인가된 개인, 단체, 장치, 프로세스만 데이터의 내용을 볼 수 있도록 해주는 서비스 (기밀성)
  - 예) 웹 서비스에서 통신 채널로 전달하는 패스워드
  - 고려 요소: 데이터의 중요도, 비밀을 유지해야 하는 기간(cover time)
    - 고려 요소에 따라 처리하는 방법(보안 강도)이 다름
- 무결성(integrity): 비인가된 데이터의 변경을 발견할 수 있도록 해주는 서비스
  - 예) 인터넷 뱅킹에서 이체 금액
  - 변경의 종류: 삽입, 삭제, 교체
  - 비밀성은 보장해야 하는 서비스이지만 무결성은 발견만 할 수 있으면 됨



# 보안 목적 (2/4)



- 인증(authentication): 식별(identification)+검증(verification)
  - 주장된 것을 검증하는 것
- 유형
  - 메시지 인증: 무결성과 같음
  - 메시지 원천지 인증: 무결성 + 메시지가 송신된 위치 또는 송신자를 검증
    - 위치(정보보호에서 보통 중요하지 않음)와 무관하게 서비스를 이용할 수 있어야 함. 하지만 보안 향상을 위해 위치나 기기 인증을 활용 가능
  - 개체 인증(entity authentication): 주장된 신원을 검증 (최근성 필요)
- 개체 인증을 위해 사용하는 요소
  - 사용자만이 알고 있는 지식 (what one knows): 예) 패스워드
  - 사용자만의 독특한 특징 (what one is): 예) 생체정보
  - 사용자만이 가지고 있는 것 (what one have): 예) ID 카드
- 2가지 요소를 함께 이용하면 2-factor 인증이라 함
  - 참고. 2단계 인증(2 step identification/verification)

# 보안 목적 (3/4)

- 부인방지(non-repudiation): 개체가 지난 행위나 약속(commitment)을 부인하지 못하도록 하는 서비스
  - 보통 제3자가 확인할 수 있어야 함
- 메시지 송수신과 관련된 부인방지
  - 송신 부인방지(Non-Repudiation of Origin, NRO)
  - 전달 부인방지(Non-Repudiation of Delivery, NRD)
  - 제출 부인방지(Non-Repudiation of Submission, NRS)
  - 수신 부인방지(Non-Repudiation of Receipt, NRR)

| 서비스 | 부인방지 내용 | 부인자 | 제공자 |
|---|---|---|---|
| NRO | 메시지의 송신 | 송신자 | 송신자 |
| NRR | 메시지의 수신 | 수신자 | 수신자 |
| NRS | 메시지의 제출 | 메시지 전달 기관 | 메시지 전달 기관 |
| NRD | 메시지의 수신 | 수신자 | 메시지 전달 기관 |

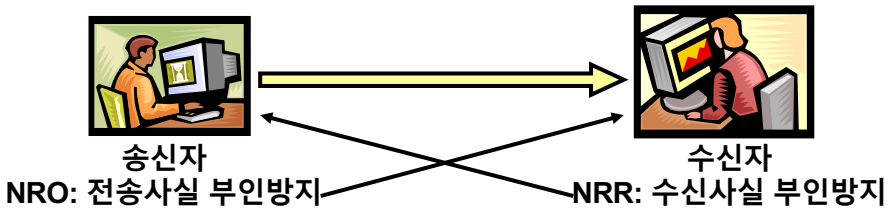
ISO/IEC 13888



# 보안 목적 (4/4)

- 부인방지 모델

- 보통 통신 메시지는 동시에 서로 교환하는 것은 아님
- 한 쪽이 메시지를 보내면 그것에 반응하여 메시지를 보내는 형태임
- 공정한 교환(fair exchange)이라는 개념도 있음



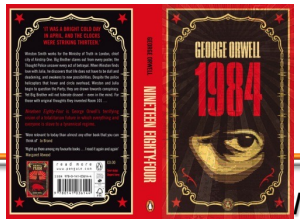


NRS: 제출된 사실 부인방지(중계자에 의한 부인)
NRD: 중계된 사실 부인방지(수신자에 의한 부인), NRR이 포함됨

- 직접 통신하는 경우와 중계자를 이용하여 통신하는 경우가 있음
- 부인방지 토큰은 보통 해당 행위를 부인할 수 있는 주체가 제공해야 하는 것임

# 프라이버시 (1/4)

- 정보화의 부작용 중 오늘날 큰 이슈가 되고 있는 것 중 하나가 프라이버시(privacy) 침해임
- 프라이버시란 개인이나 집단이 자신 또는 자신의 정보를 선택적으로 노출할 수 있는 권리를 말함
  - 개인은 자신과 연관된 정보가 수집되고 저장되는 것(by whom, to whom)을 직접 제어하거나 영향을 줄 수 있어야 함
  - 프라이버시는 매우 광범위한 의미를 지니고 있음
  - 정보보호에서 관심을 가지고 있는 것은 개인정보 노출을 포함하여 컴퓨팅 서비스를 사용하는 과정에서 침해되는 프라이버시를 보호하는 것임
    - 사용자의 익명성(anonymity)을 보장하는 것과 유사함
- Big Brother: George Orwell의 소설 1984에 나오는 등장인물로서 소설에 등장하는 나라의 독재자임. 이 독재자는 모든 국민을 완전히 감시할 수 있음
  - "Big Brother is watching you"





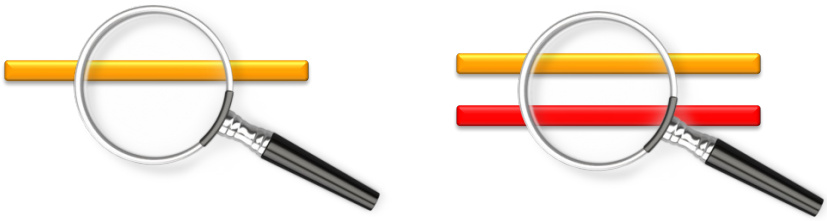

# 프라이버시 (2/4)

- 디지털 서비스를 사용할 때 교환된 통신 메시지를 통한 노출을 고려함
- 누구로부터 프라이버시를 보호: 보통 제3자
  - 서비스 제공자도 알 수 없도록 하기는 힘듦
- 프라이버시의 종류
  - 내용 프라이버시: 예) 사용자가 유투브 서비스를 이용하고 있는데, 어떤 동영상을 보고 있는지 숨기고 싶은 것을 말함
    - 비밀성 서비스를 통해 제공할 수 있음
  - 행동 프라이버시: 예) 사용자가 유투브 서비스를 사용하고 있는 것 자체를 숨기고 싶은 것을 말함. 익명기술을 사용하여 제공함
  - 위치 프라이버시: 예) 사용자가 어디서 유투브 서비스를 이용하고 있는지 숨기고 싶은 것을 말함
    - 위치 추적(location tracing): 사용자의 행적을 추적하는 것을 말함
      - 예) 핸드폰, 하이패스, 신용카드, CCTV, 출입카드 등 오늘날 비교적 쉽게 사용자의 행적을 알 수 있음

https://proxify.com/
https://www.privateinternetaccess.com/pages/browse-anonymously/

# 프라이버시 (3/4)

- 행동 프라이버시 보장을 위한 요구사항
  - 요구사항 1. 불관찰성: 특정 메시지의 송신자 또는 수신자를 알 수 없어야 한다는 것을 말함
  - 요구사항 2. 불연결성: 두 개의 메시지가 주어졌을 때, 두 개의 메시지가 동일 송신자가 전송한 것인지 또는 두 개의 메시지가 동일 수신자에게 보내는 것인지 연결할 수 없어야 한다는 것을 말함
    - 예1) 익명 게시판에 같은 익명으로 계속 글 게시
    - 예2) 비트코인에서 같은 지갑을 이용하여 거래함
  - 불연결성은 특정 메시지의 불관찰성이 깨졌을 때 그 파급효과를 최소화기 위해 제공되어야 함





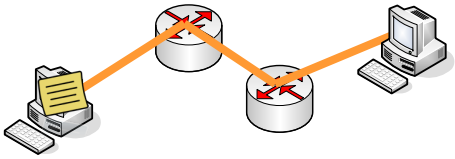
# 프라이버시 (4/4)

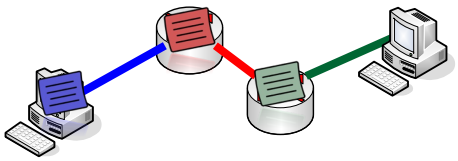
- 완전 프라이버시를 제공하면 사용자들에 의해 악용될 수 있기 때문에 이 대신에 조건부 프라이버시(conditional privacy)를 제공함
  - 조건부 프라이버시가 제공되면 신뢰할 수 있는 기관은 필요할 경우 특정 메시지의 익명을 철회(revocation)할 수 있음
  - 이 경우 특정 기관이 홀로 이 권한을 행사할 수 있으면 권한 남용이 너무 쉬움
    - 암호기술에서 권한은 키의 보유
- 이와 같은 권한 남용을 제한하기 위해 여러 기관에 권한을 분산하는 것이 필요함
  - 암호기술에서는 이 경우 임계 기반 비밀 공유기법($(t, n)$ threshold based secret sharing)을 사용함
    - $n$명에게 특정 권한을 분산하고, 이 중에 $t$명 이상이 동의하면 해당 권한을 수행할 수 있도록 함
    - 여기서 t는 보안 강도를 조절하기 위한 보안 변수임
    - 가용성 측면에서 $(n, n)$은 바람직하지 않은 형태의 서비스임

# 통신 계층과 암호기술 (1/2)

- 통신 메시지의 비밀성/무결성을 보장하기 위한 암호기술의 적용과 통신 계층 간의 관계

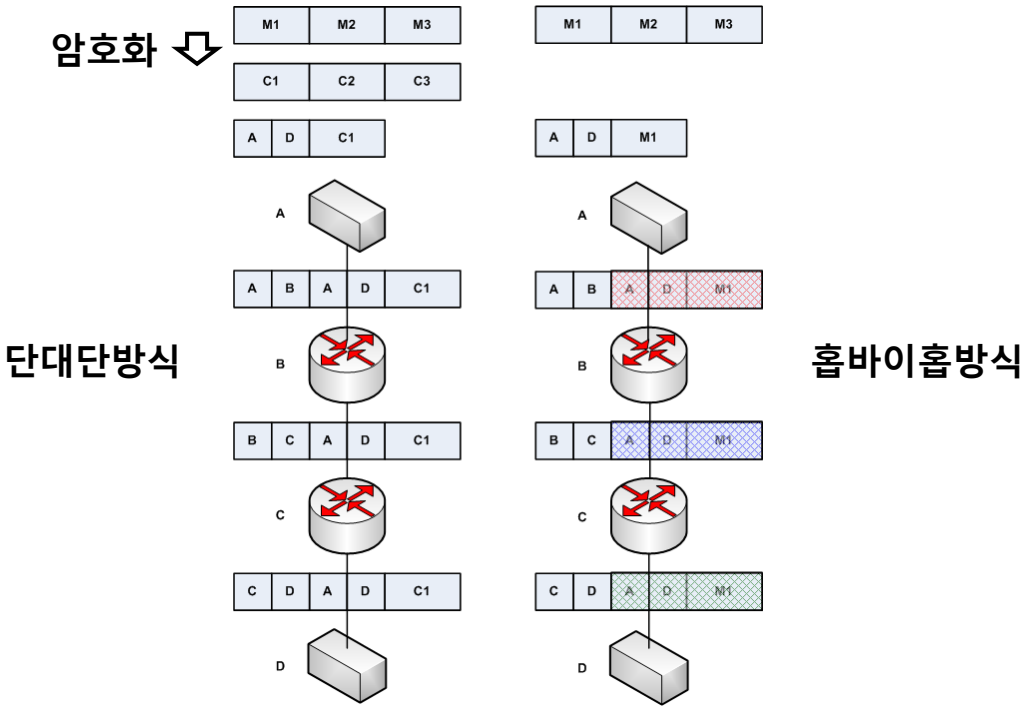
| | 단대단(end-to-end) | 홉바이홉(hop-by-hop) |
|---|---|---|
| 장점 | • 통신망과 독립적으로 수행가능<br>• 기반구조를 신뢰하지 않아도 됨 | • 트랙픽 분석이 가능하지 않음<br>• 패킷 단위로 암호화가 가능하므로 오류 발생시 해당 패킷만 재전송 |
| 단점 | • 트래픽 분석이 가능<br>• 메시지 단위로 암호화하기 때문에 오류 발생시 암호화하는 방식에 따라 재전송해야 하는 부분이 클 수 있음 | • 통신망의 각 호스트/스위치에 기능이 포함되어 있어야 함<br>• 기반구조를 신뢰해야 함 (중간 호스트/스위치는 평문을 볼 수 있음)<br>• 반복적으로 암호기술을 적용하기 때문에 효율성이 떨어짐 |
| 예 | • TLS(Transport Layer Security) | • IPSec |







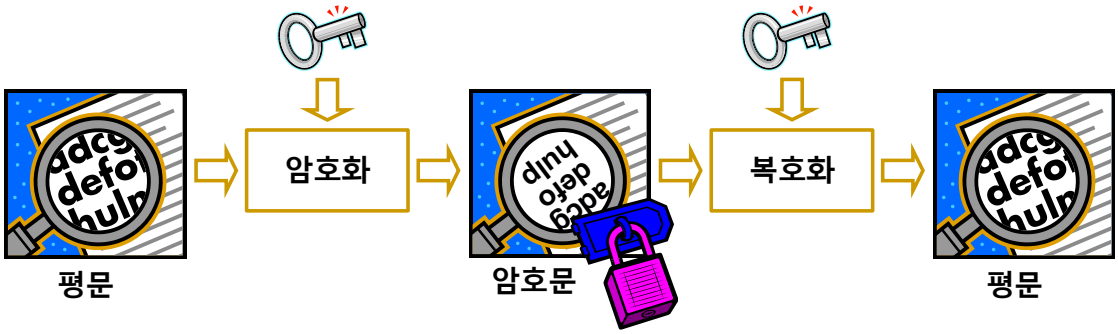
# 통신 계층과 암호기술 (2/2)



# 기본 용어 (1/2)

정보통신용어 표준
http://word.tta.or.kr/

- 평문(plaintext, cleartext)
- 암호문(ciphertext)
- 암호화(encryption, encipherment): 평문을 암호문으로 바꾸는 과정
  - 비고. encrypt, encipher: 암호화하다.
- 복호화(decryption, decipherment): 암호문을 평문으로 바꾸는 과정
  - 비고. decrypt, decipher: 복호화하다.






# 기본 용어 (2/2)

- 암호기술(cryptography): 공격자가 존재하는 상황에서 서비스가 안전하게 이루어지도록 하는 기술
  - 디지털 정보에 직접 적용하는 수학적 이론에 근거를 두는 기술
  - 비고. 암호기술자(cryptographer)
- 암호해독기술(cryptanalysis): 암호기술을 분석하여 그것의 문제점을 발견하는 기술
  - 비고. 암호해독자(cryptanalyst)
- 암호학(cryptology): 암호기술 + 암호해독기술
  - 비고. 암호학자(cryptologist)

# 암호기술의 한계

- 한계 1. 모든 보안 문제의 해결책은 아님
  - 사회공학(social engineering) 공격은 암호기술로 해결할 수 없음
- 한계 2. 제대로 구현하고 올바르게 사용하지 않으면 효과가 없음
- 한계 3. 비전문가가 직접 설계하여 사용할 수 있는 기술은 아님
  - 표준 기술을 사용해야 하며, 전문가에 의해 설계된 것도 허점이 있는 경우가 많았음

'Blockchain Bandit': 약한 랜덤 함수를 이용하여 키를 생성하는 블록체인 지갑을 이용하는 700개 이상 사용자의 암호화폐(총액: 9천만 달러)가 도난된 적이 있음