17 암호화와 네트워크 보안

쉽게 배우는 데이터 통신과 컴퓨터 네트워크

학습목표

- ✓ 암호화 원리를 바탕으로 대체 암호화와 위치 암호화를 이해
- ✓ 암호화 알고리즘인 DES, RSA의 구조를 이해
- ✓ 전자 서명의 필요성과 방법을 이해
- ✓ 네트워크 보안의 개념과 관련 이슈를 이해
- ✓ 라우터와 프록시로 구현한 방화벽의 원리를 이해

2절. 암호화 시스템

- 컴퓨터 보급 전: 수작업을 위해 알고리즘은 간단하고 암호키가 복잡하게 구성
- 컴퓨터 보급 후: 알고리즘의 복잡도가 증가됨

DES(Data Encryption Algorithm) 알고리즘

- 송수신자가 동일한 키를 사용하는 대칭키 알고리즘

동작 방식

- 암호키: 56 비트(64비트 중에서 8비트를 사용하지 않음)
- 64 비트 단위로 암호화
- 16 단계의 암호화 과정을 수행: 16 라운드 암호+ (2번의 위치 암호화) 단계

2절. 암호화 시스템

- **3DES 알고리즘**
  - **세 번의 DES 알고리즘을 수행하는 3단계 DES 알고리즘**
  - **구현이 쉬우나 DES 알고리즘에 비하여 3배 이상 속도가 느린 단점이 있음**
  - **전체적으로 168비트의 키를 지원하여 보안 기능이 한층 강화됨**

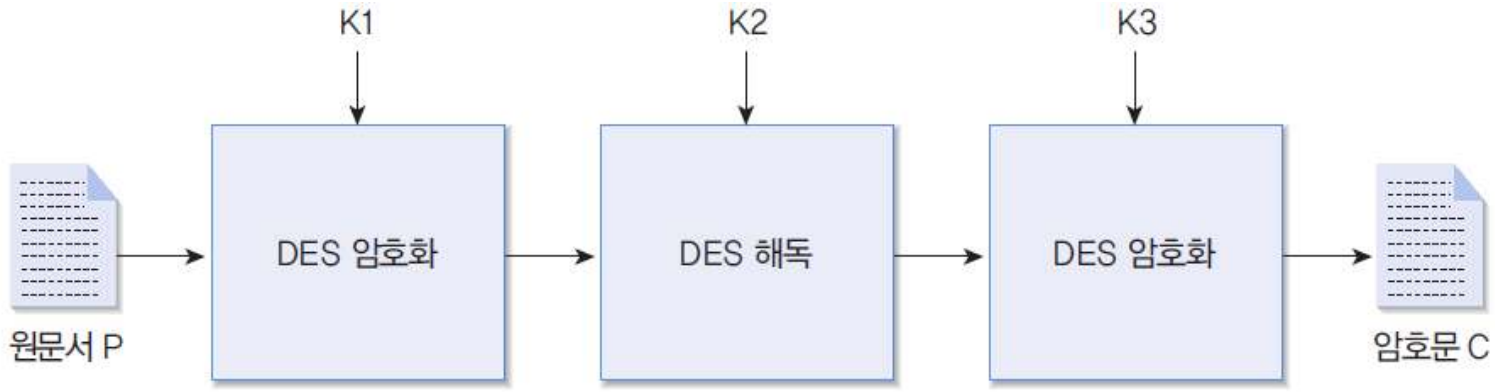


그림 17-12 3DES 알고리즘을 이용한 암호화 과정

  - **DES 키(K1, K2, K3)**
    - 키 K1으로 DES 암호화, 키 K2으로 DES 해독, 키 K3으로 DES 암호화 기능을 수행

$$C=E_{K3}(D_{K2}(E_{K1}(P)))$$

2절. 암호화 시스템

- 키 K3으로 DES 해독, 키 K2으로 DES 암호화, 키 K1으로 DES 해독기능 수행

$$P=D_{K1}(E_{K2}(D_{K3}(C)))$$

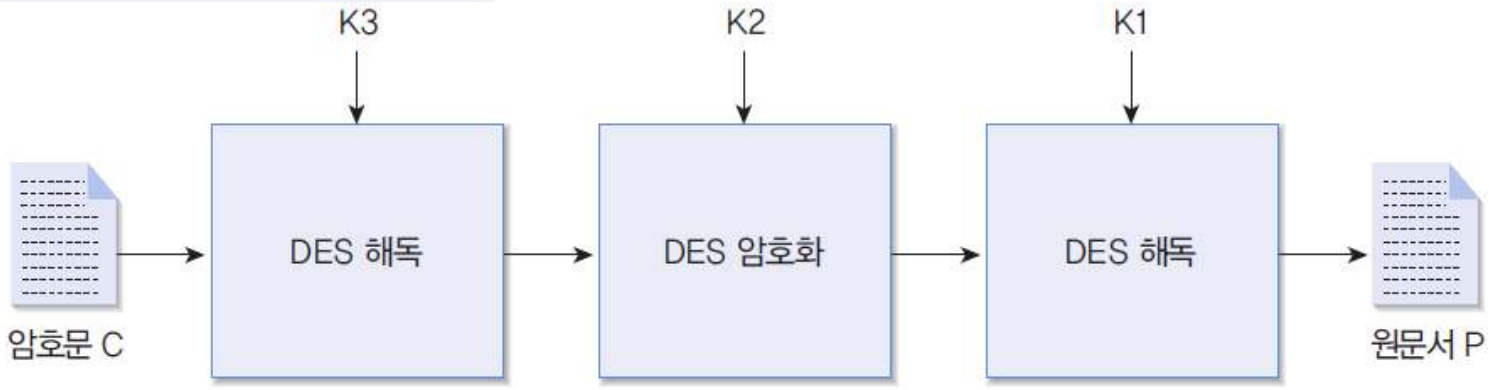


그림 17-13 3DES 알고리즘을 이용한 해독 과정

표 17-1 3DES의 암호키 옵션

옵션	설명
3개의 키가 모두 독립적	168비트의 키가 사용되므로 보안 기능이 가장 뛰어나다.
K1과 K2는 독립적, K3 = K1	112비트의 키가 사용되므로 보안 기능이 약간 떨어진다. 그러나 단순히 DES 알고리즘을 두 번 실행하는 것보다는 강화된 기능을 지원한다.
3개의 키가 모두 동일 (K1 = K2 = K3)	56비트의 키가 사용되므로 DES 알고리즘과 동일하여 현재는 권고에서 제외되어 있다.

2절. 암호화 시스템

RSA(Rivest, Shamir Adelman) 알고리즘

- 비대칭키의 공개키 알고리즘
  - 공개키: 원문서를 암호화하는 용도로 사용 (모든 사람이 암호화 과정 수행)
  - 비공개키(개인 키): 암호문을 해독하는 용도로 사용 (특정인만 해독 과정 수행)
- RSA 암호 알고리즘 [그림 17-14]
  - (공개키, 비공개키) 조합을 생성

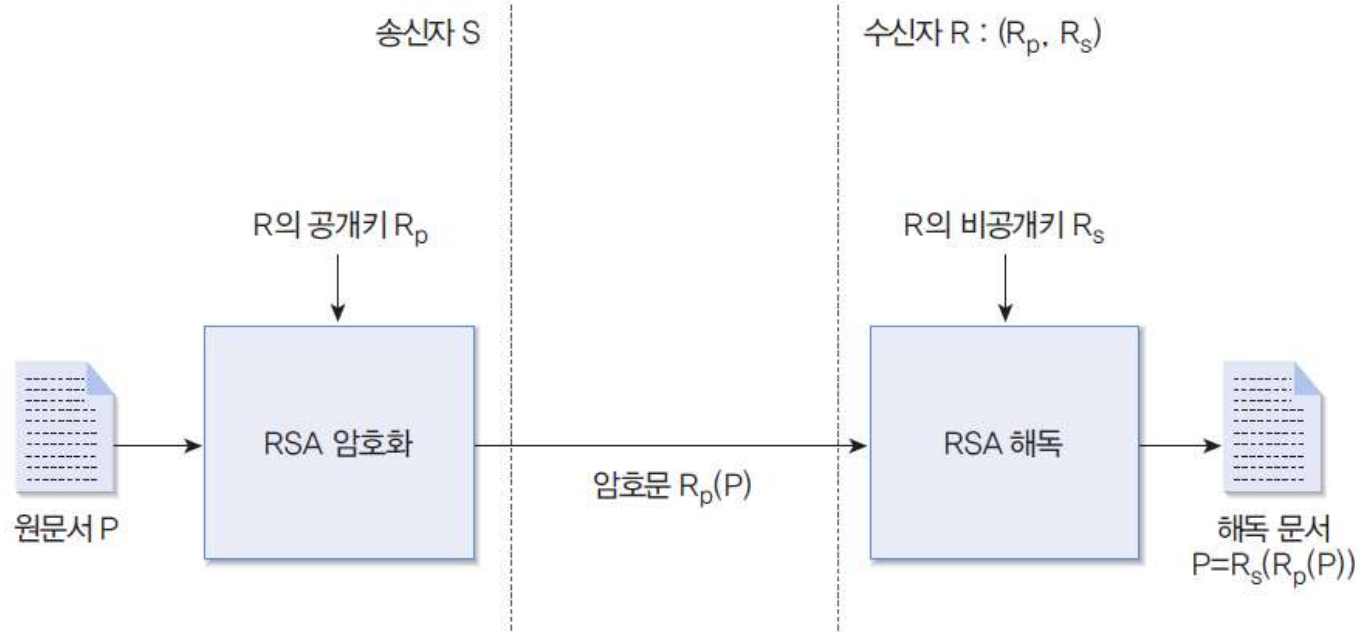


그림 17-14 RSA 알고리즘

2절. 암호화 시스템

□ 전자 서명(Digital Signature)

- 사용자의 인증 기능 제공
- RSA 알고리즘과 반대 원리로 동작 [그림 17-15]
  - 비공개키(개인키): 원문서를 암호화하는 용도로 사용 (특정인만 암호화 과정 수행)
  - 공개키: 암호문을 해독하는 용도로 사용 (모든 사람이 해독 과정 수행)

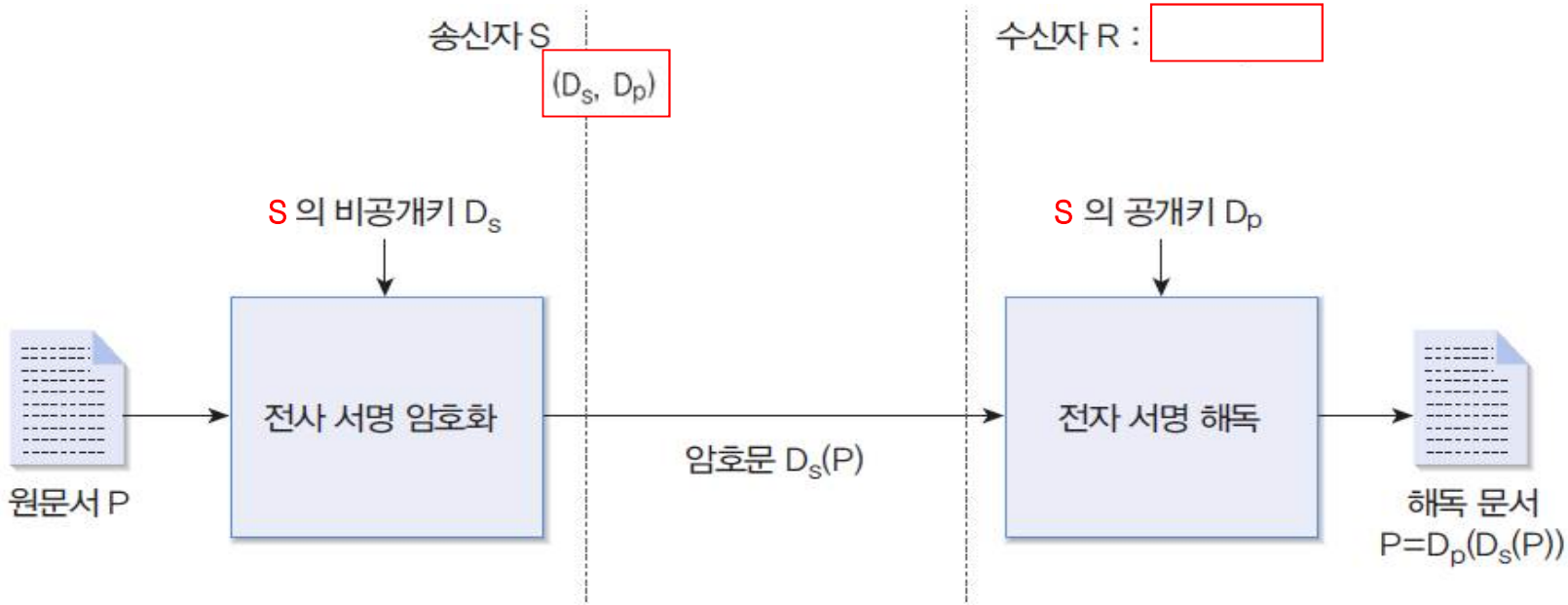


그림 17-15 전자 서명의 원리

2절. 암호화 시스템

□ 전자 서명 (Digital Signature)

- **암호화 과정 (서명 + 암호 과정)[그림 17-16]**
  - 1단계: 전자 서명 알고리즘으로 인증 정보를 암호화 **(사용자 인증)**
  - 2단계: RSA 알고리즘으로 전자 서명 정보를 암호화 **(전송 보안)**

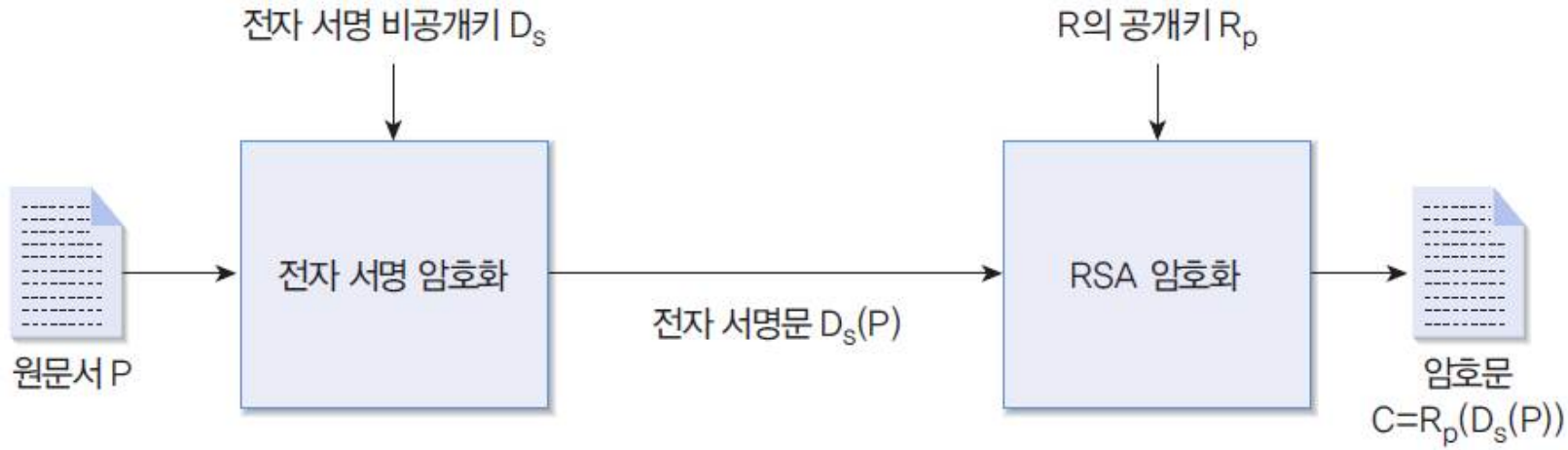


그림 17-16 전자 서명 암호화

전자 서명

- **해독 과정(복호 + 서명 검증) [그림 17-17]**
  - 1단계: RSA 알고리즘으로 전자 서명 정보를 해독
  - 2단계: 전자 서명 알고리즘으로 인증 정보 해독

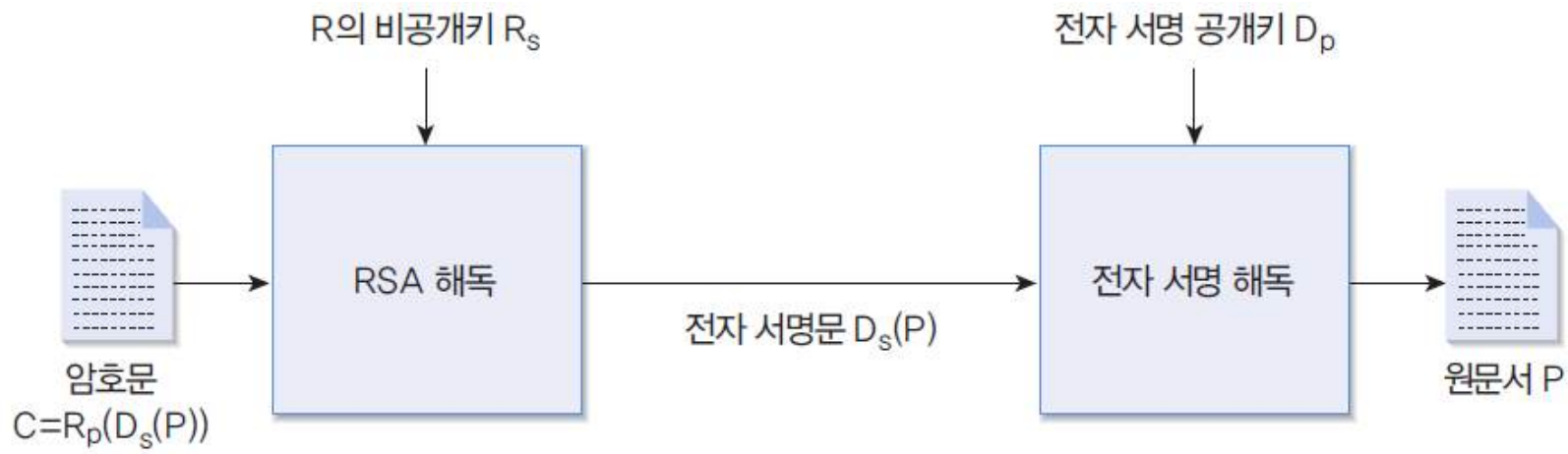


그림 17-17 전자 서명 해독

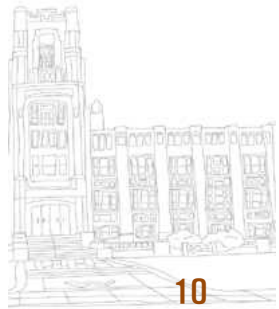
3절. 보안 프로토콜

□ 보안 프로토콜에 대한 위협

- 전송 데이터를 중간에서 감청하거나 임의로 변경하는 경우
- 호스트 데이터에 위해를 가하는 등 직접적으로 호스트 내부에 침입하는 경우
- 과도한 트래픽을 발생시켜 특정 호스트의 통신을 방해하는 경우

▪ 감청

- 허가받지 않은 자가 전송 중인 데이터를 얻어내는 것
- 유선의 통신 선로에서 패킷 감청
- 무선 통신 환경에서는 감청이 더욱 용이



3절. 보안 프로토콜

□ 보안 프로토콜 개요

▪ 암호화

- **데이터링크 계층 암호화** [그림 17-18] – 물리 계층을 통과하기 전 암호화
  - 전송 선로상의 감청으로부터 보호
  - 단점: 라우터 등 호스트 내부에서는 보호가 안됨

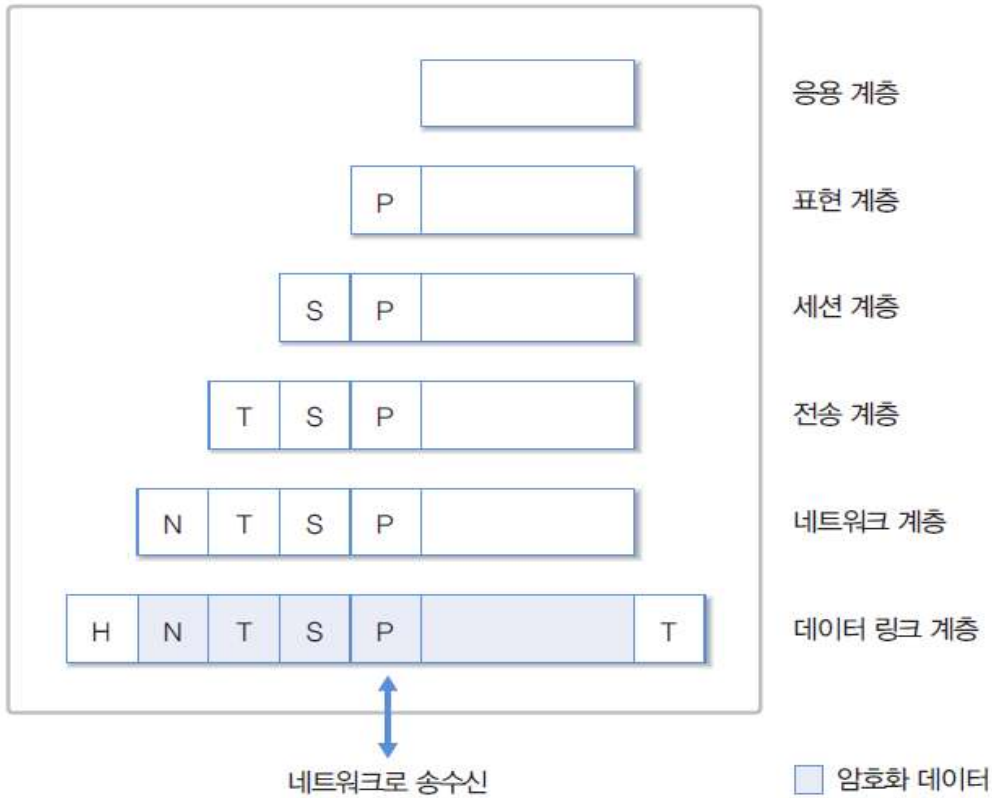


그림 17-18 데이터 링크 계층 암호화

3절. 보안 프로토콜

□ 보안 프로토콜 개요

▪ 암호화

- 응용 계층 암호화 [그림 17-19]- OSI 7계층에서는 표현계층
  - 호스트 내부에서 보안을 지원

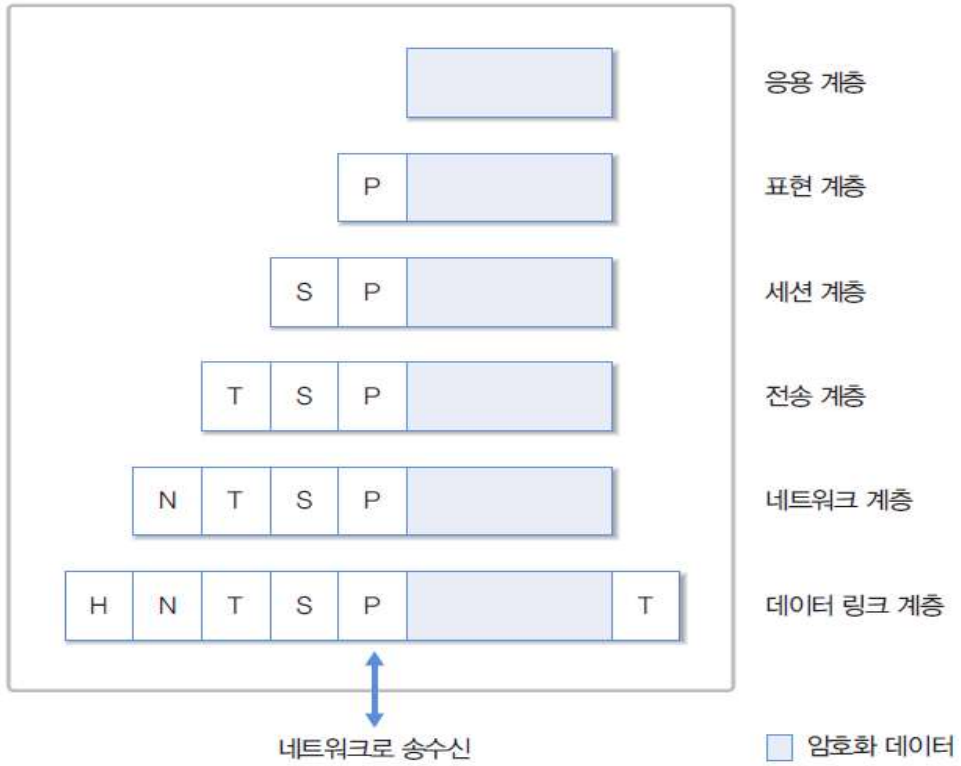


그림 17-19 응용 계층 암호화

3절. 보안 프로토콜

□ 방화벽(Firewall)

- 개방적인 공중 인터넷망과 제한된 그룹의 사설망 사이에 설치 [그림 17-20]
  - 1) 패킷 필터링 방식: 패킷을 검색하여 차단 여부 결정
  - 2) 해커와 같이 의심스러운 행위를 하는 사용자를 감시

그림 17-20 방화벽

3절. 보안 프로토콜

□ 방화벽(Firewall)

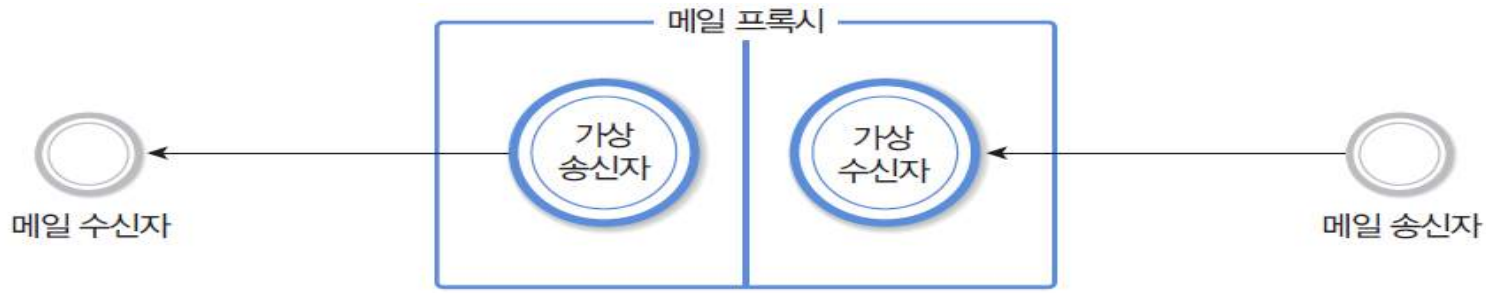
- 라우터를 기반으로 방화벽 구현- 스크리닝 라우터라고 함
  - 외부망과의 중계 기능을 수행하므로 간단하면서도 매우 효과적
  - IP 주소 기반: 위장 IP 주소의 차단 [그림 13-12]
    - 인터넷으로부터 211.223.201.X를 발신자로 하는 패킷은 입력될 수 없음
  - 포트 번호 기반: 특정 서비스 이용을 차단(응용 프로그램 접근 차단)

그림 17-21 위장 IP 주소의 차단

3절. 보안 프로토콜

□ 방화벽(Firewall)

- **프록시를 이용한 방화벽 구현**
  - 라우터: 네트워크 계층의 헤더에 기초하여 방화벽 기능 수행
    메일 내용과 같이 패킷 내부의 데이터는 제어가 불가능
  - 프록시: 응용환경하에 가상의 응용 프로그램을 시뮬레이션하는 방화벽



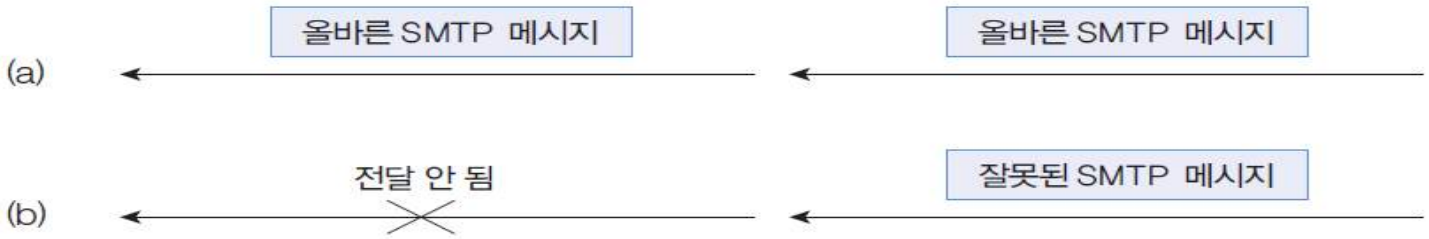


그림 17-22 메일 프록시