17 암호화와 네트워크 보안

가천대학교 - 2019학년도 1학기 -

Preview

❖ 네트워크 보안의 중요성 증대

- 단순 정보 검색을 넘어 개인정보의 유통, 홈 뱅킹, 전자 상거래 같은 상업 분야로 확대

❖ 보안의 필요성

- 허가받지 않은 외부 침입자에게 정보 유출 방지
- 외부 침입자가 보안 데이터의 내용을 조작하지 않도록 보호

Contents

학습목표

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

내용

- 암호화의 이해
- 암호화 시스템
- 보안 프로토콜

01_암호화의 이해

❖ 암호화 관련 용어

- 네트워크는 개방형 시스템으로 외부 노출 가능성 있음
- 외부 침입자 공격 행동
  - 메시지 읽기 : 전송 선로를 도청. 암호화 기법으로 해결함
  - 전송 방해 : 송수신자 간의 통신을 방해. 방화벽 기능을 통해 불법 사이트에 접속하지 못하도록 차단하는 것도 이에 해당
  - 메시지 수정 : 전송되는 메시지의 내용을 수정, 교환 메시지의 의미를 왜곡함

암호화 용어

- 암호화Encryption : 내용을 변형하여 원래의 의미를 알아볼 수 없도록 변형하는 작업
- 해독Decryption : 암호화된 문서를 원래 언어로 변형
- 원문서 : 암호화 전의 원본 문서, 암호문 : 임의의 형태로 암호화한 문서

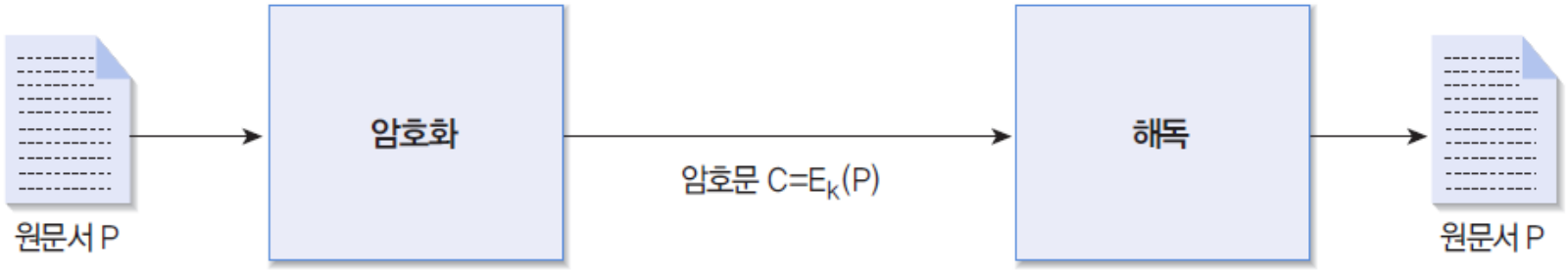


그림 17-1 암호화와 해독 과정

01_암호화의 이해

- 암호화 알고리즘
  - 암호키(k_E) : 암호화 과정에서 사용하는 키
  - 해독키(k_D) : 해독 과정에서 사용하는 키
  - 대칭키 방식 : 암호키와 해독키가 같음
    - 송수신자 외의 제3자가 키 값을 알지 못하도록 하는 것이 중요. 주기적으로 키 값 변경
  - 비대칭키 방식 : 암호키와 해독키가 다름
    - 보통 키 하나가 공개되므로, 공개되지 않는 나머지 키에 대한 보안 주의 필요

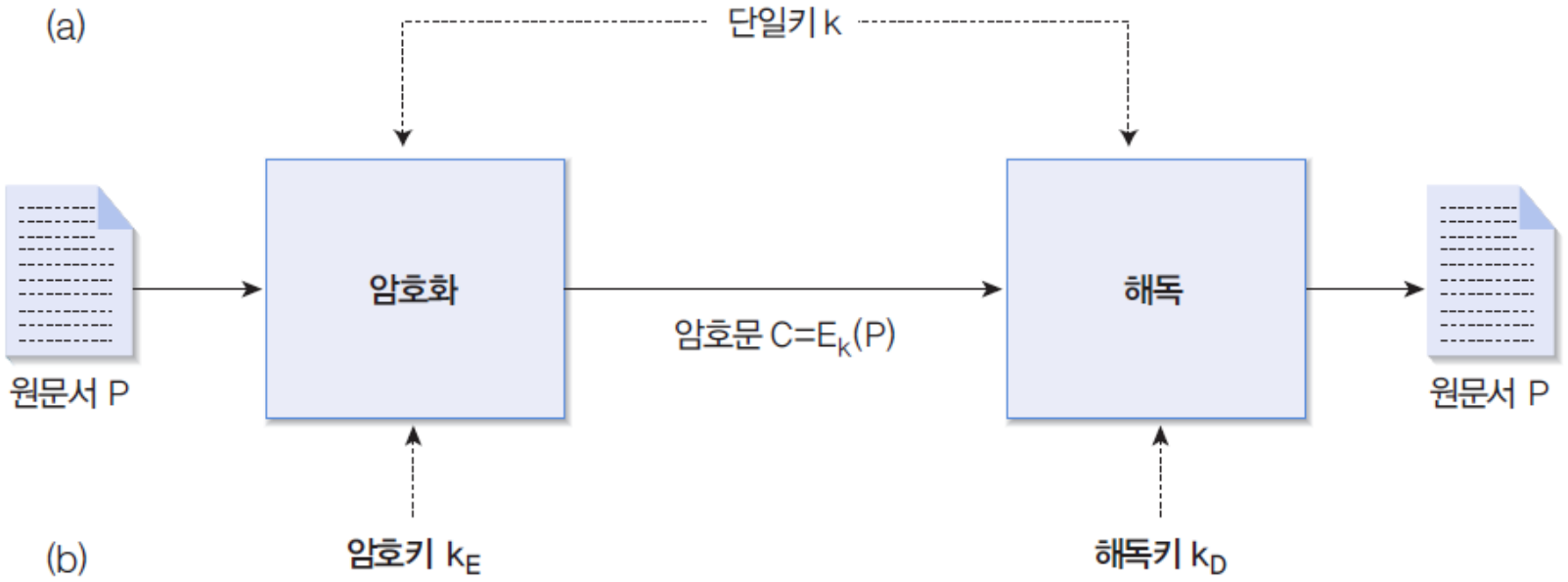


그림 17-2 키의 종류

01_암호화의 이해

❖ 대체 암호화

- 임의의 문자를 다른 문자로 대체하는 암호화. 문자와 대체 문자를 나열한 표가 암호키와 복호키가 됨
- 시저 암호화, 키워드 암호화, 복수 개의 문자 변환표 방식 등

▪ 시저 암호화

- 알파벳 문자를 세 문자씩 오른쪽으로 이동하면서 대체 문자를 사용하는 방식

원문	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
암호문	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z	a	b	c

그림 17-3 시저 암호화에서 사용하는 문자 변환표

- 장점 : 단순, 단점 : 쉽게 해독 가능

원문	N	E	T	W	O	R	K		T	E	C	H	N	O	L	O	G	Y							
암호문	q	h	w	z	r	u	n		w	h	f	k	q	r	o	r	j	b							

그림 17-4 시저 암호화를 이용한 암호화 예

01_암호화의 이해

- 키워드 암호화
  - 지정 단어를 암호문 앞줄에 적고, 키워드에 표시된 문자를 뺀 나머지 문자를 알파벳 순으로 기술하는 방식

  - 예) 키워드 : seoul

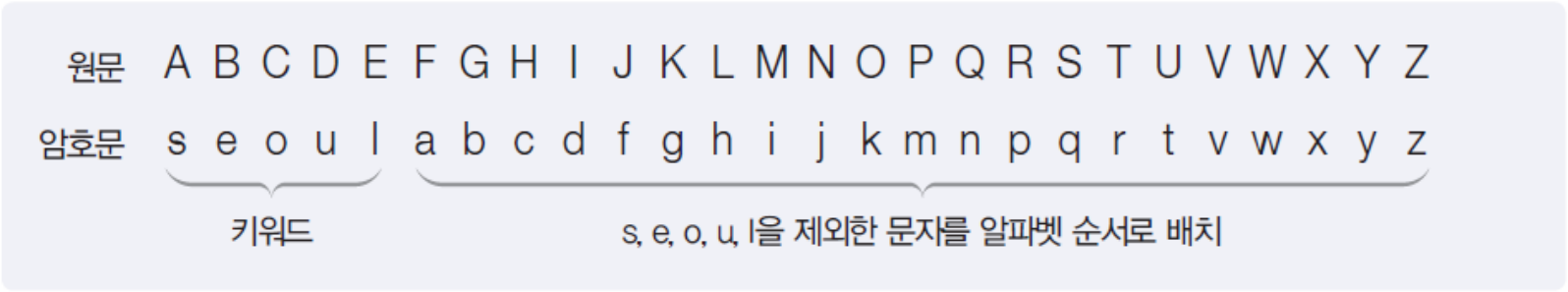


그림 17-5 키워드 암호화에서 사용하는 문자 변환표

  - 키워드를 모르면 시저 암호화보다 대체 문자 변환표 추측 어려움
  - 대체 문자 변환표의 오른쪽으로 갈수록 원문과 암호문의 문자가 같아질 확률이 높아 시저 암호문보다 나쁜 결과 초래 가능

01_암호화의 이해

- 복수 개의 문자 변환표
  - 문자 변환표를 둘 이상 사용
  - 장점 : 원문서의 동일 문자가 암호문에서는 다르게 암호화되므로 해독이 어려움

원문	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
암호문	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z	a	b	c

(a) 홀수 위치에 있는 문자

원문	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
암호문	s	e	o	u	l	a	b	c	d	f	g	h	i	j	k	m	n	p	q	r	t	v	w	x	y	z

(b) 짝수 위치에 있는 문자

그림 17-6 두 개의 문자 변환표

  - 예) NETWORK TECHNOLOGY를 암호화

1	2	3	4	5	6	7		8	9	10	11	12	13	14	15	16	17
N	E	T	W	O	R	K		T	E	C	H	N	O	L	O	G	Y
q	l	w	w	r	p	n		r	h	u	k	j	r	h	r	b	b

그림 17-7 두 개의 문자 변환표를 이용한 암호화 예

01_암호화의 이해

❖ 위치 암호화

- 문자의 배열 순서를 변경해 암호화. 컬럼 암호화, 키워드 암호화 등

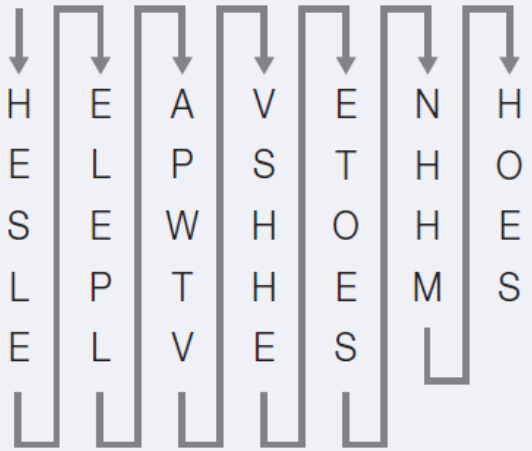
■ 컬럼 암호화 : 전체 문장을 컬럼을 기준으로 다시 배치

- 예) 컬럼의 길이가 7인 컬럼 암호화

(a) 원문서

HEAVEN HELPS THOSE WHO HELP THEMSELVES

(b) 컬럼 암호화 과정



(c) 암호문 1 hesle elepl apwtv vshhe vshhe etoes nhhm hoes

(d) 암호문 2 hesle elepl apwtv vshhe vshhe etoes nhhmz heosz

그림 17-8 **컬럼 암호화 예**

01_암호화의 이해

- 키워드 암호화
  - 중복된 문자를 포함하지 않는 임의의 단어를 암호키로 제공
  - 예) 키워드 : NETWORK

(a) 원문서

HEAVEN HELPS THOSE WHO HELP THEMSELVES

(b) 암호화 과정

키워드	N	E	T	W	O	R	K
순서	3	1	6	7	4	5	2
	H	E	A	V	E	N	H
	E	L	P	S	T	H	O
	S	E	W	H	O	H	E
	L	P	T	H	E	M	S
	E	L	V	E	S	Z	Z

(c) 암호문

elepl hoesz hesle etoes nhhmz apwtv vshhe

그림 17-9 키워드 암호화 예

02_암호화 시스템

- 암호문은 기본적으로 대체 암호화와 위치 암호화 방법을 적절히 조합하여 작성
- 컴퓨터 보급 전 수작업으로 암호화 : 알고리즘 간단, 암호키에 문자 많이 사용
- 고성능 컴퓨터 보급에 따라 연산 속도가 빨라져 알고리즘의 복잡도를 높이는 방식으로 암호화 하게 됨. 예) DES와 RSA 알고리즘

❖ DES Data Encryption Standard 알고리즘

- 비밀키(대칭키)
  - 암호키와 암호문을 해독할 때 사용하는 해독키가 같음
  - 비공개키 알고리즘 : 외부사용자에게 노출되지 않아야 하는 암호키로 암호화 하는 알고리즘
  - 미국 정부가 개발하여 여러 하드웨어, 소프트웨어에서 사용
  - 암호화를 64비트 단위로 수행, 암호키의 크기는 56비트

02_암호화 시스템

- 동작 방식
  - 크기가 64비트인 데이터 블록을 32비트씩 둘로 나누어 독립적으로 처리
  - 32비트 블록 하나를 암호키로 암호화 한 후, 두 블록의 위치를 맞바꾸는 과정을 16번 반복

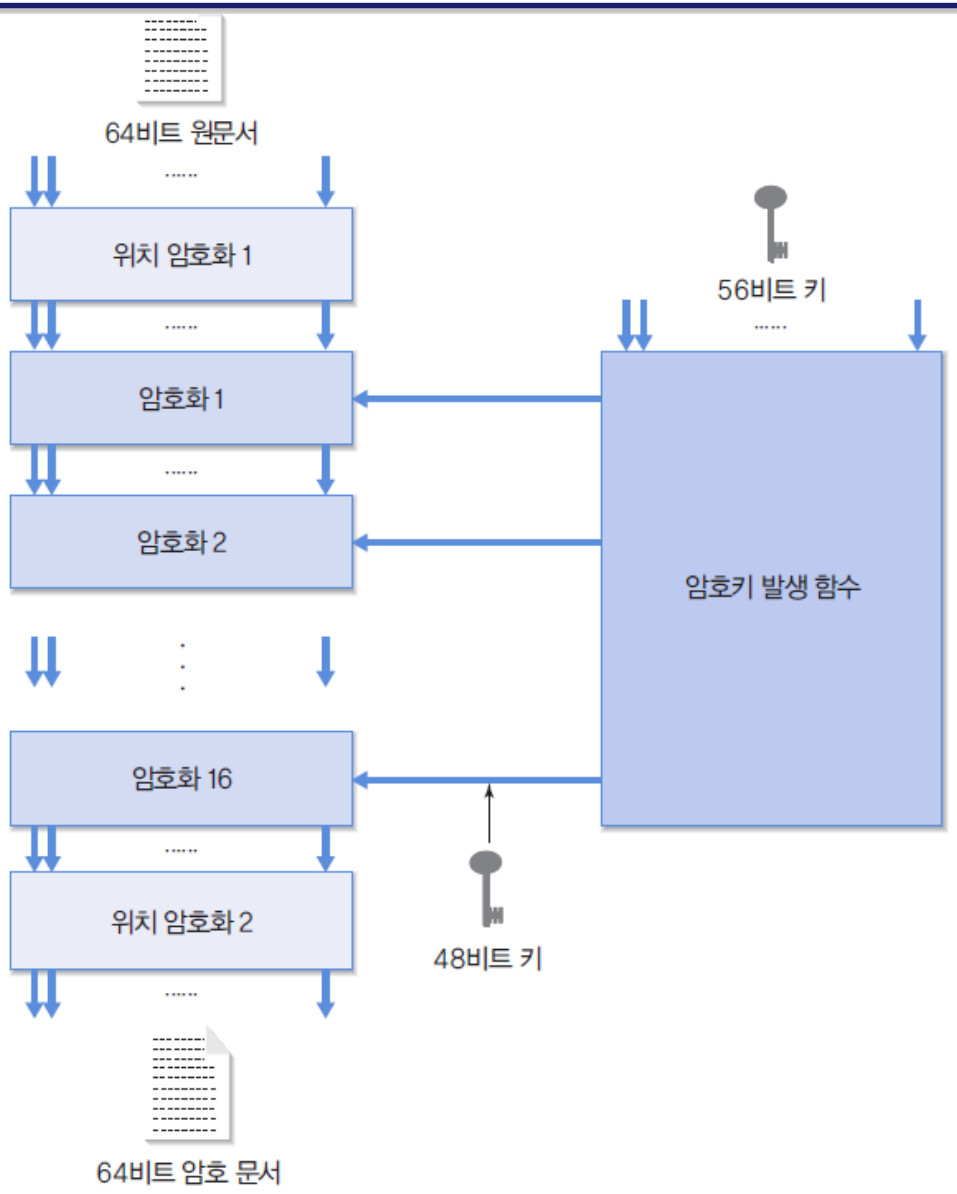


그림 17-10 DES 알고리즘 동작 과정

02_암호화 시스템

- 16단계의 암호화

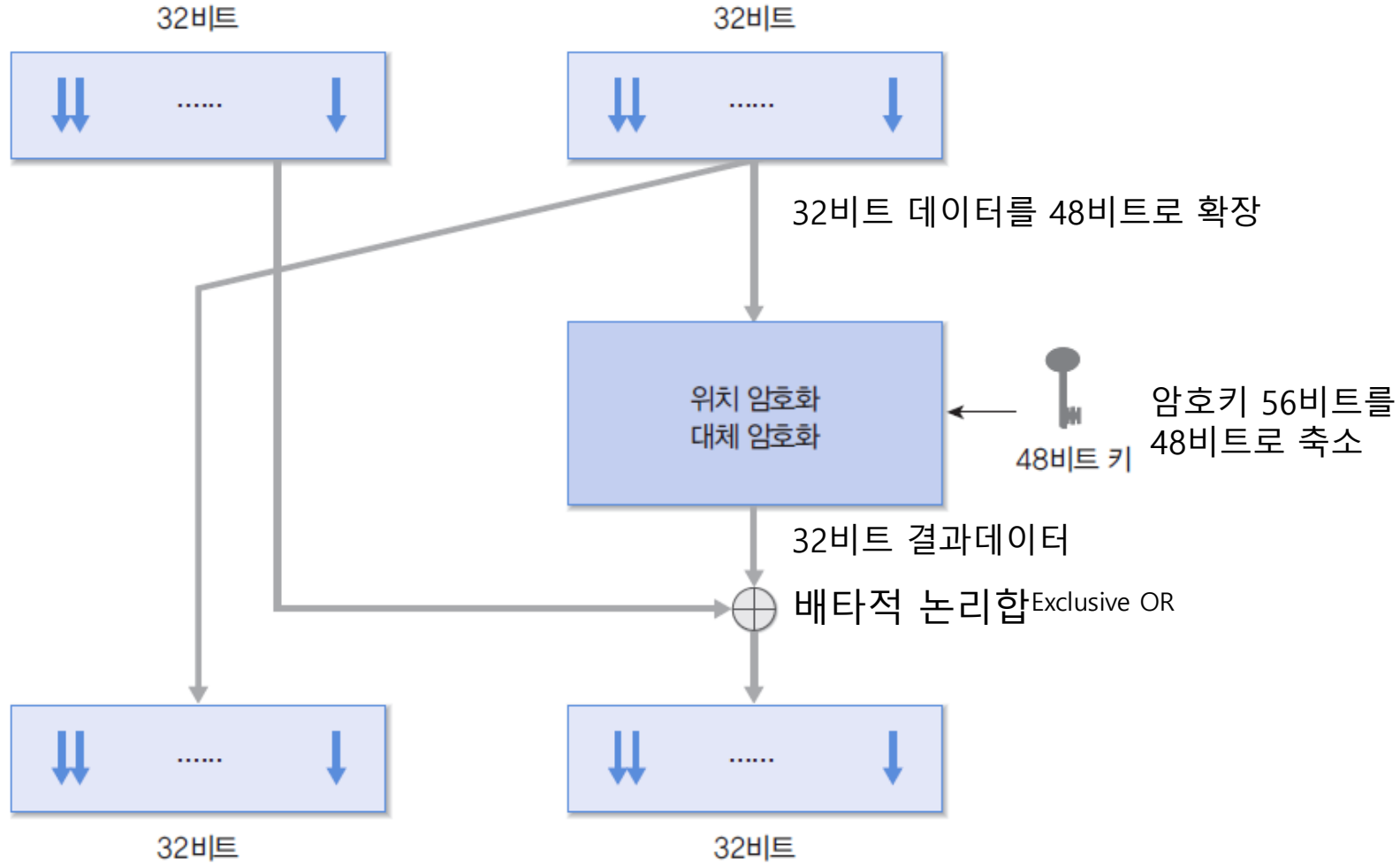


그림 17-11 [그림 17-10]의 16단계 암호화 알고리즘

02_암호화 시스템

- 3DES 알고리즘
  - 세 번의 DES 알고리즘을 수행하는 3단계 DES 알고리즘
    - DES 알고리즘은 56비트의 비교적 작은 키 사용으로 여러 평가에서 보안 기능 문제점 노출. 특히 고성능 컴퓨터를 이용한 반복적 공경에 취약
  - 구현이 쉬우나 DES 알고리즘에 비하여 3배 이상 속도가 느린 단점이 있음
  - 전체적으로 168비트의 키를 지원하여 보안 기능이 한층 강화됨

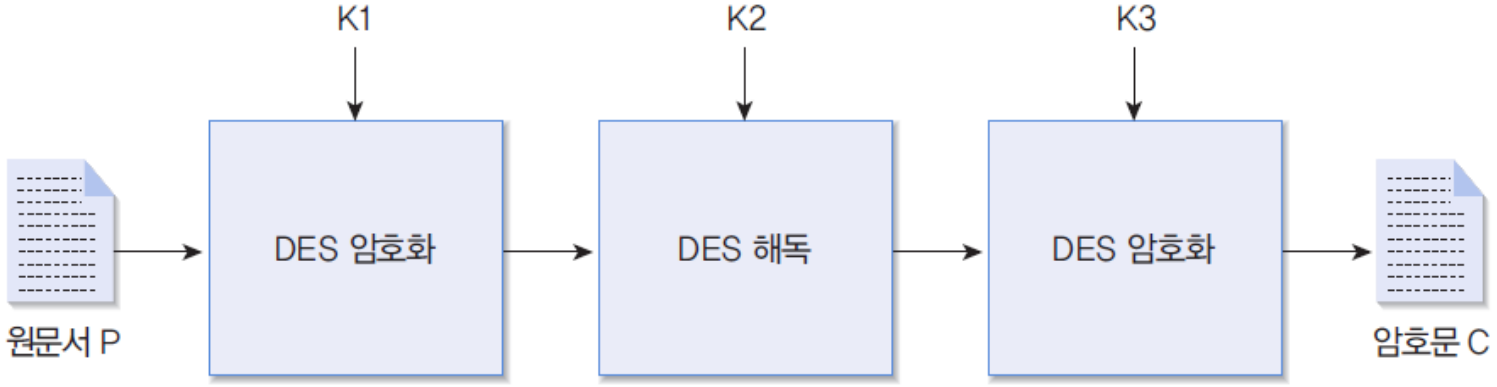


그림 17-12 3DES 알고리즘을 이용한 암호화 과정

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

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

02_암호화 시스템

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

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

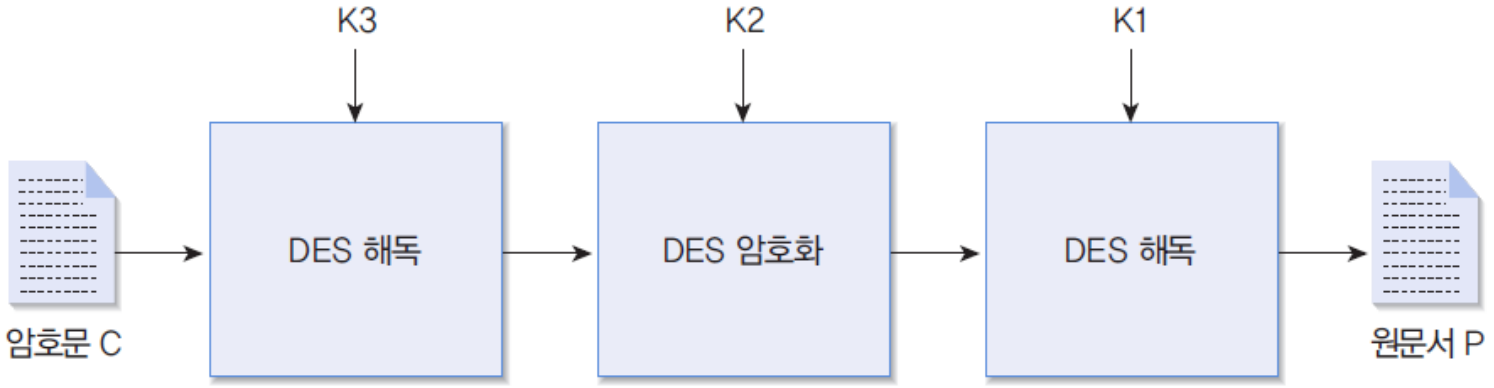


그림 17-13 3DES 알고리즘을 이용한 해독 과정

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.

02_암호화 시스템

RSA Rivest, Shamir, Adelman 알고리즘

- 공개키 알고리즘
  - 암호키와 해독키가 동일하지 않은 방식
  - 암호키가 외부에 공개되어도 해독키를 모르면 암호문을 해독할 수 없음
  - 두 개의 암호키(공개키, 비공개키) 조합을 사용
  - 예) RSA 알고리즘 : (공개키, 비공개키) 조합을 만드는 방법을 제시

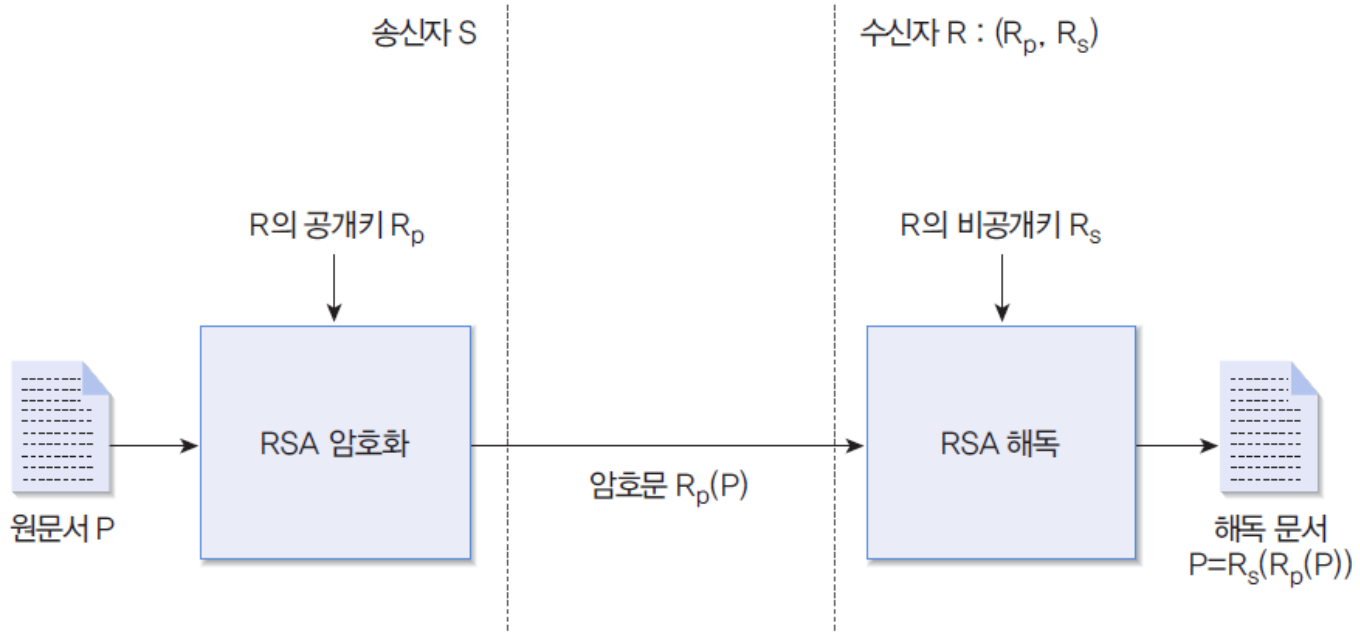


그림 17-14 RSA 알고리즘

02_암호화 시스템

❖ 전자 서명 Digital Signature

- 사용자의 인증 기능 제공
- RSA 알고리즘과는 반대 원리
- 비공개키 알고리즘과 공개키 알고리즘의 조합을 사용

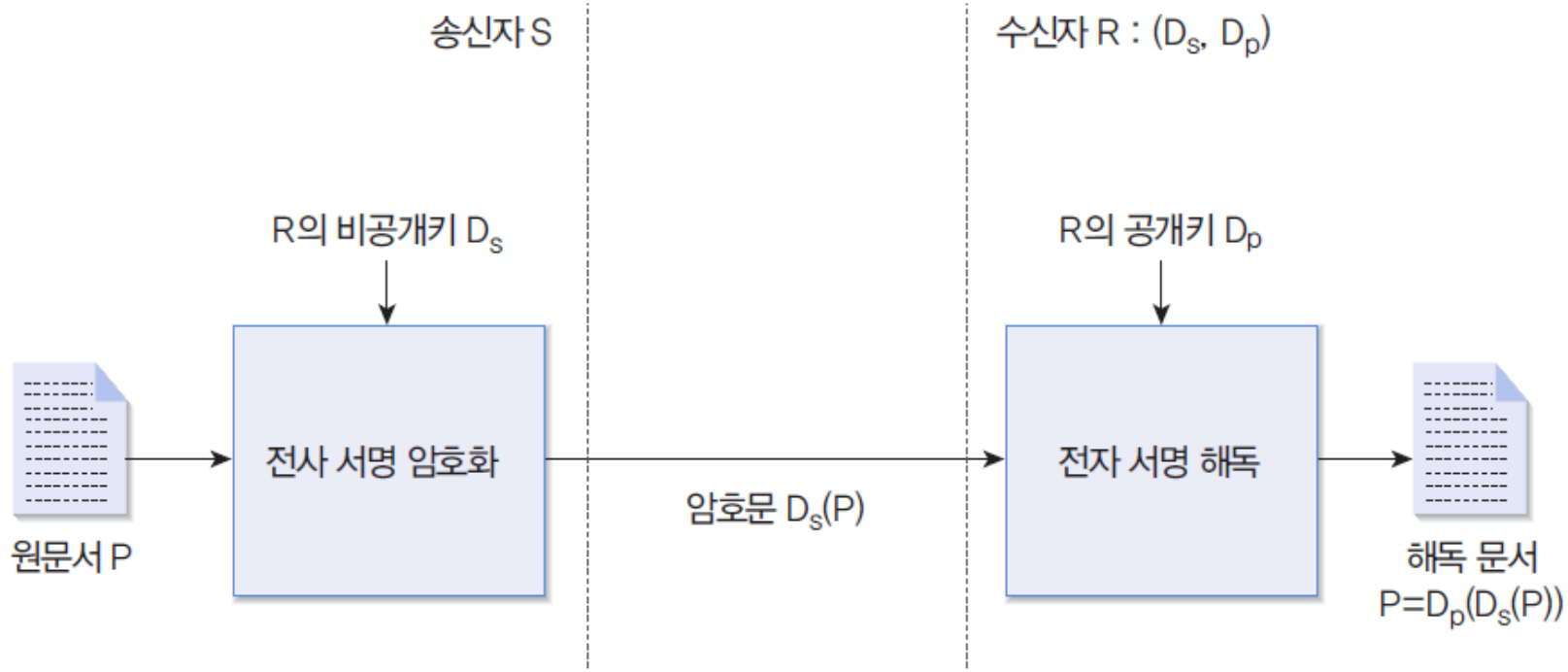


그림 17-15 전자 서명의 원리

02_암호화 시스템

- 암호화 과정
  - 1단계 : 전자 서명 알고리즘으로 인증 정보를 암호화 (사용자 인증)
  - 2단계 : RSA 알고리즘으로 전자 서명 정보를 암호화 (전송 보안)

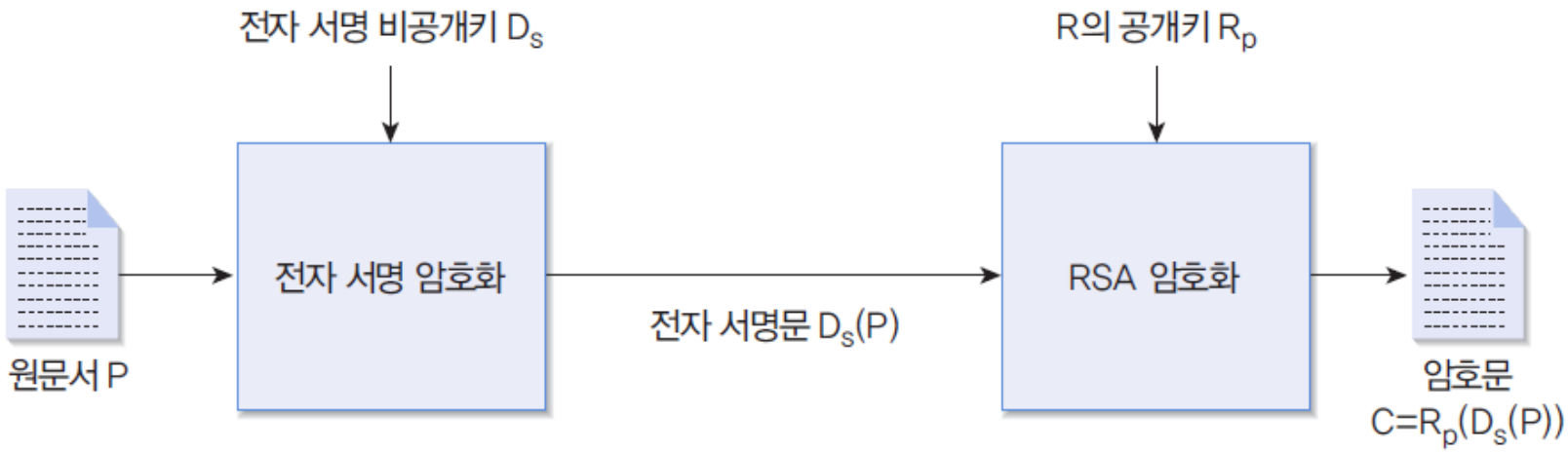


그림 17-16 **전자 서명 암호화**

02_암호화 시스템

- 해독 과정
  - 1단계 : RSA 알고리즘으로 전자 서명 정보를 해독
  - 2단계 : 전자 서명 알고리즘으로 인증 정보 해독

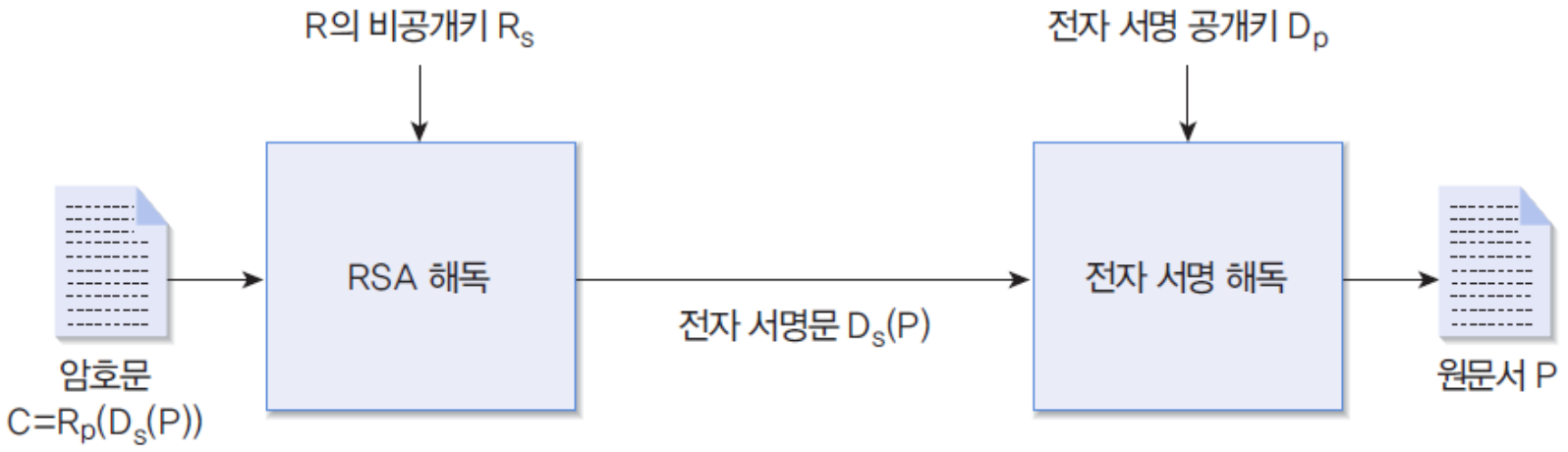


그림 17-17 **전자 서명 해독**

- 2단계 암호화 이유
  - RSA 알고리즘을 이용해 전송 과정에서 발생할 수 있는 보안 문제 해결
  - 전자 서명의 기본 목적인 인증문제 해결을 위해 비공개키인 전자 서명을 사용해 암호화

03_보안 프로토콜

❖ 보안 프로토콜의 개요

- 보안 문제 위협 요소
  - 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
  - 허가 받지 않은 자가 전송 중인 데이터를 얻어내는 것
    - 불법으로 획득한 정보를 변경한 후 통신 과정에 다시 입력하여 통신 내용을 왜곡하는 것도 넓은 의미에서 감청에 포함
  - 유선의 통신 선로에서 패킷 감청
    - 예: 인터넷의 경우 이더넷 선로에 감청하려는 호스트의 MAC 주소와 같은 값으로 설정한 장비를 연결하여 전달되는 패킷 감청
  - 무선 통신 환경에서는 감청이 더욱 용이

03_보안 프로토콜

- 암호화
  - 데이터링크 계층 암호화 : 전송 선로상의 감청으로부터 보호
    - 단점 : 라우터 등 호스트 내부에서는 보호가 안됨

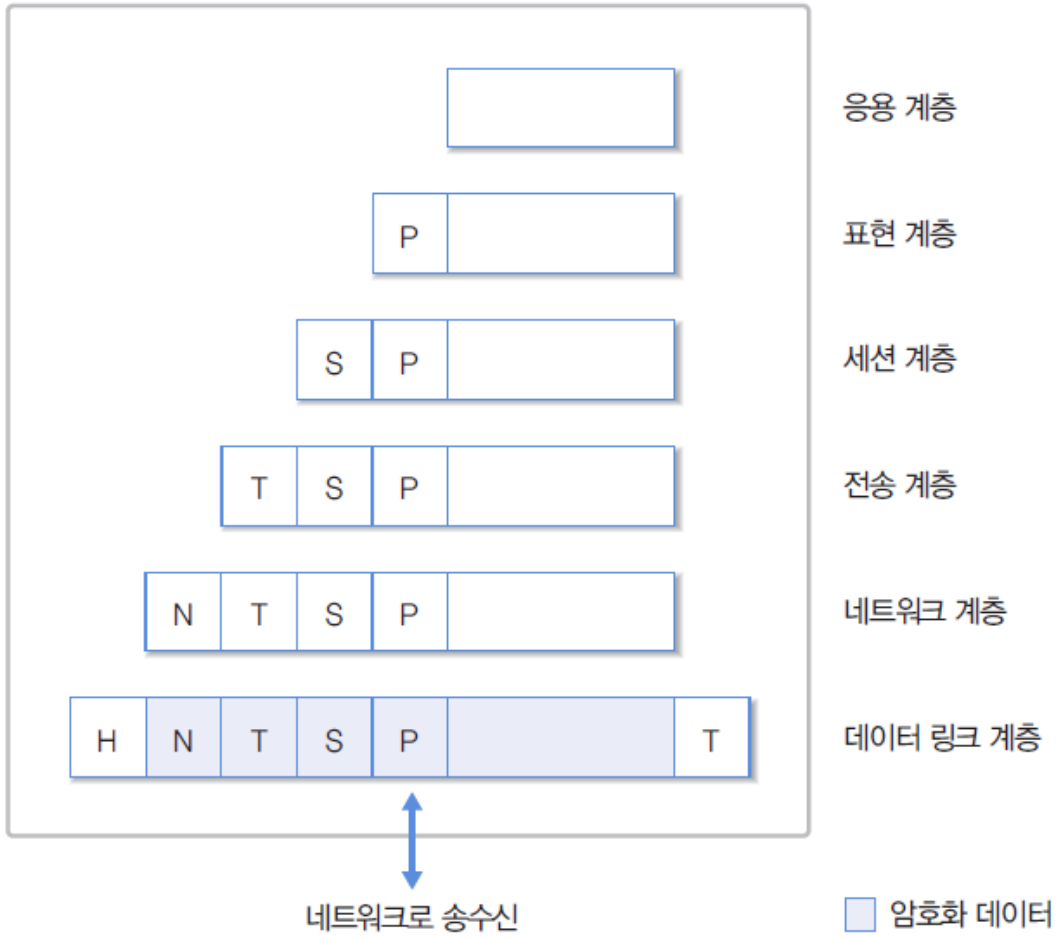


그림 17-18 데이터 링크 계층 암호화

03_보안 프로토콜

- 응용 계층 암호화 : 호스트 내부에서 보안을 지원
  - 라우팅을 포함하여 모든 전송 과정에서 보안유지 가능

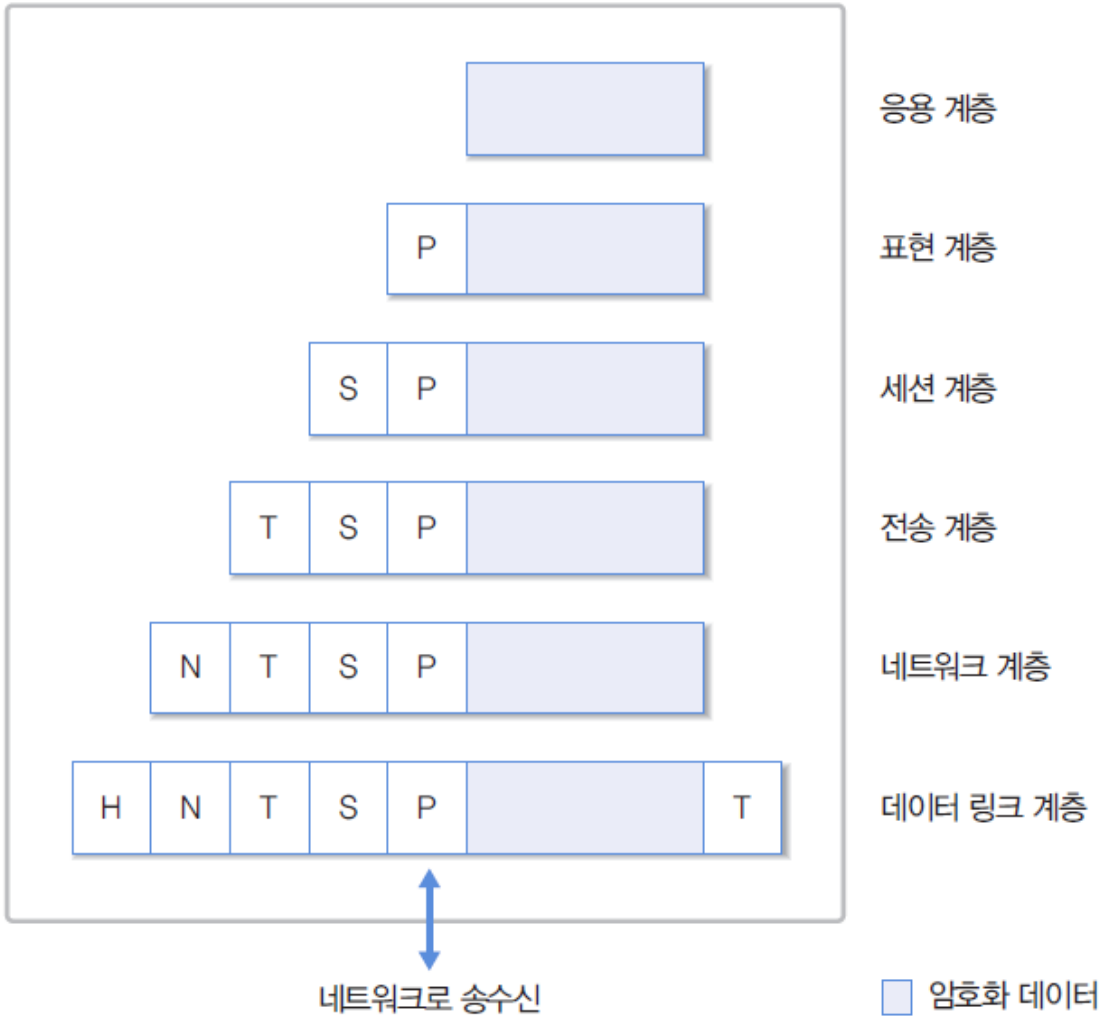


그림 17-19 응용 계층 암호화

03_보안 프로토콜

- 트래픽 제어
  - 특정 호스트가 누구와 통신을 많이 하는지의 정보도 네트워크 보안에 포함됨
    - 예: 전쟁 중 지휘 본부와 특정 부대사이의 교신량이 많은 경우 그 지역에서 군사작전이 있을 확률이 높음. 특정 회사끼리 접촉이 잦으면 상업적인 협력이 늘고 있을 가능성 높음
  - 가공 데이터를 여러 호스트에서 주기적으로ㅗ 발생시킴으로써 통신량 통계 자료에 혼선을 발생시킴

- 방화벽
  - 개방적인 공중 인터넷망과 제한된 사용자 그룹에 허가된 사설망 사이에 설치
    - 패킷 필터링 방식 : 패킷을 검색하여 차단 여부 결정
    - 해커같은 의심스러운 행위를 하는 사용자를 감시

그림 17-20 **방화벽**

03_보안 프로토콜

- 라우터를 이용한 방화벽 구현
  - 외부망과의 중개 기능을 수행하므로 간단하면서도 매우 효과적
  - IP 주소 기반 : 위장 IP 주소의 차단
    - 인터넷으로부터 211.223.201.X를 발신자로 하는 패킷은 입력될 수 없음
  - 포트 번호 기반 : 특정 서비스 이용을 차단

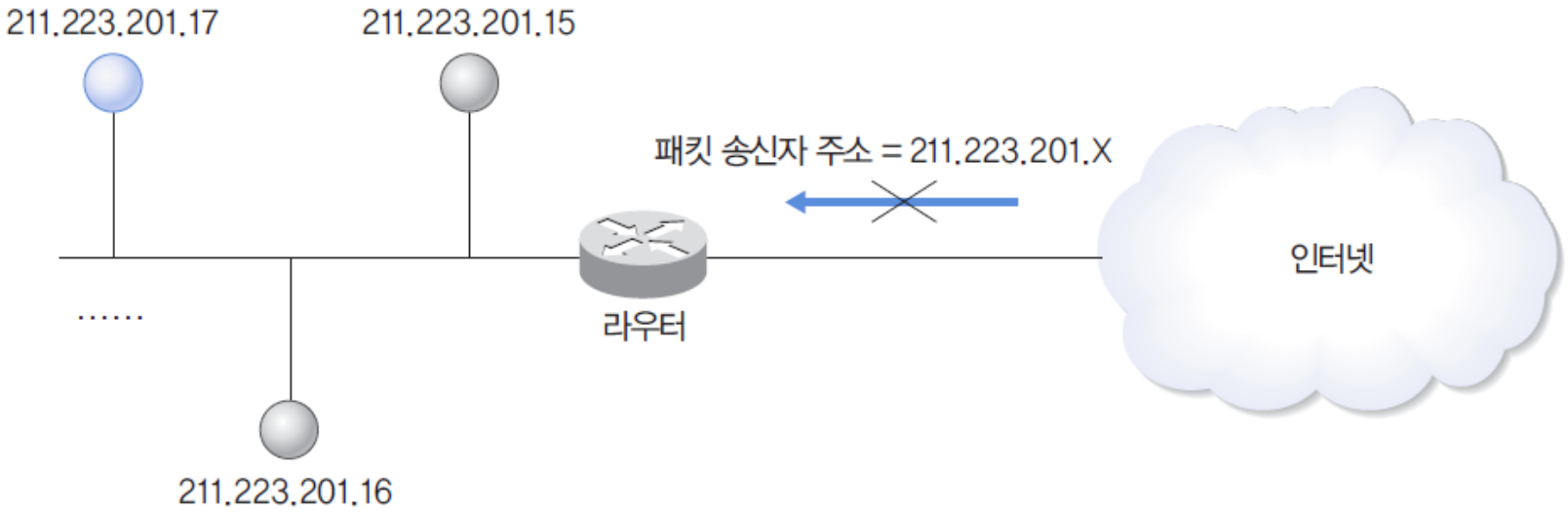


그림 17-21 위장 IP 주소의 차단

03_보안 프로토콜

- 프록시를 이용한 방화벽 구현
  - 라우터 : 네트워크 계층과 전송 계층의 헤더에 기초하여 방화벽 기능 수행
  - 프록시 : 가상의 응용 프로그램을 시뮬레이션하는 방화벽

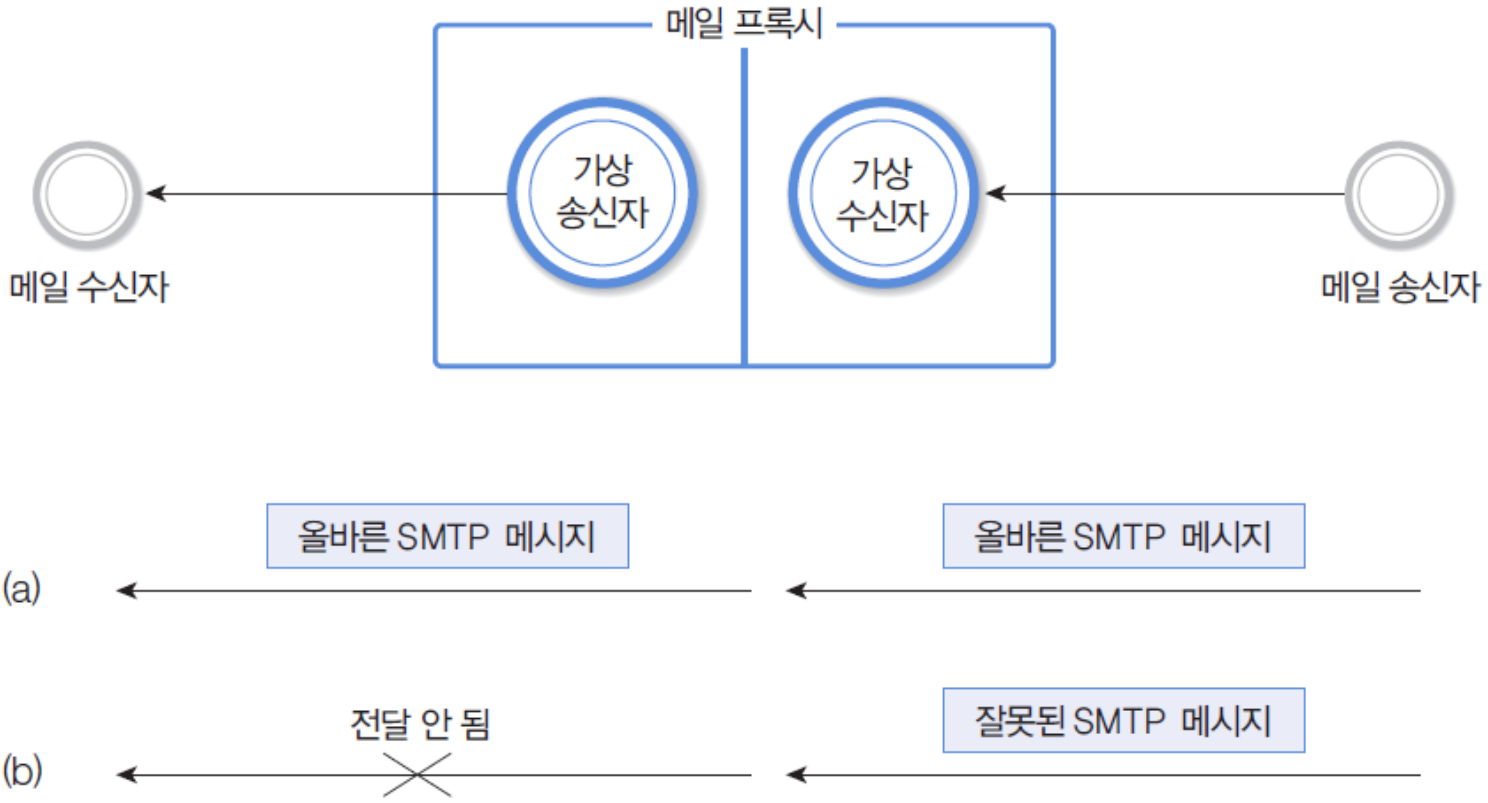


그림 17-22 메일 프록시

Thank You