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

1절. 암호화의 이해

□ 암호화 관련 용어

- 네트워크: 개방형 시스템
- 외부침입자(intruder, attacker)의 위해 행동

  ➔ 메시지 읽기, 전송방해, 메시지 수정

- 메시지 읽기 (Eavesdropping)
  - 전송 선로의 신호를 도청
  - 암호화 기법으로 해결
- 전송 방해 (Denial Of Service)
  - 메시지가 수신자에게 도착하지 못하도록 방해
  - 분산형 전송방해 행위도 있음(DDoS)
- 메시지 수정 (Modification)
  - 전송 메시지를 수정하여 메시지 의미를 왜곡

1절. 암호화의 이해

□ 정보에 대한 보안 목표 : CIA

- 기밀성(Confidentiality), 무결성(Integrity), 가용성(Availability)으로 정의

□ 기밀성을 위협하는 공격

- 도청(eavesdropping) 트래픽 분석(traffic analysis) 등

□ 무결성을 위협하는 공격

- 메시지 변경(modification) 혹은 삭제(deletion), 재사용(replaying), 부인(repudiation) 등

□ 가용성을 위협하는 공격

- 서비스 거부 공격(Denial of Service, DoS)

1절. 암호화의 이해

□ 기밀성 유지를 위한 방법 : 암호화

□암호화 관련 용어

- 암호화 용어 [그림 13-1]
  - 암호화(Encryption): 메시지 내용을 변형하여 원래의 의미를 알 수 없도록 변형
  - 해독(Decryption): 암호화된 문서를 원래의 원어로 복원
  - 원문서(P): 암호화되기 전의 원본 문서
  - 암호문(C): 암호화된 문서
  - 암호키(k): 암호문을 작성하는 과정에서 사용하는 임의의 패턴

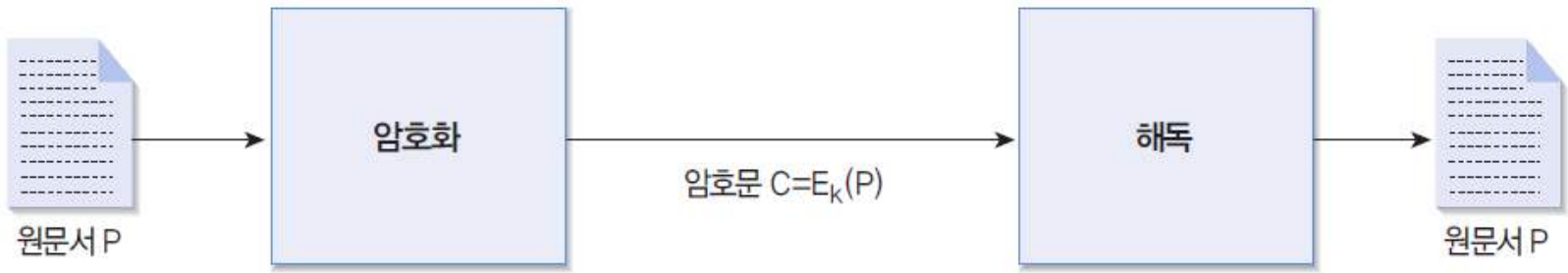


그림 17-1 암호화와 해독 과정

1절. 암호화의 이해

□ 암호화 관련 용어

- **암호화 알고리즘**
  - 암호키(k_E): 암호화 과정에서 사용하는 키
  - 해독키(k_D): 해독 과정에서 사용하는 키

  - 대칭키(Symmetric key) 방식: 암호키 = 해독키
  - 비대칭키(Asymmetric key) 방식: 암호키 ≠ 해독키

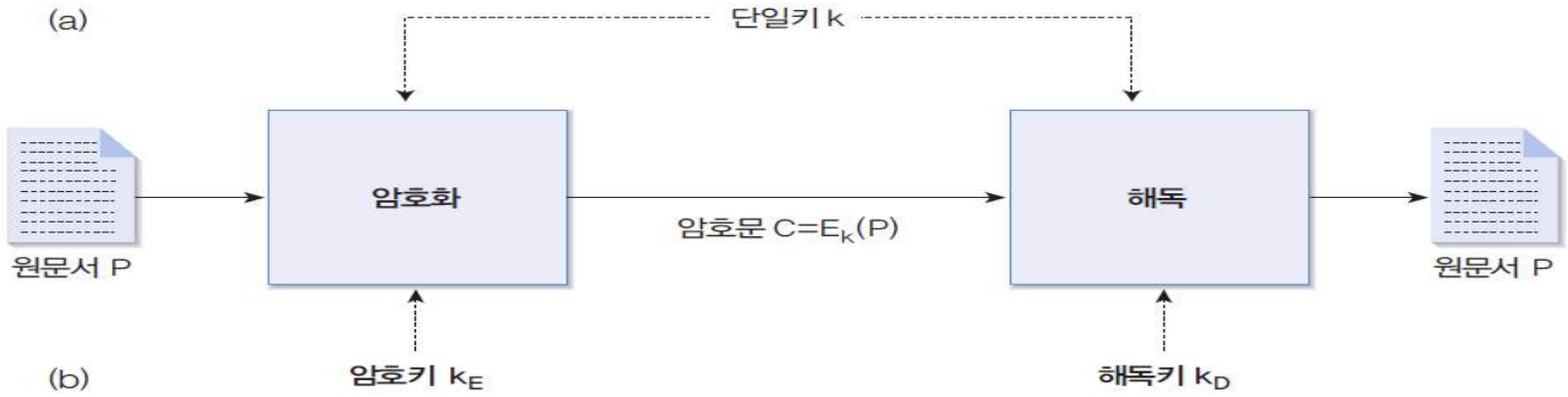
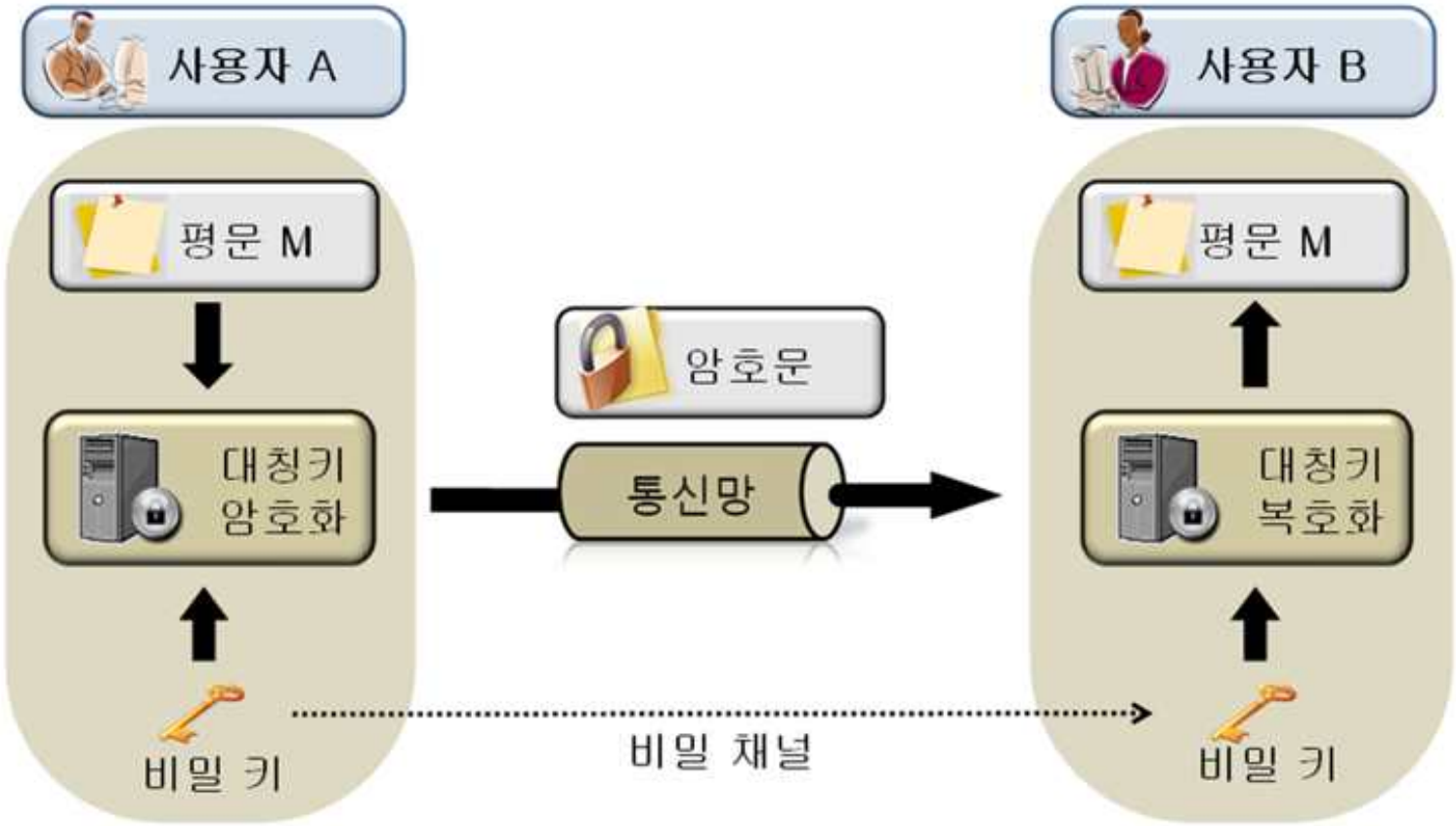


그림 17-2 키의 종류

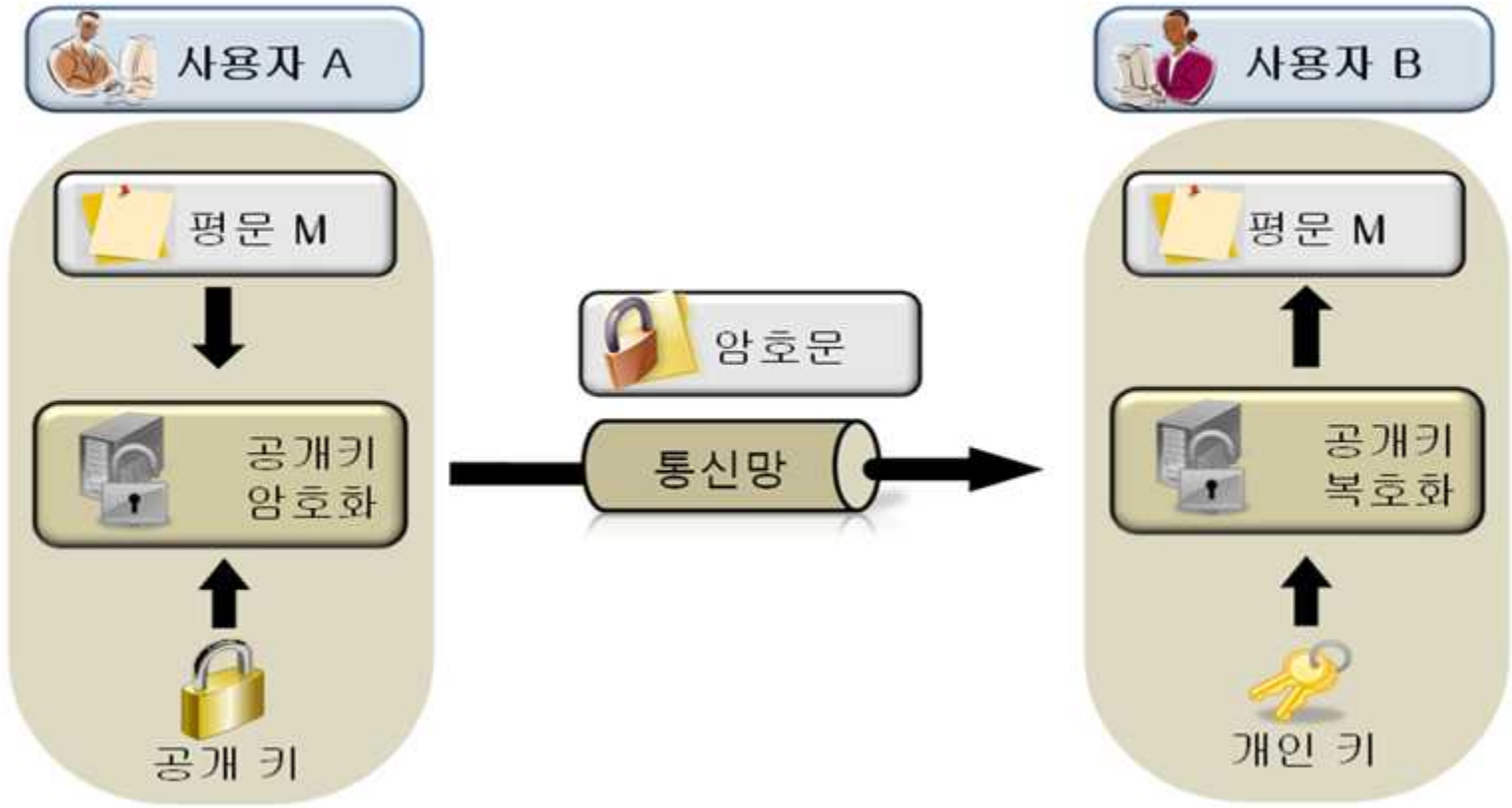
1절. 암호화의 이해

□대칭 키(비밀 키) 암호 시스템



1절. 암호화의 이해

□비대칭 키(공개 키) 암호 시스템



1절. 암호화의 이해

□ 대칭 키(비밀 키) 암호 시스템

- 고대 사회부터 시작 Caesar 암호
- Vigenere 암호
- 제 2차 세계 대전에 사용된 ENIGMA 등
- 1977년 미국의 상무성 표준국(National Institute of Standard and Technology, NIST)에서 암호 알고리즘 표준으로 DES(Data Encryption Standard) 선정
- 2000년이후 ~ AES(Advanced Encryption Standard)가 국제 표준

1절. 암호화의 이해

□ 대칭 키 암호 기본 원리

- 대체(Substitution)와 전치(Transposition)를 이용

□대체 암호화(Substitution Cipher)- 대칭 키 암호

- 특정 문자를 다른 문자로 1:1 대응

▪ 시저 암호화(Caesar Cipher)

- 알파벳 문자를 순차적으로 세 문자씩 오른쪽으로 이동
- 암호 키(테이블)

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

- 암복호의 예

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

□대체 암호화 (Substitution Cipher))- 대칭 키 암호

- **키워드 암호화(Keyword Cipher)**
  - 키워드로 지정된 단어의 문자를 먼저 적고, 나머지 문자를 알파벳 순으로 기술
  - 암호키: seoul

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
	키워드					s, e, o, u, l을 제외한 문자를 알파벳 순서로 배치																				

그림 17-5 키워드 암호화에서 사용하는 문자 변환표

  - v 이후의 평문은 암호문과 동일한 취약성

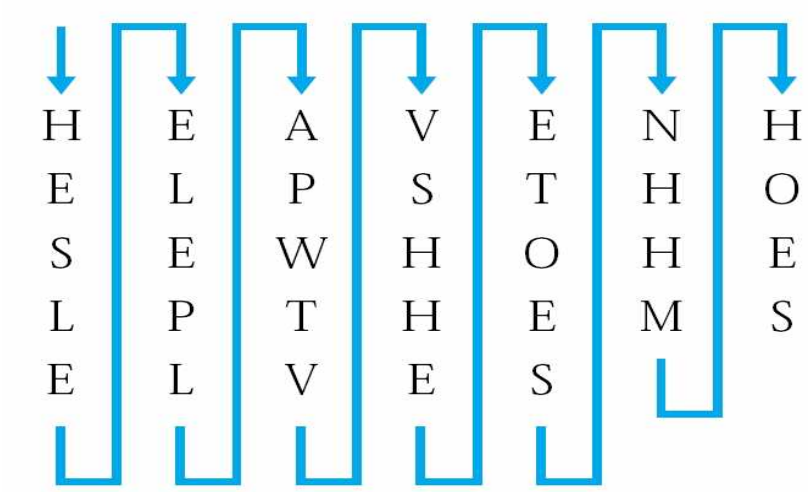
1절. 암호화의 이해

☐ 전치 혹은 치환 암호화(Transposition Cipher)- 대칭 키 암호

- 문자들의 배열 순서를 변경

▪ 컬럼 암호화(Column Cipher)-방법 1

- 전체 문장을 컬럼(열)을 기준으로 다시 배치
- 예: 컬럼의 길이가 7 인 경우
  - 원문서: HEAVEN HELPS THOSE WHO HELP THEMSELVES
  - 암호문1: hesle elepl apwtv vshhe etoes nhhm hoes



1절. 암호화의 이해

□ 전치 혹은 치환 암호화(Transposition Cipher)- 대칭 키 암호

- 키워드 암호화(Keyword Cipher)
  - 임의의 단어를 이용하여 컬럼의 순서를 결정
  - 예: NETWORK

(a) 원문서

HEAVEN HELPS THOSE WHO HELP THEMSELVES

키워드	N	E	T	W	O	R	K
순서	3	1	6	7	4	5	2

(b) 암호화 과정

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