컴퓨터 네트워크

13장. 네트워크 보안 (1)
- 암호화의 이해

이번 시간의 학습 목표

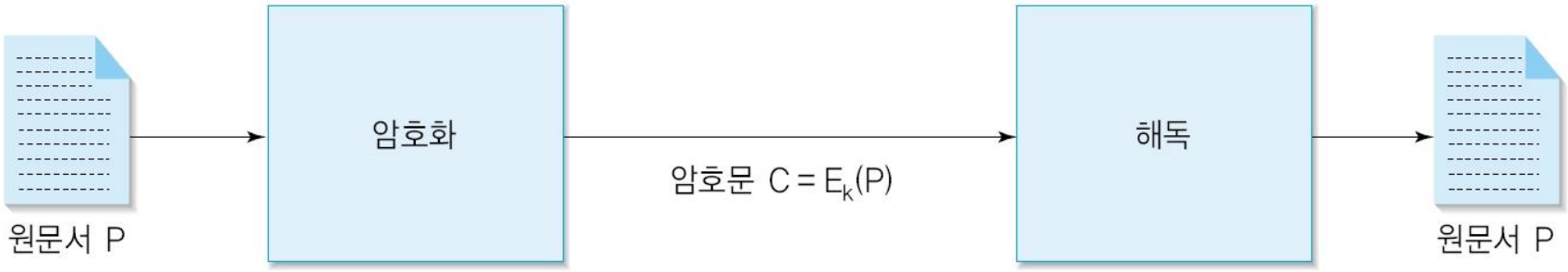
- 암호화 원리 이해
- 대체 암호화와 위치 암호화 이해

개요

- 문서의 내용을 암호화(encryption)하여 전달함으로써 외부 침입자로부터 문서 내용 보호
- 문서를 암호화하고 복호화하는 과정에 자신들만이 아는 비밀키 사용
- 컴퓨터 네트워크에서는 중간 전송매체를 통해 메시지 송수신
- 외부 침입자의 전송 메시지에 가하는 위해
  - 메시지 읽기
    - 전송 선로의 신호를 도청
    - 암호화 기법으로 해결
  - 전송 방해
    - 메시지가 수신자에게 도착하지 못하도록 방해
    - 방화벽의 불법 사이트 차단 기능도 여기에 해당
    - DoS (Denial of Service) 공격
  - 메시지 수정
    - 전송 메시지를 수정하여 메시지 의미를 왜곡

암호화 용어

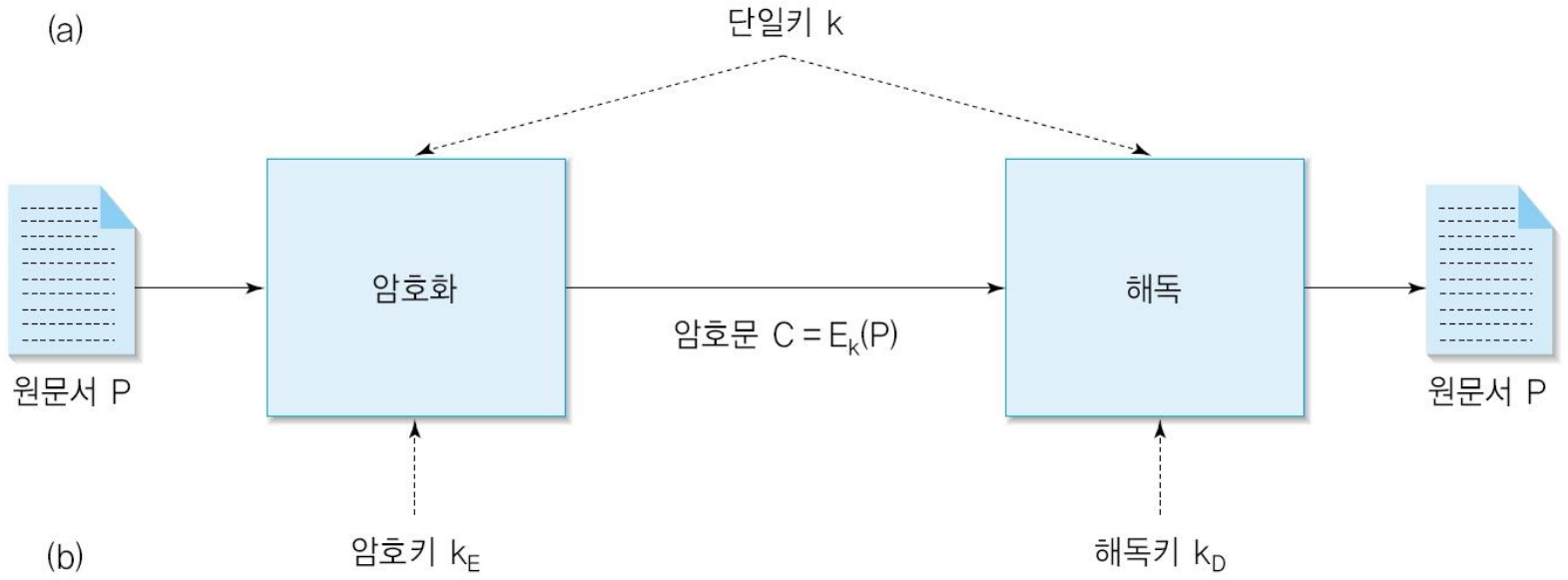
- 암호화: 메시지의 내용을 변형하여 원래의 의미를 알 수 없도록 변형
- 해독: 암호화된 문서를 원래의 원문서로 복원
- 원문서(Plain Text): 암호화되기 전의 원본 문서
- 암호문(Cipher Text): 암호화된 문서
- 암호키(k): 암호문을 작성하는 과정에서 사용하는 임의의 패턴



[그림 13-1] 암호화 과정과 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 13-2] 키의 종류

대체 암호화 (1)

- 특정 문자를 다른 문자로 1:1 대응
- 시저 암호화
  - 알파벳 문자를 순차적으로 세 문자씩 오른쪽으로 이동
  - 암호키

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

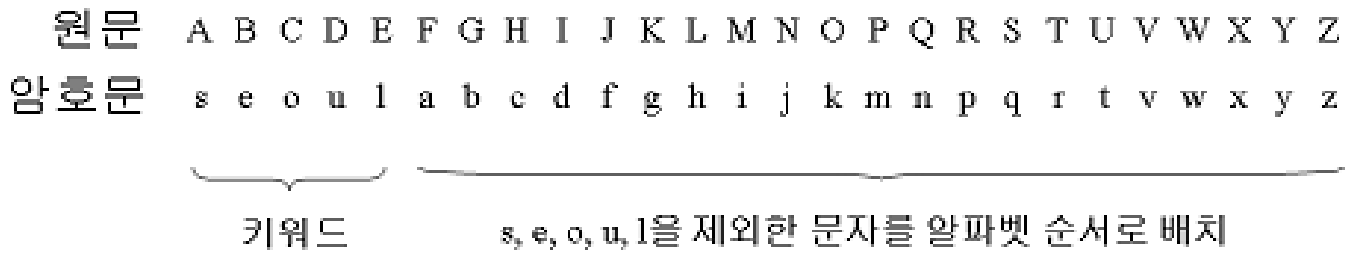
  - 예

N E T W O R K T E C H N O L O G Y

q h w z r u n w h f k q r o r j b

대체 암호화 (2)

- 키워드 암호화
  - 키워드로 지정된 단어의 문자를 먼저 적고, 나머지 문자를 알파벳 순으로 기술
  - 암호키: seoul



  - 시저 암호화에 비해 대체 문자표 추출이 어려워지나, 오른쪽으로 갈수록 원문과 암호문의 문자가 같을 확률이 높아짐

대체 암호화 (3)

- 복수개의 문자표
  - 둘 이상의 문자표를 사용
  - 예: 홀수 위치와 짝수 위치의 문자표를 다르게 사용

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	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

짝수 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

대체 암호화 (4)

- 복수개의 문자표 (계속)
  - 예

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

홀수 위치에 있는 문자

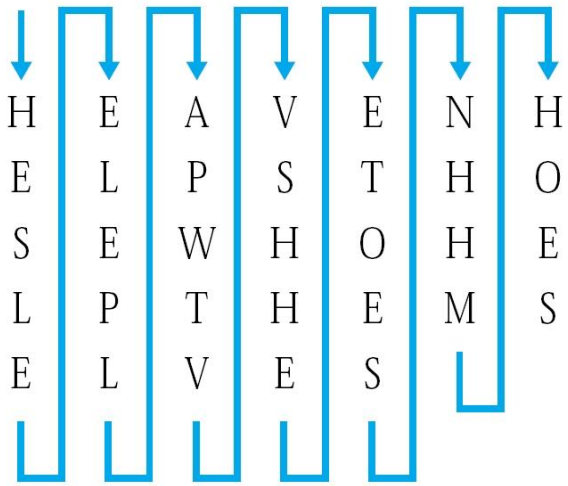
원문	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
암호문	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z	a	b	c

짝수 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

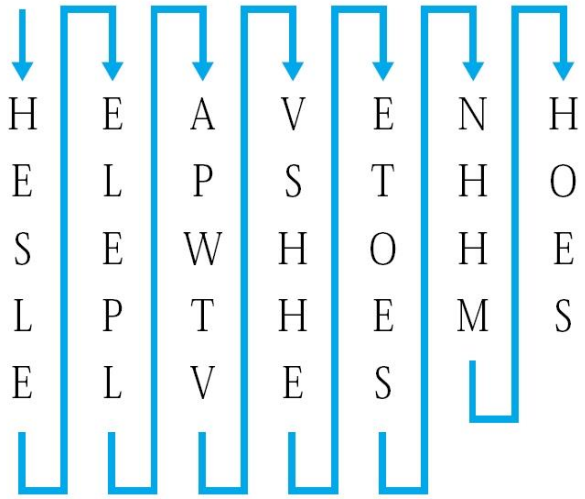
위치 암호화 (1)

- 문자들의 배열 순서를 변경하여 암호화하는 위치 암호화(Transposition Cipher)
- 각 문자의 모양은 그대로 유지한 채 문자의 배열 위치를 임의로 변경
- 컬럼 암호화
  - 전체 문장을 컬럼(열)을 기준으로 다시 배치
  - 예: 컬럼의 길이가 7 인 경우



위치 암호화 (2)

- 컬럼 암호화 (계속)
  - 예: 컬럼의 길이가 7이며, 공백에 z 문자를 강제로 채운 경우
    - 암호문2: hesle elepl apwtv vshhe etoes nhhmz heosz



  - 컬럼암호화를 두 번 수행하는 이중 컬럼암호화

위치 암호화 (3)

- 키워드 암호화
  - 임의의 단어를 이용하여 컬럼의 순서를 결정
  - 예: NETWORK
    - 원문서: HEAVEN HELPS THOSE WHO HELP THEMSELVES
    - 암호문: elepl hoesz hesle etoes nhhmz apwtv vshhe

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

질의 / 응답