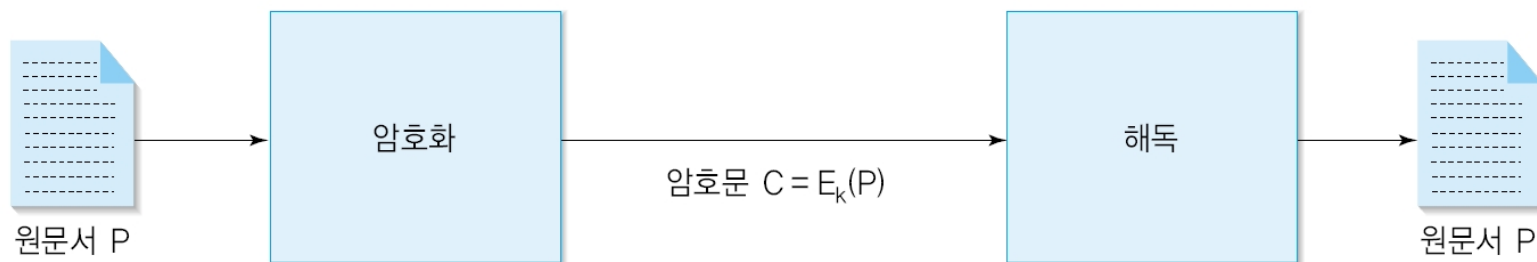


1절. 암호화의 이해

- 암호화 관련 용어

- 암호화 용어 [그림 13-1]

- 암호화: 메시지의 내용을 변형하여 원래의 의미를 알 수 없도록 변형
 - 해독: 암호화된 문서를 원래의 원어로 복원
 - 원문서(P): 암호화되기 전의 원본 문서
 - 암호문(C): 암호화된 문서



[그림 13-1] 암호화 과정과 용어

1절. 암호화의 이해

- 암호화 관련 용어

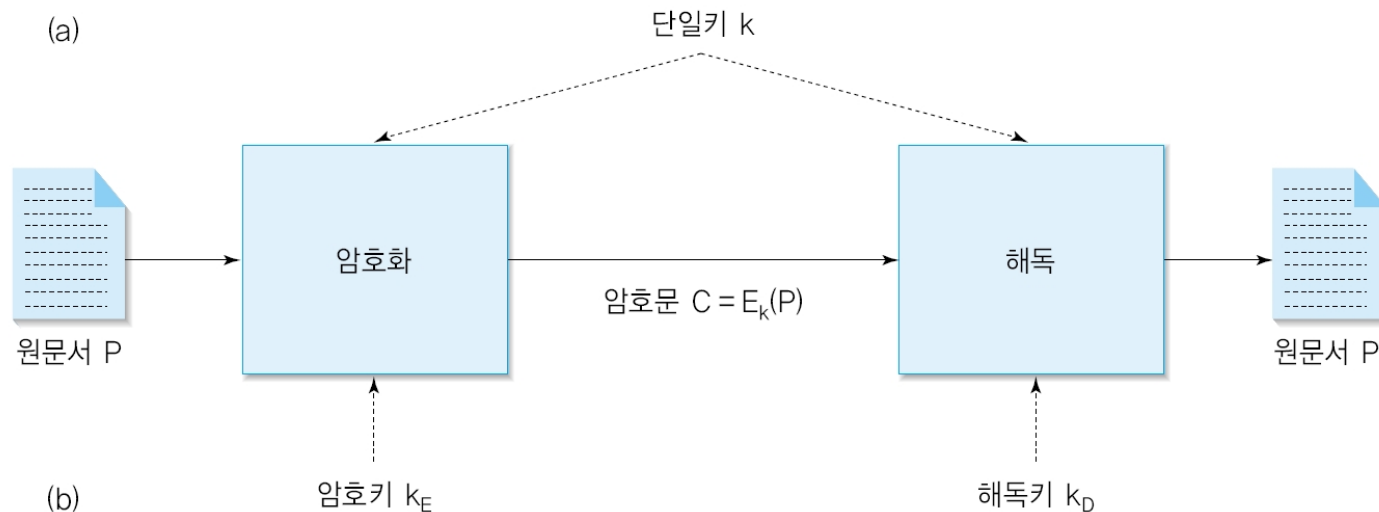
- 암호화 알고리즘

- 암호키(k_E): 암호화 과정에서 사용하는 키

- 해독키(k_D): 해독 과정에서 사용하는 키

- 대칭키 방식: 암호키 = 해독키 [그림 13-2(a)]

- 비대칭키 방식: 암호키 \neq 해독키 [그림 13-2(b)]



[그림 13-2] 키의 종류



암호화의 이해

- 대체 암호화

- 키워드 암호화

- 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

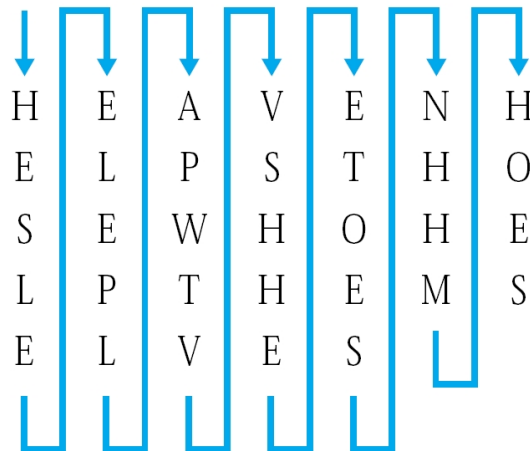
암호화의 이해

- 위치 암호화

- 문자들의 배열 순서를 변경

- 컬럼 암호화

- 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



암호화의 이해

- 위치 암호화

- 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
<hr/>							
	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