정보보안에 대한 이해

01_암호기초

- **암호학(Cryptology)**
  - "비밀코드"를 만들거나 해독하는 과학
- **암호생산(Cryptography)**
  - "비밀코드"를 만드는 것
- **암호분석(Cryptanalysis)**
  - "비밀코드"를 해독하는 것
- **암호(Crypto)**
  - 암호학, 암호생산, 암호분석 세가지 모두 또는 그 이상
- **암호체계는 평문을 암호화 하는데 사용**
- **암호화 결과는 암호문**
- **암호문을 평문으로 복원하는 것은 복호화**
- **키는 암호체계를 만드는데 사용**
- **대칭키 암호체계는 같은 키를 암호화와 복호화를 위해 사용**
- **공개키 암호체계는 공개키는 암호화, 개인키는 복호화(서명)에 사용**

01_암호기초

❖ 암호 체계

- 기본 가정
  - 서로 다른 암호체계는 완전히 공격자에게 알려져 있고, 단지 키만이 유일한 비밀

☞ **커크호프 원칙(Kerckhoffs Principle) → 암호 알고리즘은 비밀이 아니다.**

- 왜 이런 가정을 하는가?
  - 경험적으로 볼 때, 비밀 알고리즘들은(공개되었을 때) 알고리즘 자체는 강력하지 않을 경우가 많다.
  - 비밀 알고리즘은 결국 공개된다.
  - 사전에 취약점을 발견하는 것이 유리하다.
  - 더 많은 사람이 분석하면 할수록 보안상 결점을 더 확실하게 발견 할 수 있다.

01_암호기초

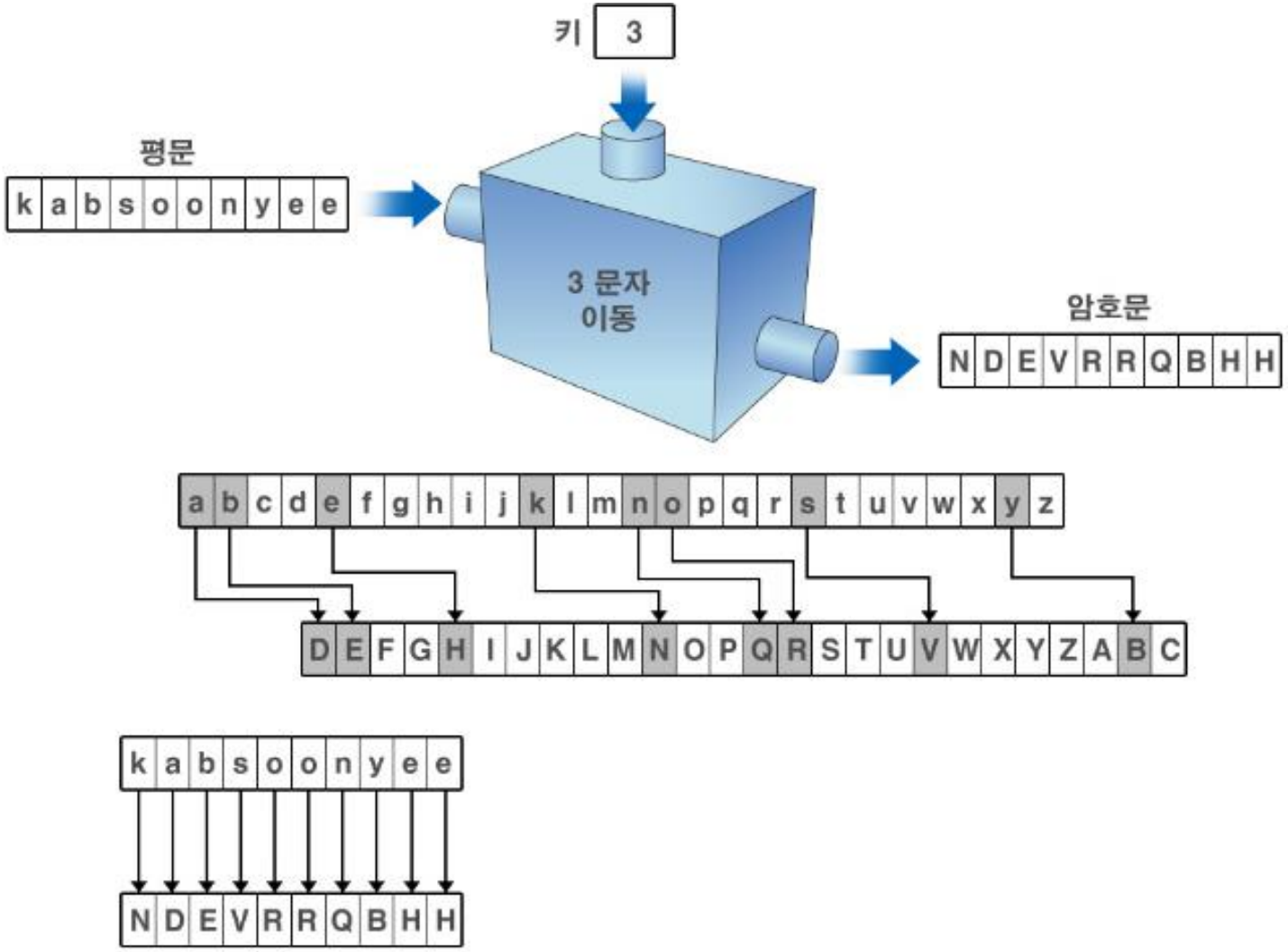
❖ 고전암호-치환용 암호

- 평문의 문자 하나하나를 암호문의 문자로 바꾸는 것
- 대표적으로 카이사르 암호
  - 암호기원전 100년경에 로마의 장군 카이사르가 썼던 암호로, 시저 암호라고도 불린다
  - 평문: **fourscoreandsevenyearsago**
  - Key

평문	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
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

  - 암호문: **IRXUVFRUHDAGVHYHABHDUVDIR**

01_암호기초


키
3
평문
k a b s o o n y e e
3 문자
이동
암호문
N D E V R R Q B H H
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
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
k a b s o o n y e e
N D E V R R Q B H H

#_TEST

카이사르 암호(Key=3)체계가 사용되었다면 다음 암호문을 복호화하여 평문을 찾으시오.

암호문 VSRQJHEREVTXDUHSDQWU

평문

01_암호기초

단순하지만 않은 치환 경우

- 주어진 n ∈ {0,1,2,…,25}에서 n 시프트
- 키는 n
- 예제: 키 = 7

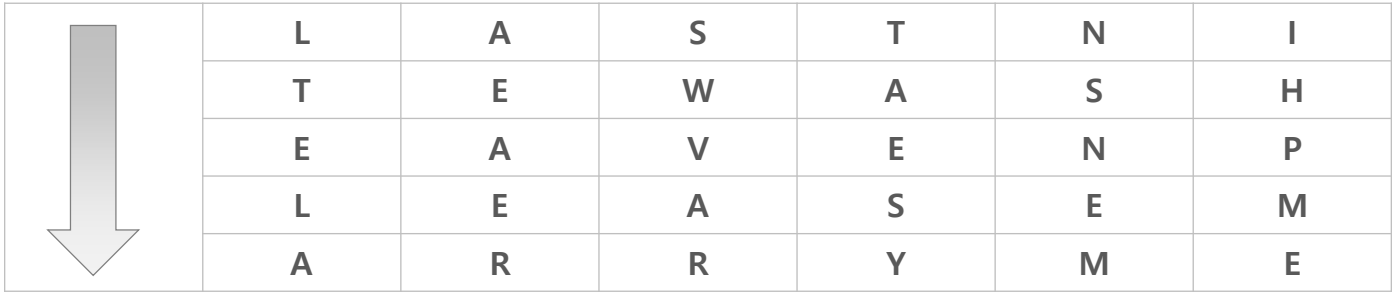
평문	a	b	c	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y
암호문	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F

01_암호기초

❖ 고전암호-전치형 암호 (자리를 옮기다)

- 평문의 문자 위치를 바꾸는 방법
  - FIVE AM → IVEA MF

    ☞ 문자가 재배치 되었다고 하더라도 암호문의 모든 문자들은 평문의 문자들과 동일
  - 평문: LAST NITE WAS HEAVEN PLEASE MARRY ME
  - 암호문: LTELAAEAERSWVARTAESYNSNEMIHPME



L	A	S	T	N	I
T	E	W	A	S	H
E	A	V	E	N	P
L	E	A	S	E	M
A	R	R	Y	M	E

  - 6열로 된 처리 장치 (5*6 행렬로 해당 행렬로 문자를 읽어내는 방법이 암호화 방법)
  - 이 암호를 풀어야 하는 사람은 2가지를 알아야 한다.

    → 몇행 몇열의 행렬인지, 행렬들의 문자들을 어떤 식으로 읽었는지

#_TEST

다음 평문을 이용하여 5*6 행열의 전치암호를 통해 암호문을 만드시오.

평문: OUR STUDENTS ARE STUDYING THIS BOOK

01_암호기초

❖ 고전암호의 약점 : 언어적인 패턴을 숨기지 못했다.

- 평문: EVERYONE MUST ATTACK BEFORE FIVE AM
- 암호문: HYHUBRQH PXVW DWWDFN EHIRUH IOYH DP
  - H=6개

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
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

☞ 알파벳 문자 중에 E는 가장 많이 사용되는 알파벳 문자
☞ 알파벳 문자 중에 T는 두 번째로 많이 사용되는 알파벳 문자

※ 언어적인 패턴과 단어의 중복 사용을 숨기지 못했기 때문

01_암호기초

❖ 문자와 단어의 사용빈도

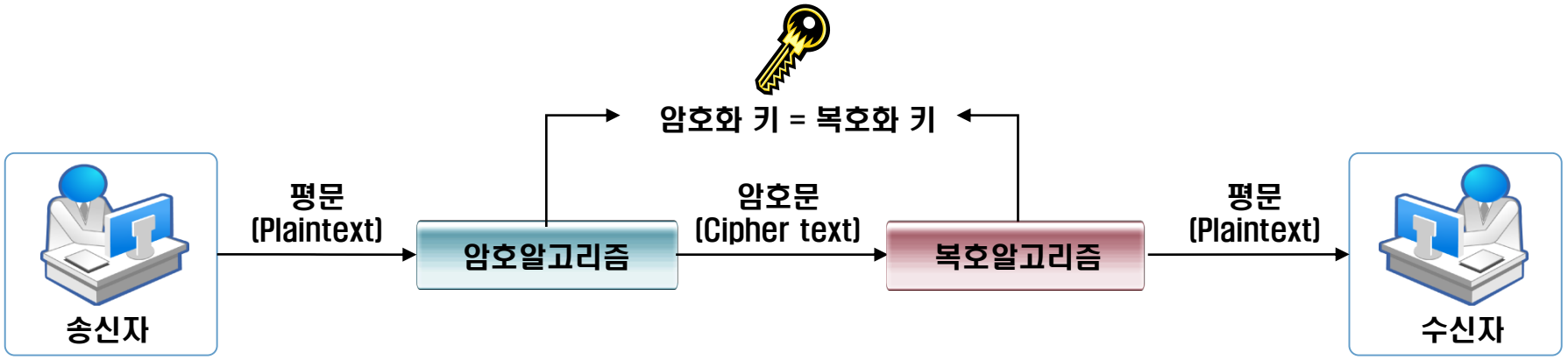
아랍의 언어학자들이 천년 전보다 더 이전에 아랍 언어에 대해서 통계적인 분석을 시작했던 이래로, 어떤 언어에서 문자와 단어의 쓰임에 대한 연구가 메시지를 암호화하거나 복호화하는데 도움을 주었다. 영어의 경우에 해당하는 문자와 문자간의 결합과 단어의 사용빈도에 대한 통계자료가 아래에 있다.

- E는 가장 많이 쓰이는 문자이다. 그 다음이 T이고, O, A, N 순이다.
- T는 단어의 시작에 가장 많이 쓰이는 문자이다. E는 단어의 끝에 가장 많이 쓰이는 문자이다.
- A와 I는 영어에서 오직 하나의 문자로 구성된 단어이다. (가령, a house, I am 등) "to"와 "in"이라는 단어는 영어에서 가장 빈번하게 쓰이는 두 개의 문자로 구성된 단어이다. "the"와 "and"는 영어에서 가장 빈번하게 쓰이는 세 개의 문자로 구성된 단어이다. "that"은 영어에서 가장 빈번하게 쓰이는 네 개의 문자로 된 단어이다.
- "ll", "ee", "tt", "ff", "oo", "rr", "nn", "pp", "cc"는 영어에서 가장 많이 쓰이는 중복된 문자들이다. "the", "ing", "ion", "ent"는 가장 빈번하게 쓰이는 세문자의 결합이다.
- N은 모음 뒤에 가장 빈번하게 쓰이는 자음이다.

02_대칭키 암호와 공개키 암호

관용암호

- 비밀키 암호, 대칭 암호, 단일키 암호 방식이라 부른다.
- 암호화, 복호화에 같은 키를 사용하는 방식으로 키의 개수: N(N-1)/2
- DES, 3DES, SEED, AES 등



대칭 암호시스템의 장점

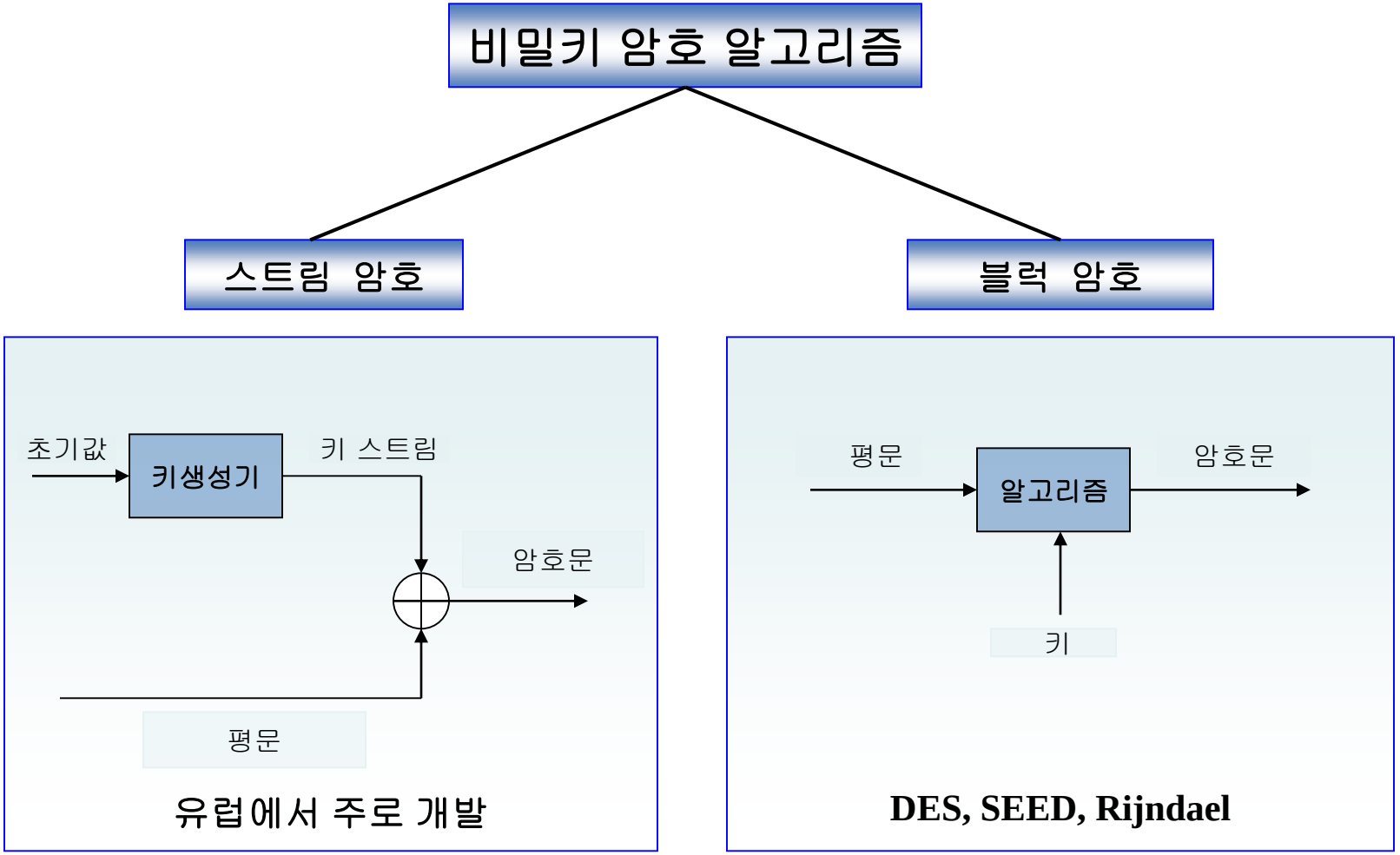
- 구현이 용이 (적은 비용)
- 빠른 속도(실시간 서비스)
- 키 크기가 상대적으로 작음
- 각종 암호시스템의 기본으로 작용

대칭 암호시스템의 단점

- 안전하게 키를 공유하는 방법에 제한
- 관리할 키의 가지 수가 많음
- 자주 키를 교환해야 하는 경우에 불편
- 디지털 서명 등의 기법에 적용하기가 곤란

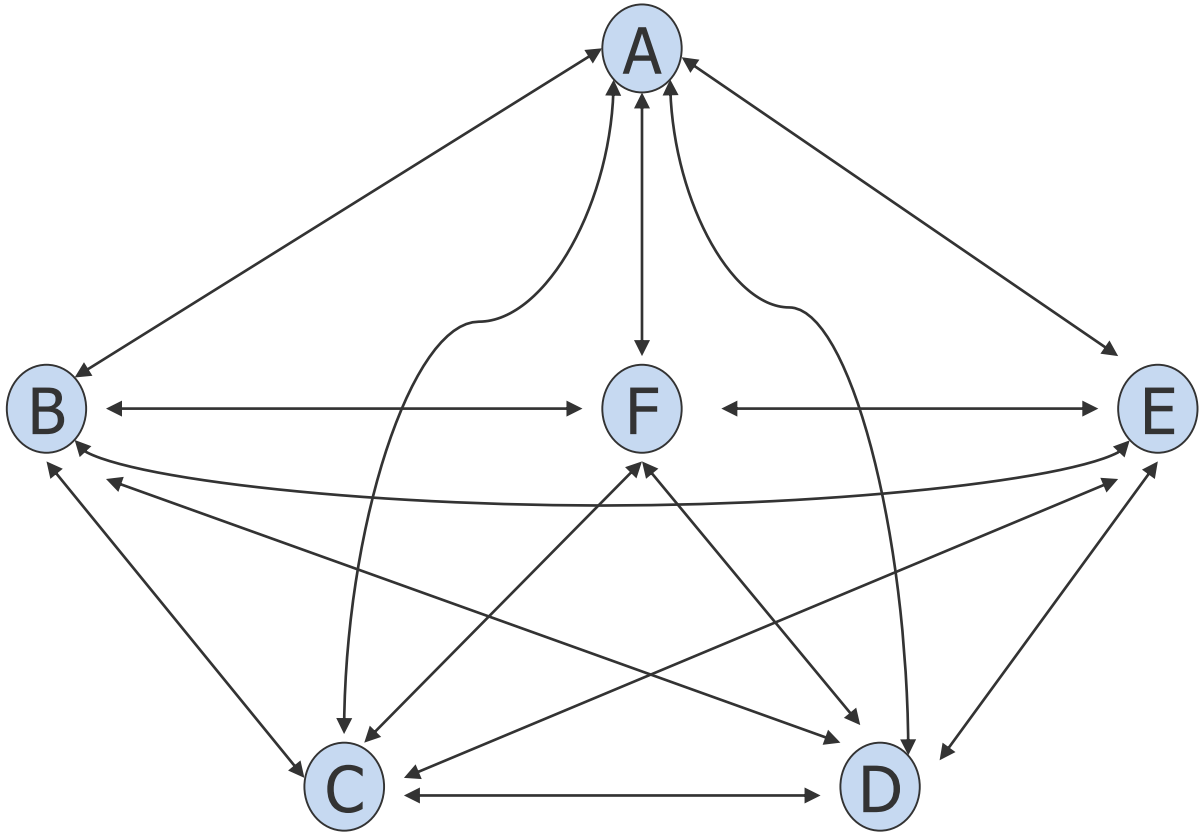
02_대칭키 암호와 공개키 암호

❖ 비밀키암호 알고리즘 분류



02_대칭키 암호와 공개키 암호

❖ 공개키 암호의 출현 배경: 키 관리 문제 발생



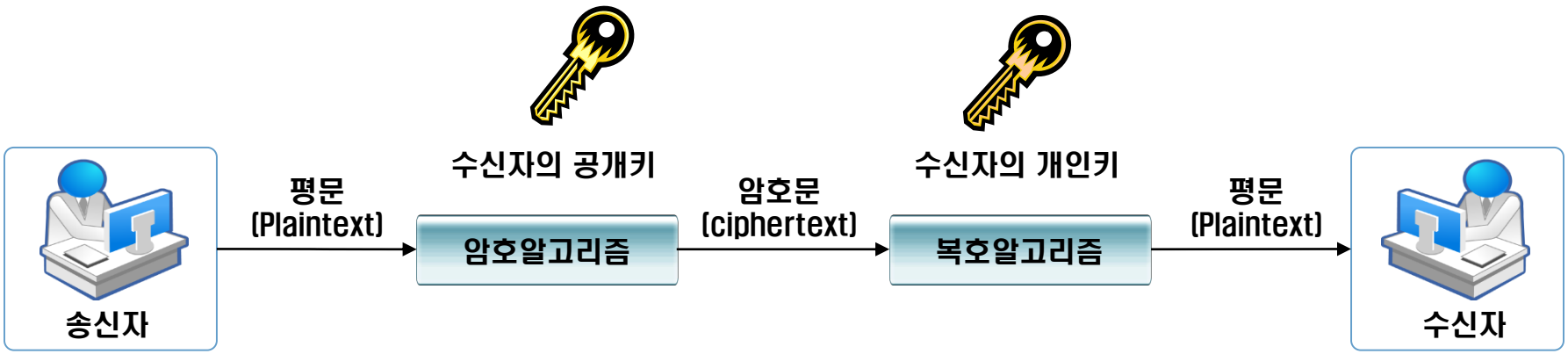
비밀키암호를 이용하면
${}_nC_2 = n(n-1)/2$
개의 키쌍이 필요

⇒ 키 전송을 위한 안전한 채널이 필요! 키 관리 문제 대두

02_대칭키 암호와 공개키 암호

❖ 공개키 암호

- 암호 알고리즘과 암호키를 알아도 복호키 계산 불가능
- 암호화, 복호화에 다른 키를 사용하는 방식으로 키의 길이 2N
- RSA, DH, ECC 등



공개키 암호시스템의 장점

- 키 분배 및 키 관리 의 용이성
- 디지털 서명에 적용 가능
  문서 서명효과, 발신처 인증, 부인봉쇄
- 키 보유 수가 적음

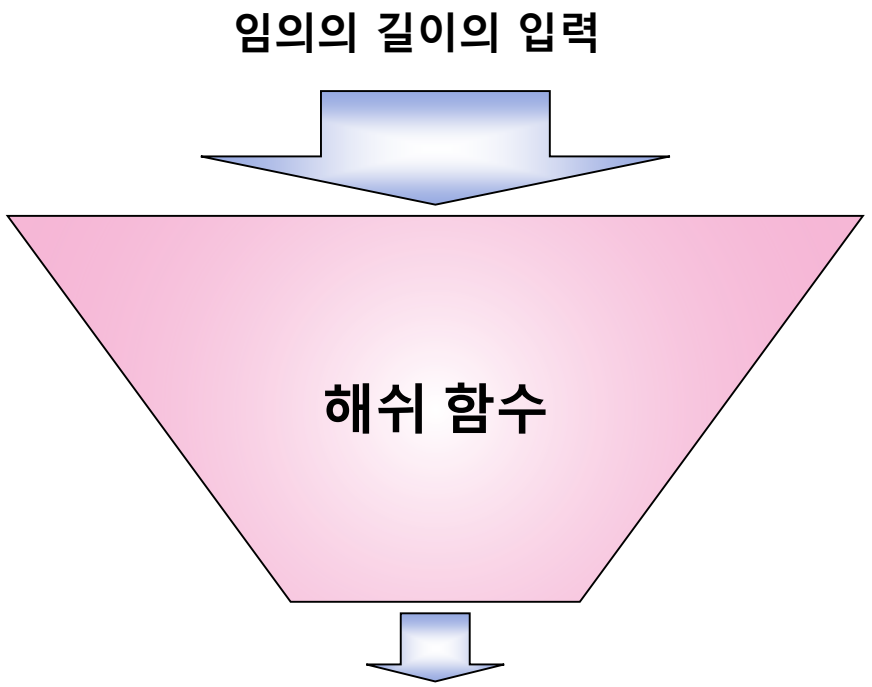
공개키 암호시스템의 단점

- 속도가 느림
- 구축 비용이 많이 듬

03_해쉬함수

해쉬 함수란

- 임의의 길이의 입력을 받아 고정된 짧은 길이의 출력을 생성하는 함수
- 해쉬 값은 다음 식과 같은 함수 H에 의해서 만들어진다.
  - h = H(M)



03_해쉬함수

❖ 해쉬 함수의 용도

- 일반적
  - 전체 data를 작은 길이의 고정된 축약 값으로 만들어 효율적으로 저장, 관리하기 위한 방법
- 암호학적
  - 송신자의 인증과 메시지 인증, 데이터의 무결성, 디지털서명을 효율적으로 처리하기 위한 방법

04_전자서명

패러다임의 변화

현재

종이문서

계약문서

무역거래

예금청구서

전자화

정보화사회

전자문서

전자계약문서

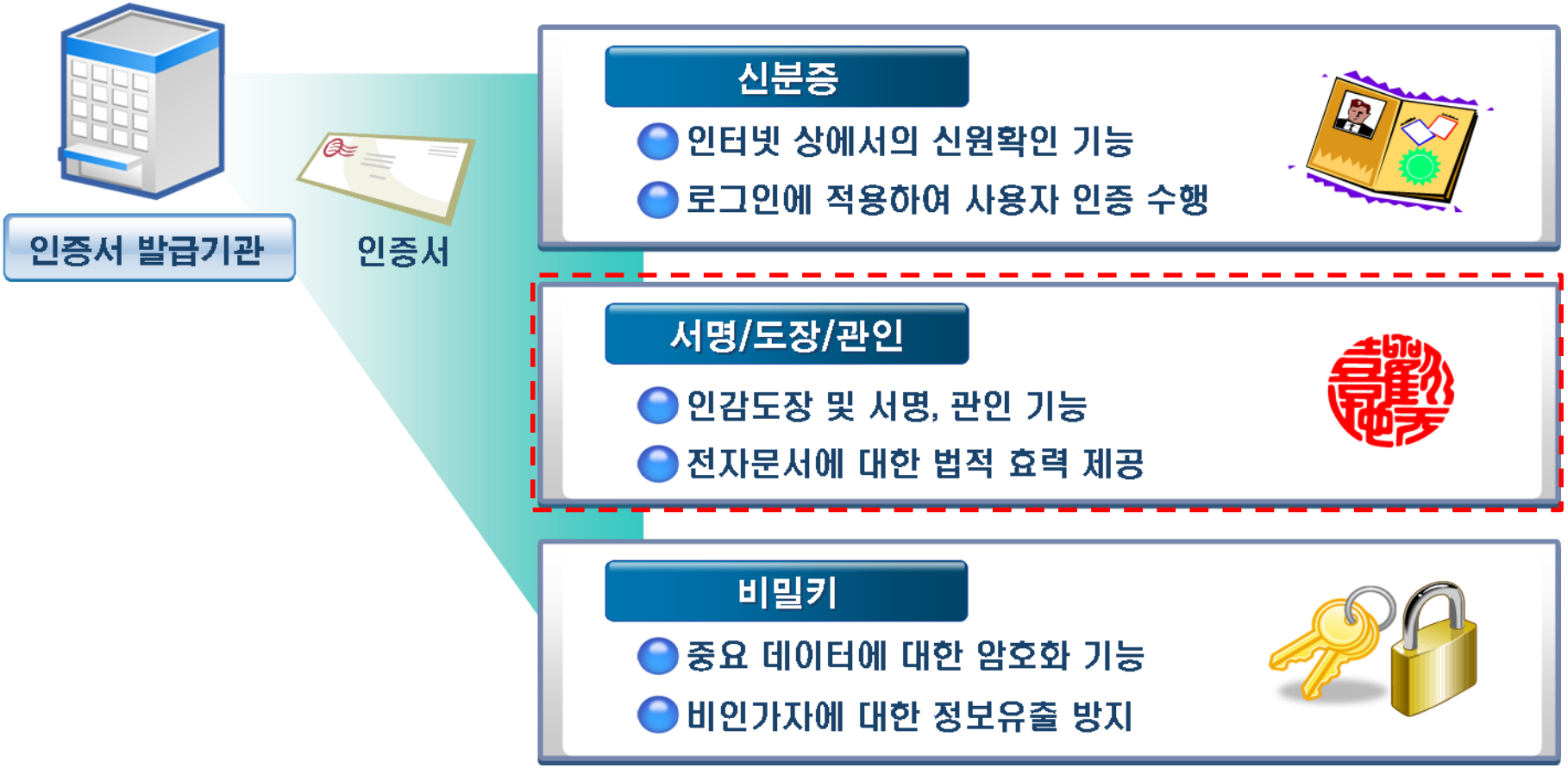
EDI

홈뱅킹

전자화된 서명방식 구현의 필요성

04_전자서명

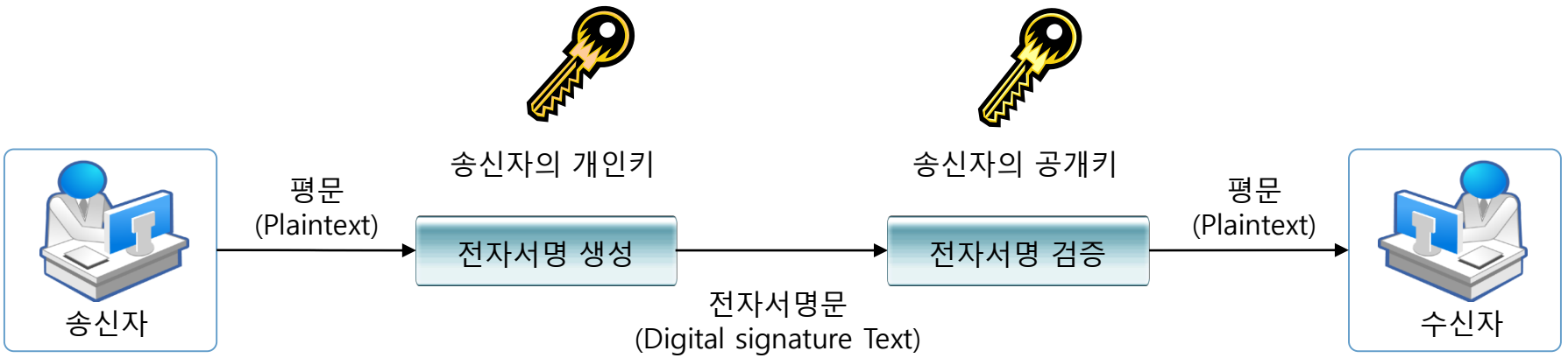
❖ PKI기반의 인증서 용도



04_전자서명

❖ 전자서명의 용도

- 전자서명 기술은 공개키 암호 방식의 역 변환을 이용하여 하는 것으로 서명자의 신원을 확인하고 자료의 내용에 대한 그 사람의 승인을 나타낼 목적으로 사용



전자 서명이란?

➢ 나만 할 수 있는 능력으로 문서나 메시지를 보낸 사람의 신원이 진짜임을 증명하기 위해 사용되는 기술 [서명자의 도움 없이도 검증 가능]

➢ 데이터의 위조를 막고, 부인방지를 위한 방법으로 가장 많이 사용됨

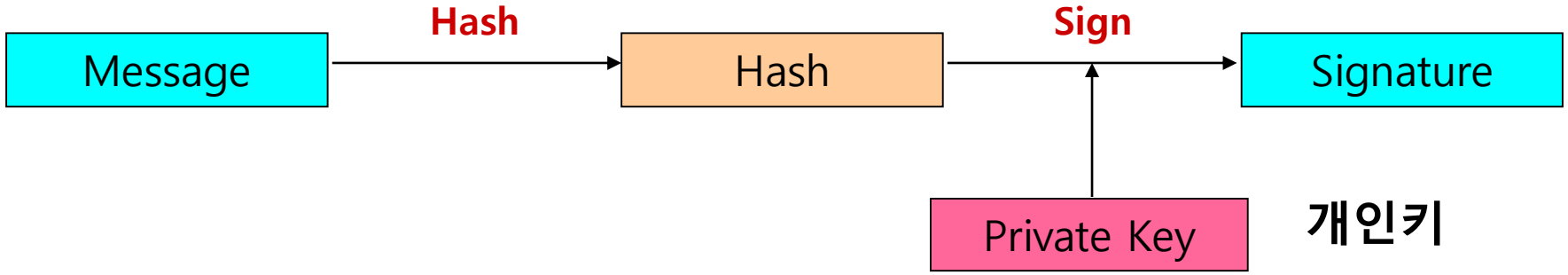
➢ 전자서명 법에 의거하여 법적 효력 발생

전자서명 알고리즘

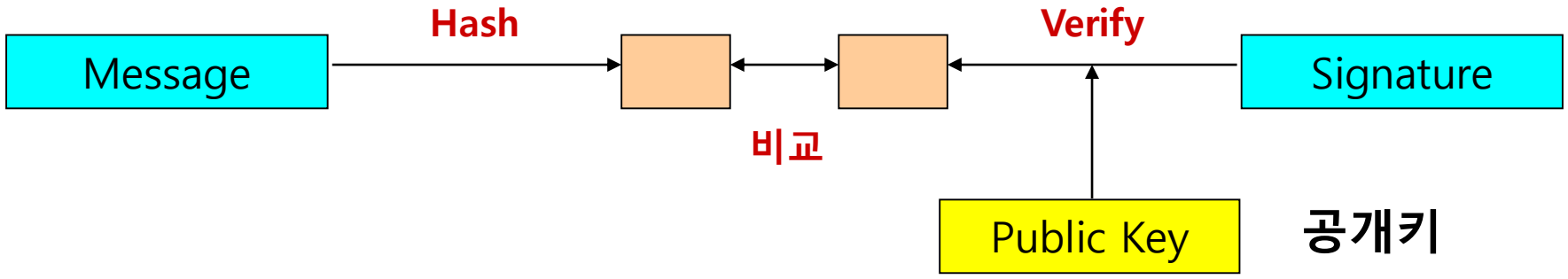
➢ RSA 서명, DSS (Digtal signature Standard), KCDSA 등 다양한 공개키 알고리즘으로 적용이 가능

04_전자서명

서명 생성



서명 검증



04_전자서명

전자서명의 요구조건

- 위조불가 (Unforgeable)
- 서명자인증 (Authentic)
- 부인불가 (Nonrepudiation)
- 변경불가 (Unalterable)
- 재사용불가 (Not Reusable)

전자서명을 통해 제공되는 주요 서비스

- 사용자 인증 (User Authentication)
- 데이터 무결성 (Data Integrity)
- 부인 방지 (Non repudiation)