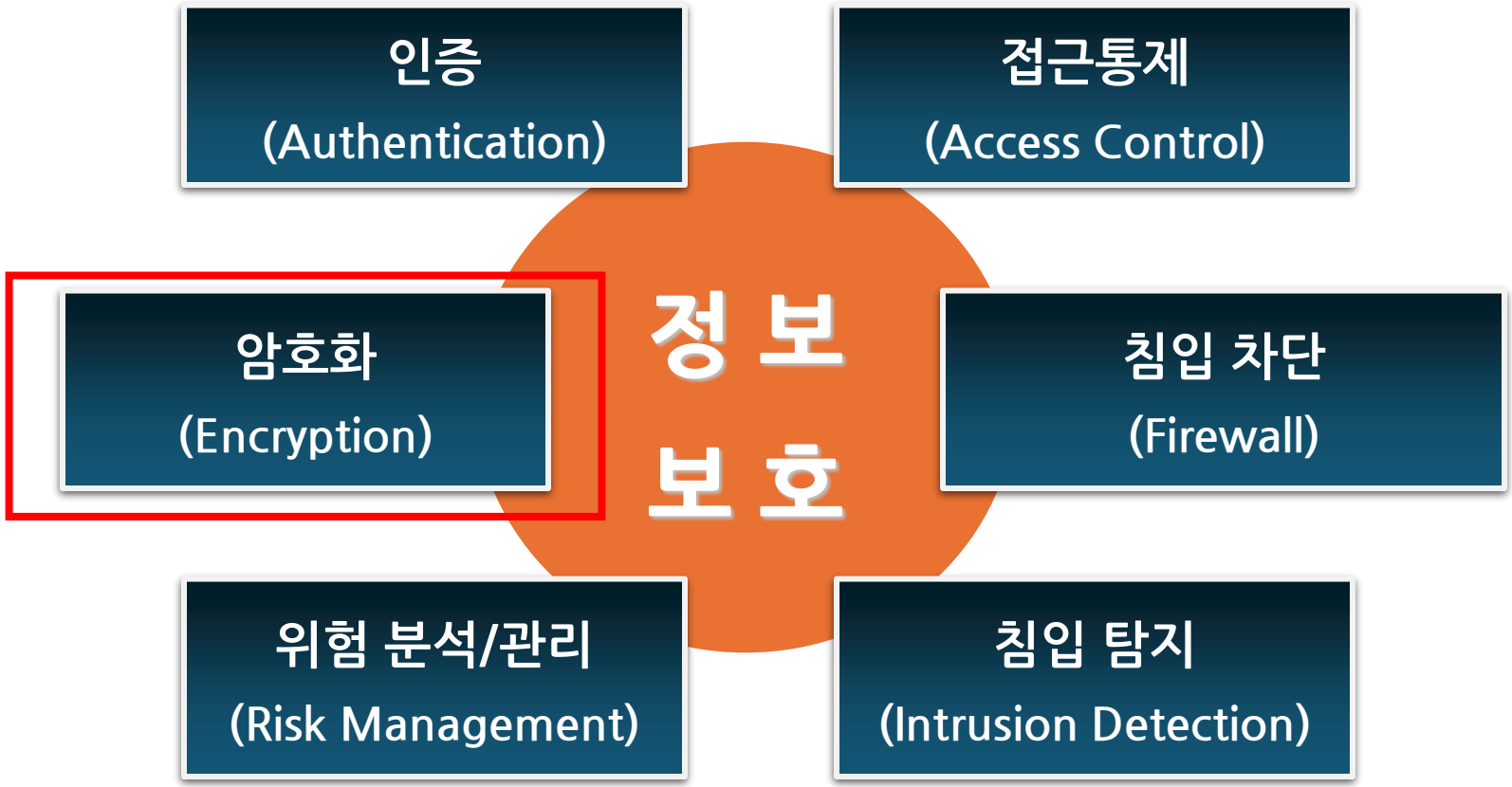
암호 기술 (Encryption)

2024. 9

컴퓨터·소프트웨어공학과
이 형 효
(hlee@wku.ac.kr)

정보보안 기술 - 암호기술


인증
(Authentication)
접근통제
(Access Control)
암호화
(Encryption)
정 보
보 호
침입 차단
(Firewall)
위험 분석/관리
(Risk Management)
침입 탐지
(Intrusion Detection)

정의

- 암호화, 복호화를 위한 원리, 수단, 방법 등을 취급하는 기술이나 과학
  - **암호화: 평 문 → 암호문**
  - **복호화: 암호문 → 평 문**

주요 용어(terminology)(1)

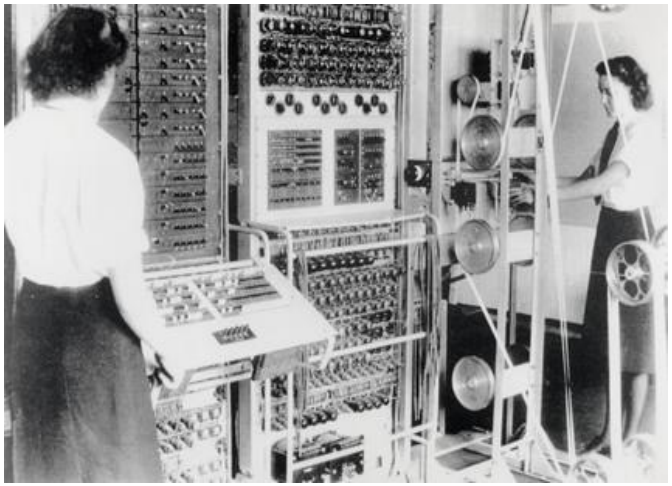
- **평문, 원문(P, plain text)**
  - 암호화되지 않은 상태의 정보
- **암호문(C, cipher text)**
  - 암호화 과정을 거쳐 암호화된 정보
- **암호화 과정(E, Encryption)**
  - plain text → cipher text
  - 암호 알고리즘(=암호 방법)
- **복호화 과정(D, Decryption)**
  - cipher text → plain text

주요 용어(terminology)(2)

- **암호 키(Encryption Key)**
  - 암호화 과정에 사용되는 정보(키)
- **복호 키(Decryption Key)**
  - 복호화 과정에 사용되는 정보(키)
- **암호 시스템(Cryptosystem)**
  - 암호/복호 알고리즘과 암호/복호 키
- **암호 분석가(Cryptanalyst)**
  - 수학 또는 기타 지식을 이용하여 암호문을 분석하는 사람

암호시스템과 전쟁

독일군 암호 장비(enigma) 수수께끼, 암호

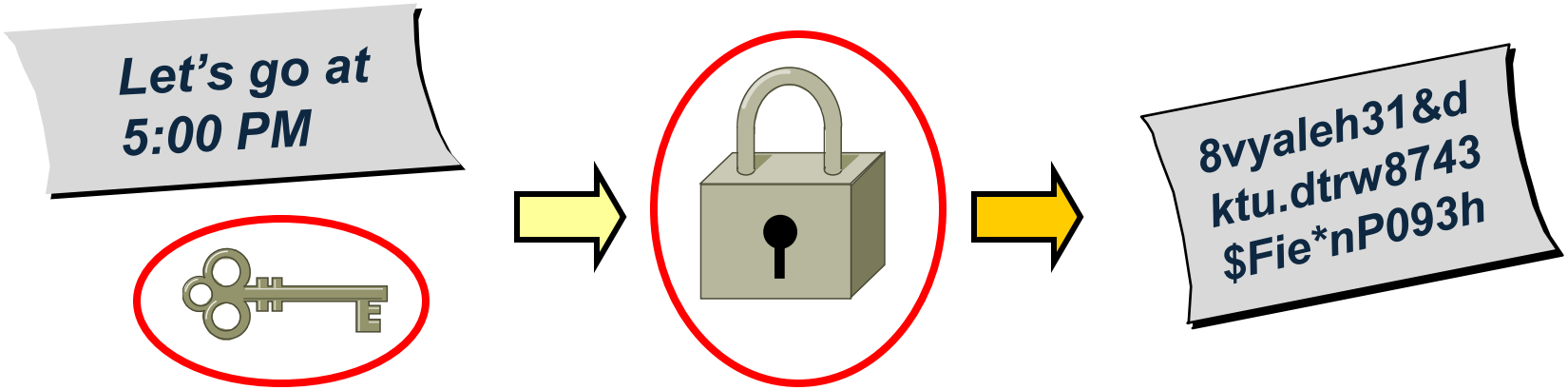


영국의 Colossus 컴퓨터
(1943, 1944)

Alan Turing(1912~1954)

주요 용어(terminology)(3)

- 암호화(Encryption)

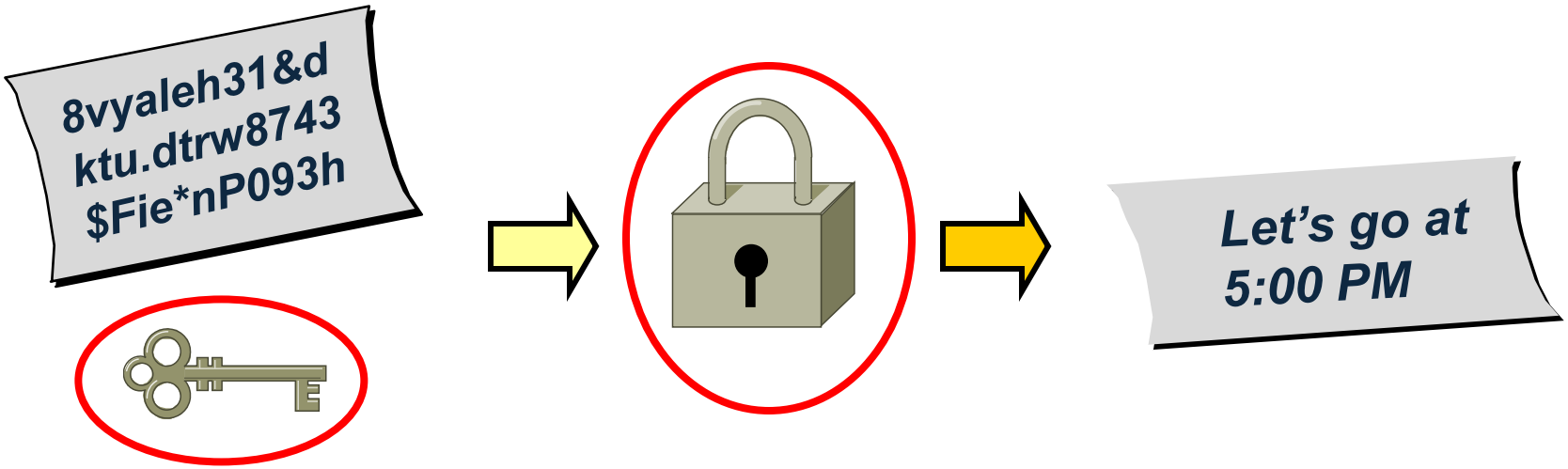


- 평문(plain text)
- 암호 키(encryption key)
- 암호 알고리즘(encryption algorithm)
- 암호문(cipher text)

암호시스템

주요 용어(terminology)(4)

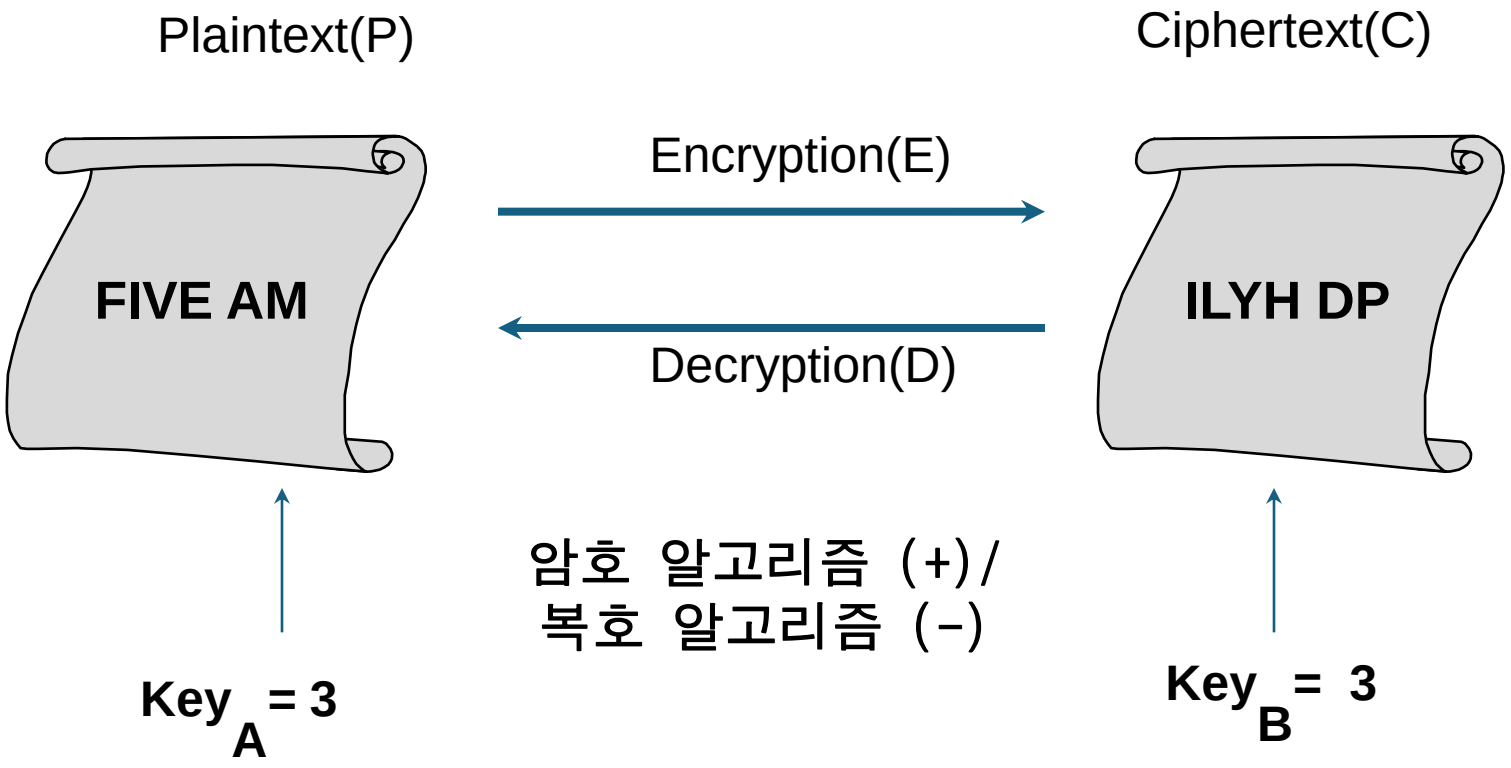
- 복호화(Decryption)



- 암호문(cipher text)
- 복호 키(decryption key)
- 복호 알고리즘(encryption algorithm)
- 평문(plain text)

암호시스템

Caesar Cipher(1)



Caesar Cipher(2)

- 암호 알고리즘(방법)
  -
- 복호 알고리즘(방법)
  -
- 암호 키
  -
- 복호 키
  -

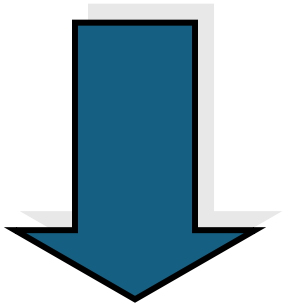
Caesar Cipher(3)

- **Substitution 방식**
  - 치환(**置換**), 대체(**代替**) 방식
- **취약점**
  - 가능한 키의 수가 25개로 제한
    - ✓ 암호 키: 1, 2, 3, …, 25
    - ✓ 복호 키: 1, 2, 3, …, 25
  - 글자와 단어의 반복 횟수로 평문 추정 가능

Caesar Cipher(4)

- **암호문: I L Y H D P**
  - (1) H K X G C O
  - (2) G J W F B N
  - (3) F I V E A M
  - (4) E H U D Z L
  - ….
  - (24) K O A J F R
  - (25) J M Z I E Q

D W W D F N



A T T A C K

Caesar Cipher(5)

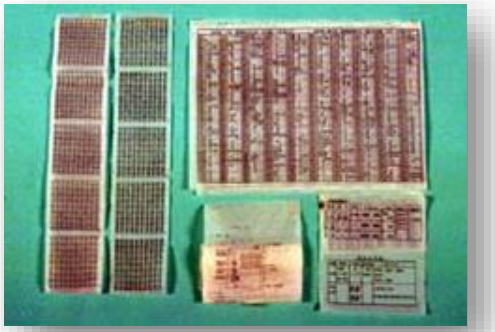
- **문제점**
  - **암호/복호 알고리즘이 널리 알려져 있음**
    - ✓ 덧셈, 뺄셈
  - **사용가능한 키의 수가 작고 한정적임**
    - ✓ 25개의 키
  - **평문의 내용이 인식가능함**
    - ✓ 영어
  - 따라서, brute-force 공격에 취약

Caesar Cipher(6)

- **키에 대한 Brute-Force 공격**
  - 성능이 뛰어난 컴퓨터를 이용한 키 계산 시간

키 크기 (bit)	가능한 키의 수	1 마이크로초(μs)당 1번의 암호화 실행	1 마이크로초 (μs) 당 10^6번의 암호화 실행
32	$2^{32}=4.3 \times 10^9$	2^{31} = 35.8 min.	2.15 ms
56	$2^{56}=7.2 \times 10^{16}$	2^{55} = 1142(Y)	10.01(H)
128	$2^{128}=3.4 \times 10^{38}$	$2^{127} = 5.4 \times 10^{24}$ (Y)	5.4×10^{18} (Y)
26문자	$26! = 4 \times 10^{26}$	6.4×10^{12}(Y)	6.4×10^6(Y)

Substitution(대체) 암호



- 예
  - 암호 알고리즘: **대체표**
  - 복호 알고리즘: **대체표**
  - 암호/복호 알고리즘(대체표)을 공개하지 않는 방식

평문 SELL 100 SHARES OF ABCD INDUSTRIES. JOHN SMITH.

대체표

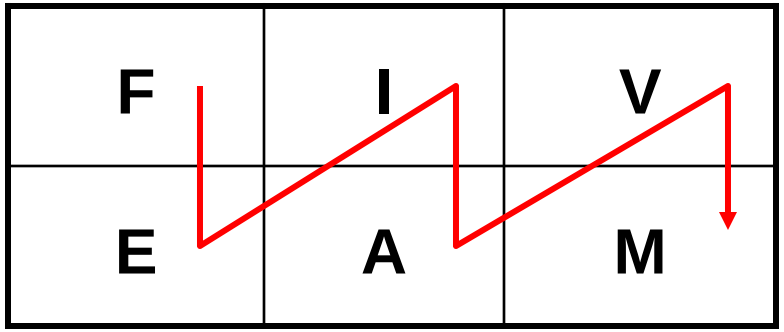
A	B	…	E	…	H	…	S	…	9	0	⌀	,	.
J	U	…	P	…	4	…	5	…	L	V	X	Z	1

암호문 5PEEXIVVX54JYP5X,2XJUTKXBCK95RYBP51XQ,4CX53BR41

Transposition(전치) 암호(1)

- Transposition
  - 전치(**轉置**, 위치를 바꿈)
  - 단순한 글자의 대체 대신 글자의 순서를 변경
- 예

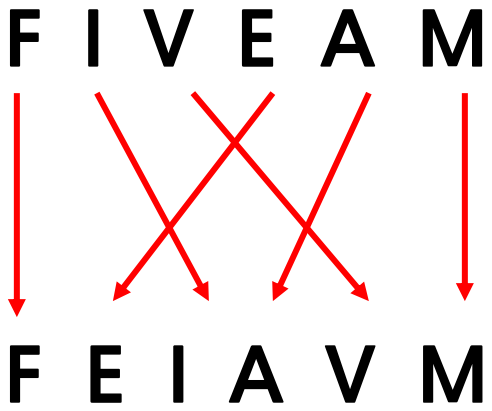
F I V E A M



F E I A V M

Transposition(전치) 암호(2)

- 예(계속)



F	I	V
E	A	M

1	2	3	4	5	6
1	3	5	2	4	6

암호 복호

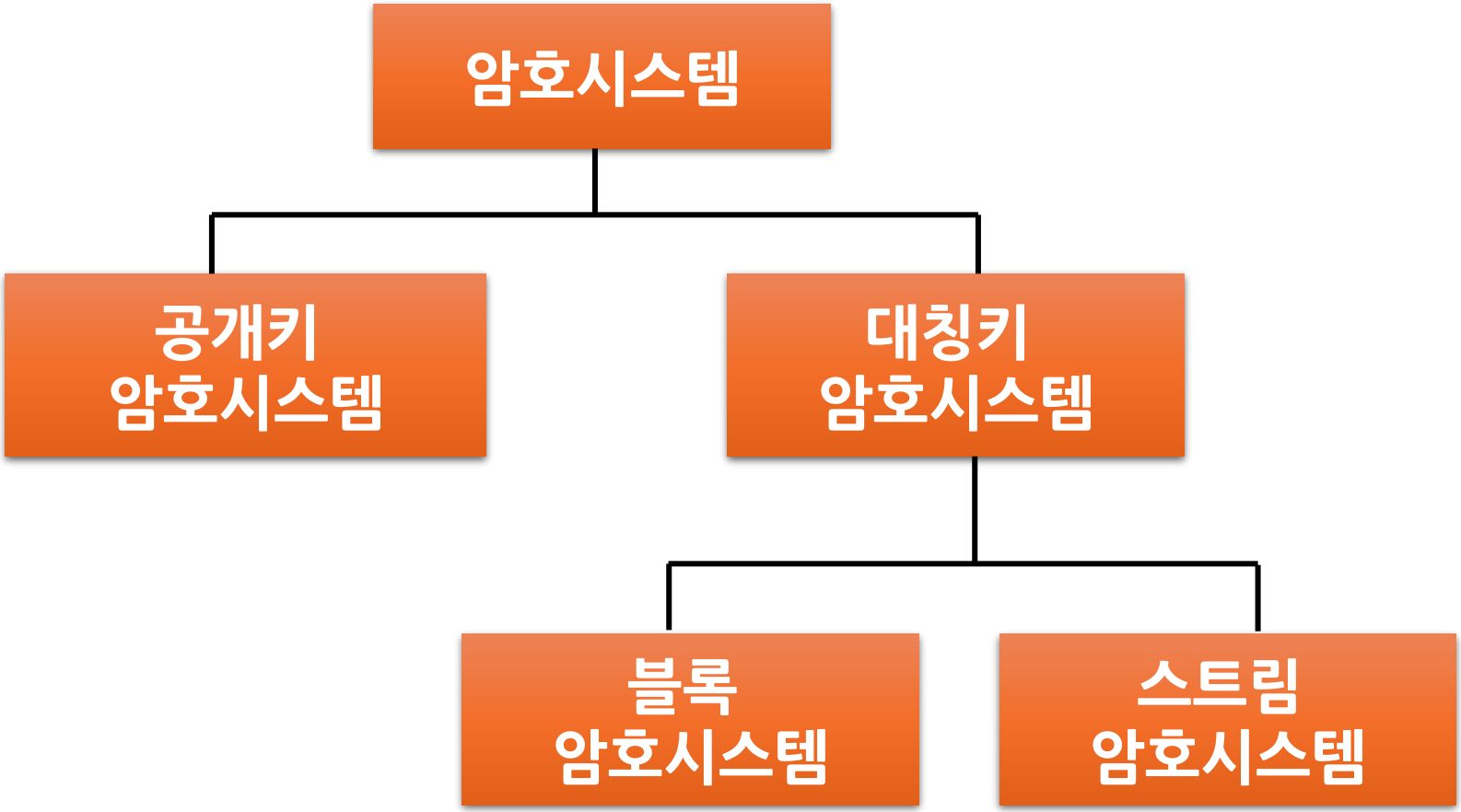
Diffusion 기법

- **Diffusion**
  - 확산, 흐림
- **암호화 과정**
  - Substitution 기법
  - Transposition 기법
- **목적**
  - **평문**과 **암호문**간의 **연관성을 쉽게 알지 못하도록**
  - 암호문으로부터 평문을 추론할 수 없도록

Confusion 기법

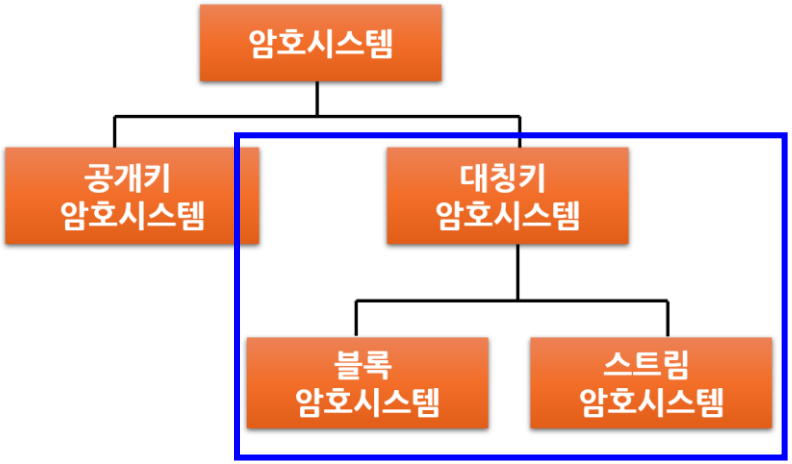
- **목적**
  - **암호문**과 **암호키**간의 **연관성이 없도록**
  - 암호분석가가 수집된 여러 개의 암호문을 분석하여 암호키를 추론해 낼 수 없도록 하는 성질

암호시스템 분류



대칭키 암호 시스템(1)

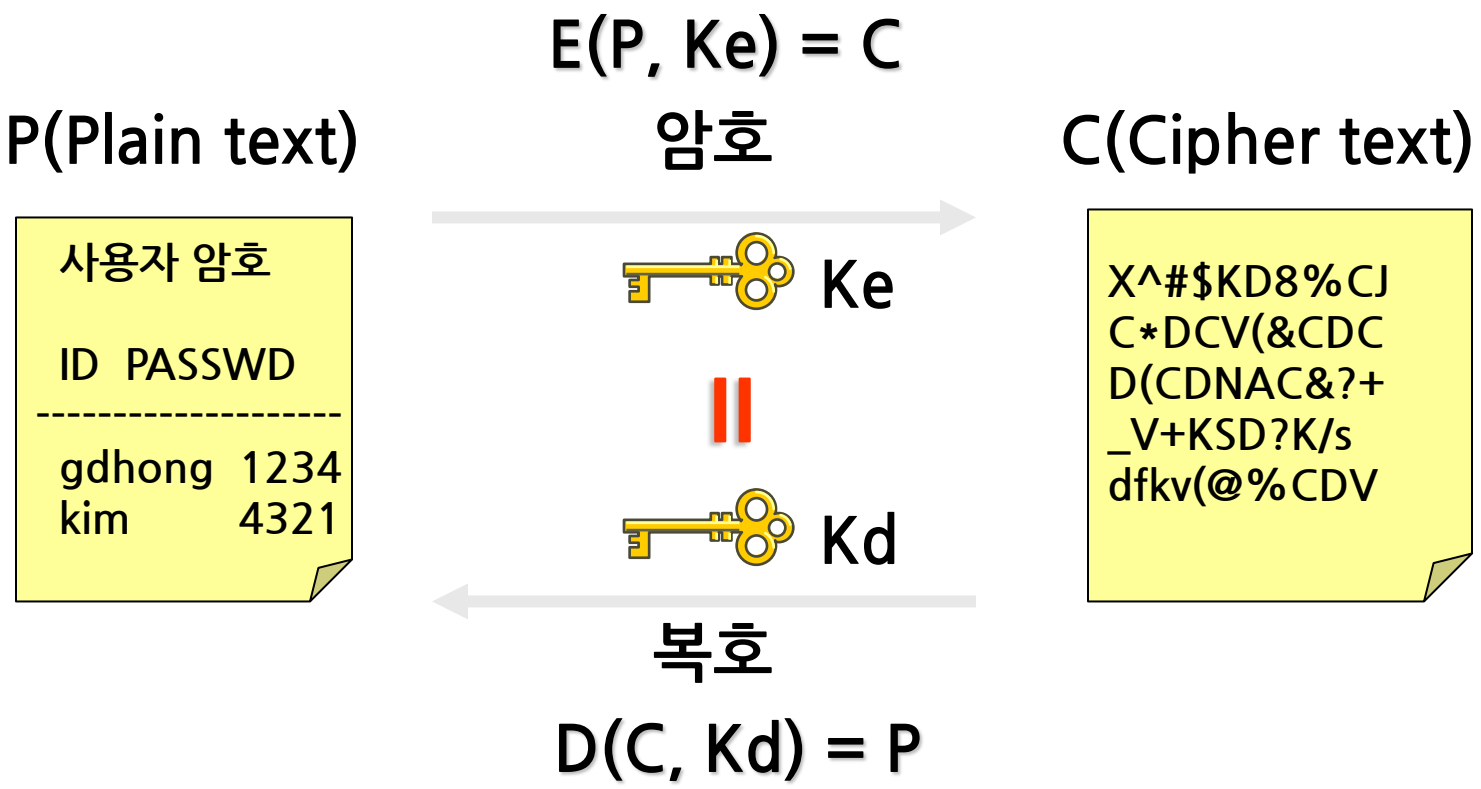
- Symmetric Cryptosystem
  - 비밀키 암호 시스템
  - 관용키 암호 시스템
- 특 징
  - 오랜 역사
  - 암호키와 복호키가 동일
  - 알고리즘의 동작속도가 빠름
  - 키의 길이가 공개키 암호 시스템에 비해 짧음



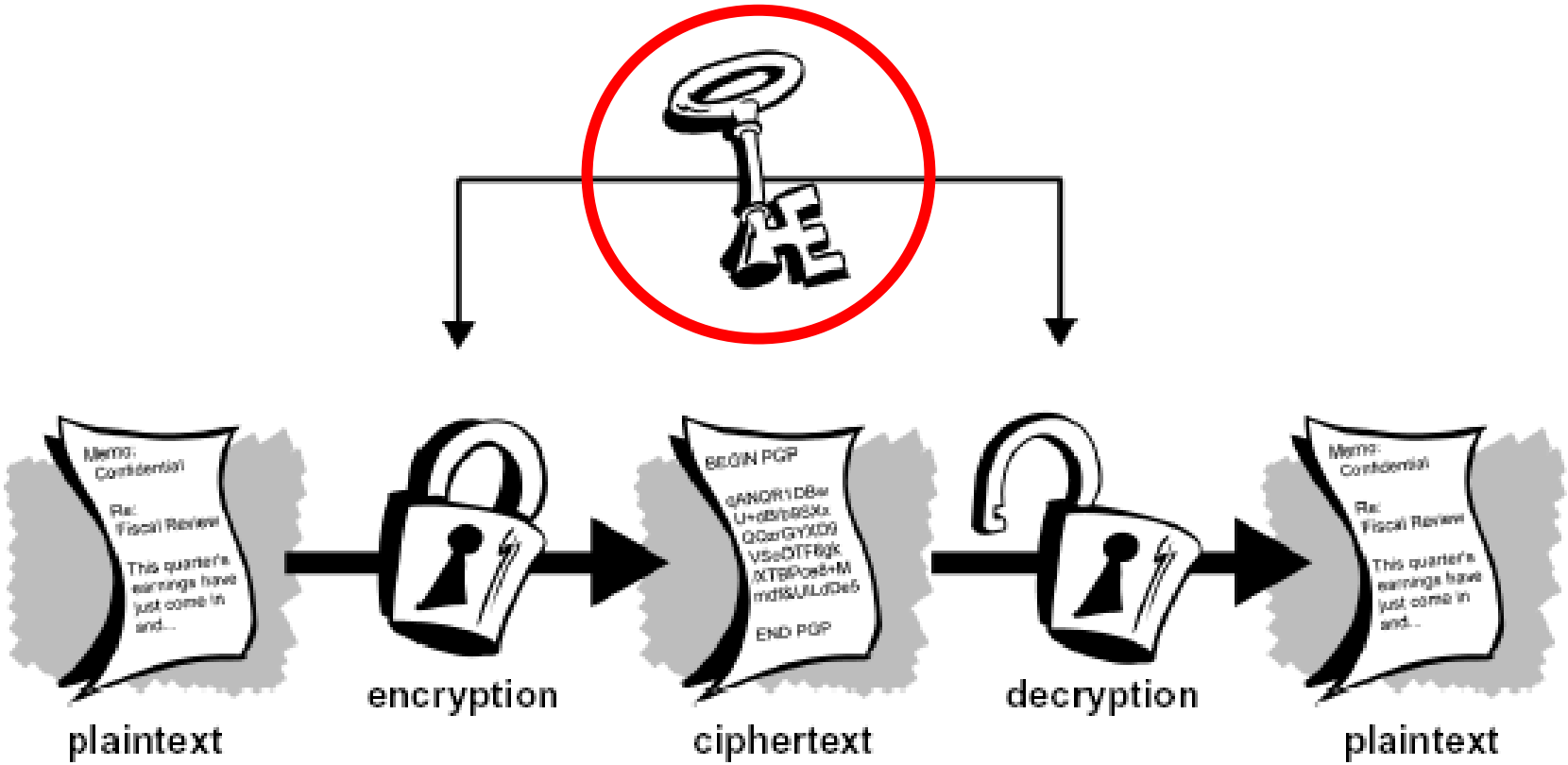
대칭키 암호 시스템(2)

- **표기법**
  - 암호 알고리즘: **E**, 암호키: **Ke**
  - 복호 알고리즘: **D**, 복호키: **Kd**
- **암호화 과정**
  - **E(P, Ke) = C**
- **복호화 과정**
  - **D(C, Kd) = P**

대칭키 암호 시스템(3)


E(P, Ke) = C
P(Plain text)
암호
C(Cipher text)
사용자 암호
ID PASSWD
gdhong 1234
kim 4321
Ke
=
Kd
X^#$KD8%CJ
C*DCV(&CDC
D(CDNAC&?+
_V+KSD?K/s
dfkv(@%CDV
복호
D(C, Kd) = P

대칭키 암호 시스템(4)

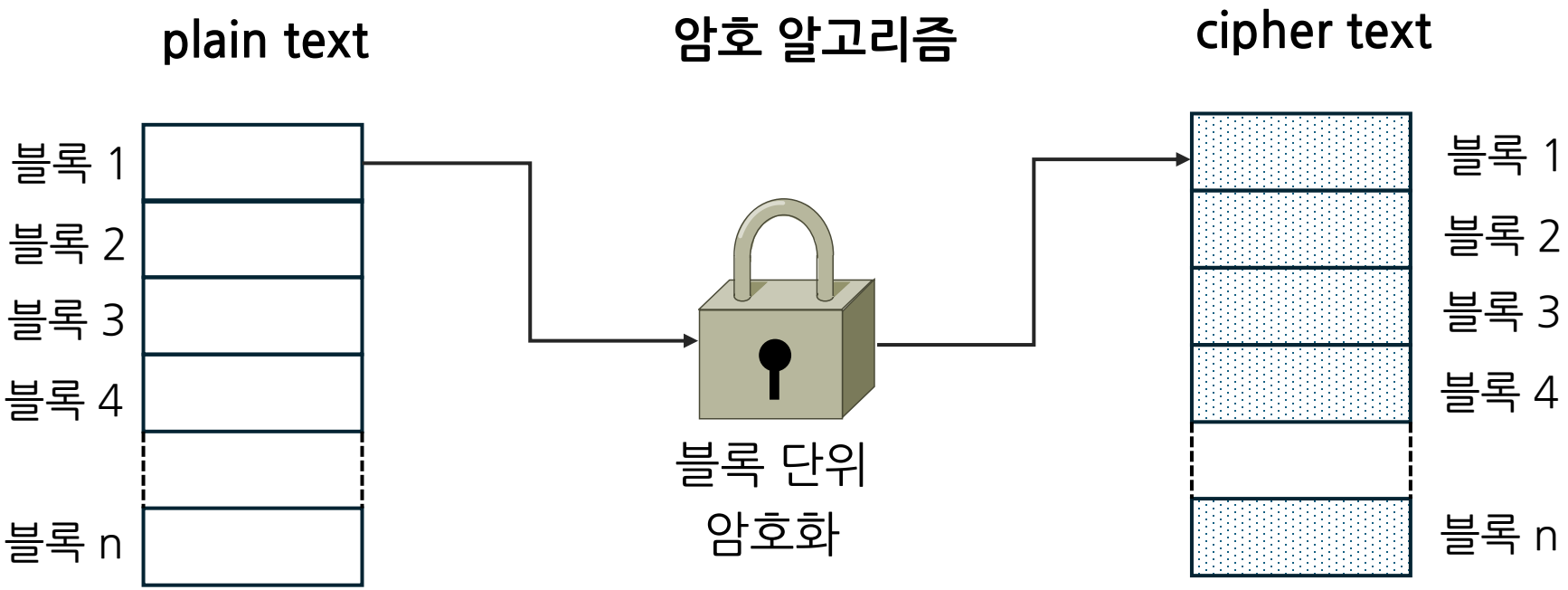

Memo:
Confidential
Re:
Fiscal Review
This quarter's
earnings have
just come in
and...
encryption
BEGIN PGP
qANQR1DBw
U+dBfbR9Xx
QOsrGYXD9
VSoDTF8gk
XTBPce8+M
mdf&URLdDe5
END PGP
decryption
Memo:
Confidential
Re:
Fiscal Review
This quarter's
earnings have
just come in
and...
plaintext
ciphertext
plaintext

대칭키 암호 시스템(5)

- **암호키 = 복호키**
- **암호키(복호키)는 메시지 송, 수신자만이 인지**
  - 메시지 수신자에게 복호키 전송 필요
  - 전송방법, 전송과정의 안전성 문제
  - **필연적**으로 **키 분배(key distribution) 문제 발생**
    - ✓ **키 분배 문제:** 안전하게 암호키(복호키)를 수신자에게 전달하는 문제
- **동작 속도가 빠름**

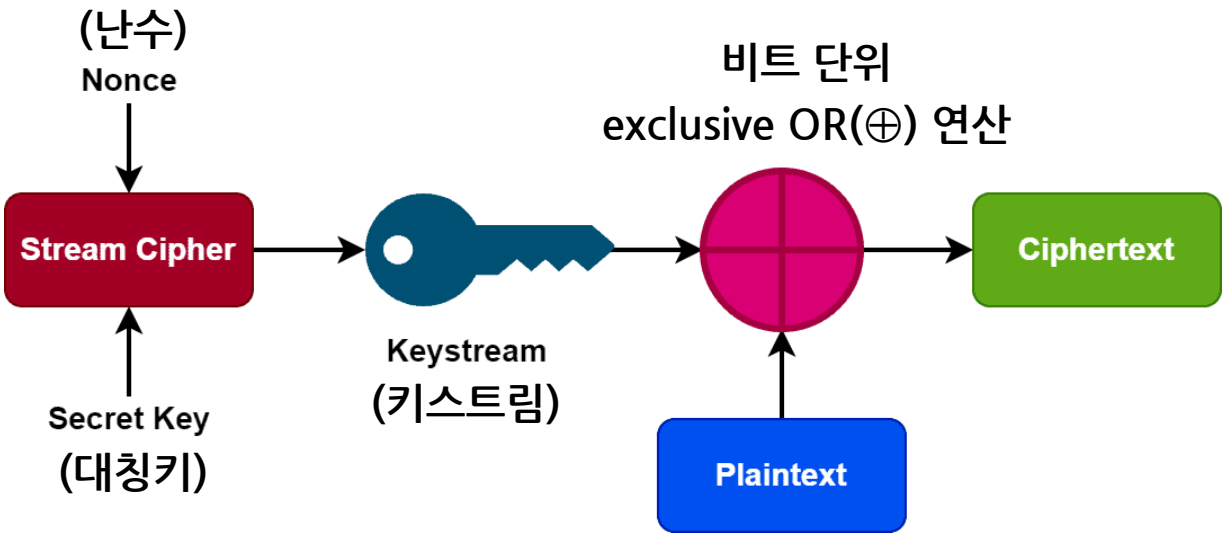
대칭키 암호 시스템(6) - 블록 암호

- 주어진 평문을 정해진 길이의 **블록**(64 혹은 128비트)으로 나누어 **블럭단위**로 암호화 수행
  - 대부분의 암호 알고리즘에서 채택



대칭키 암호 시스템(7) - 스트림 암호

- 평문과 같은 길이의 키 스트림(stream)을 생성
- 평문과 키 스트림를 비트단위로 합하여(Exclusive OR) 암호문을 얻는 알고리즘

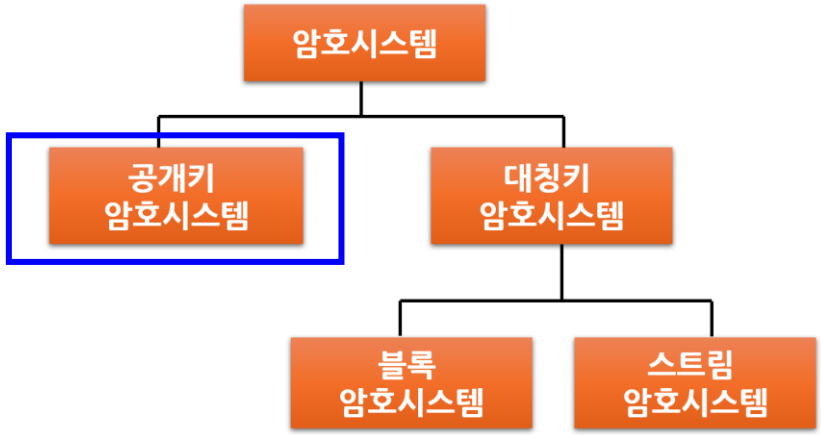


exclusive OR(⊕) 연산

Inputs		Output
A	B	X
0	0	0
0	1	1
1	0	1
1	1	0

공개키 암호 시스템(1)

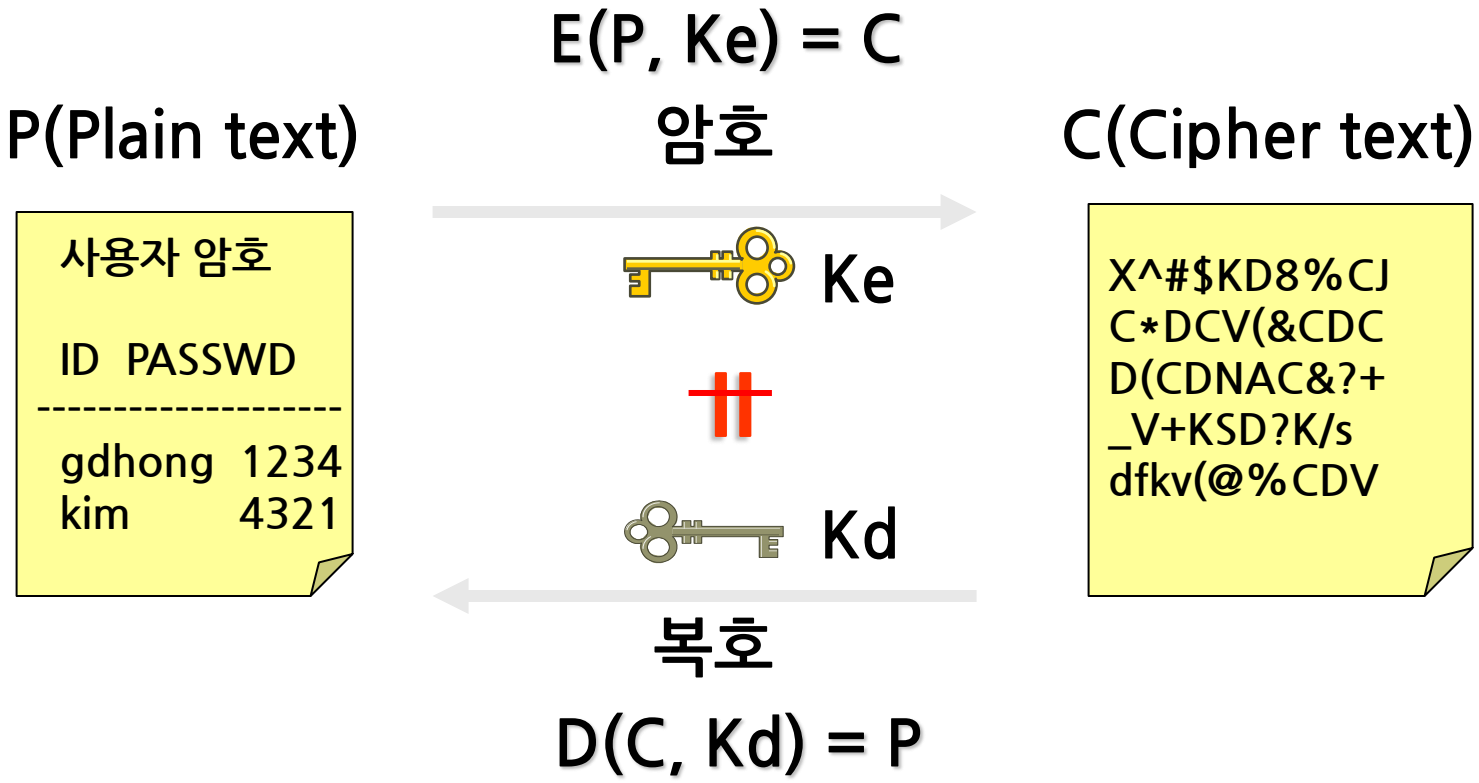
- Asymmetric Cryptosystem
  - 비대칭키 암호 시스템
- 특 징
  - 사용자당 2개의 키 소유
    - ✓ 개인키: 사용자가 안전하게 보관
    - ✓ 공개키: 일반에게 공개
  - 개인키와 공개키는 서로 다름
    - ✓ 공개키를 이용하여 개인키를 알아내기가 매우 어려움
  - 키의 길이가 대칭키 암호 시스템에 비해 긴 특징
  - 알고리즘의 동작속도가 느림



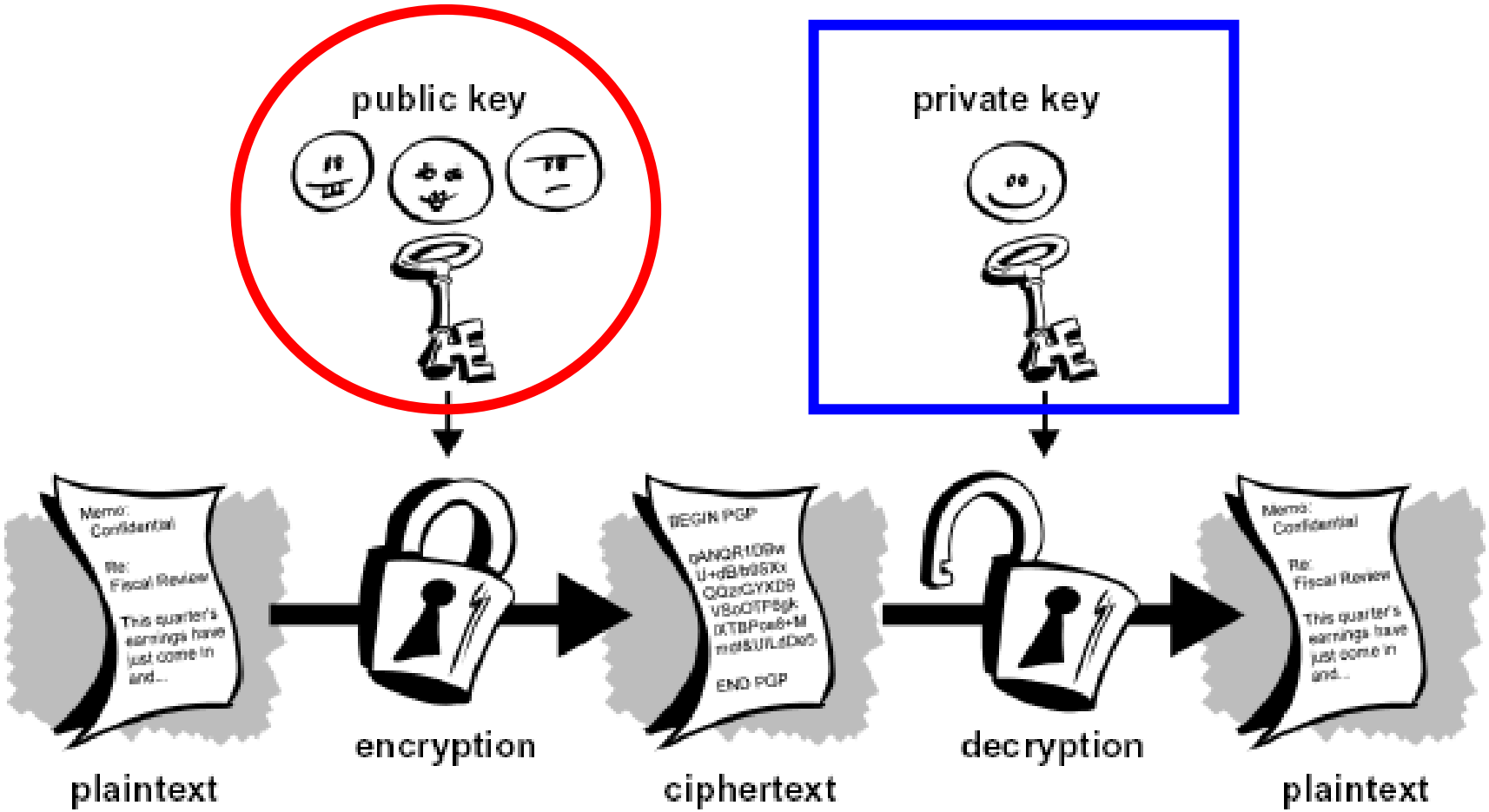
공개키 암호 시스템(2)

- **표기법**
  - 암호 알고리즘: **E**, 암호키: **Ke**
  - 복호 알고리즘: **D**, 복호키: **Kd**
- **암호화 과정**
  - **E(P, Ke) = C**
- **복호화 과정**
  - **D(C, Kd) = P**

공개키 암호 시스템(3)


E(P, Ke) = C
P(Plain text)
암호
C(Cipher text)
사용자 암호
ID PASSWD
gdhong 1234
kim 4321
Ke
≠
Kd
X^#$KD8%CJ
C*DCV(&CDC
D(CDNAC&?+
_V+KSD?K/s
dfkv(@%CDV
복호
D(C, Kd) = P

공개키 암호 시스템(4)


public key
private key
Memo:
Confidential
Re:
Fiscal Review
This quarter's earnings have just come in and...
encryption
BEGIN PGP
END PGP
decryption
plaintext
ciphertext
plaintext

공개키 암호 시스템(5)

- **특 징**
  - 한 사용자당 2개의 키(**공개키**, **개인키**) 소유
  - **개인키(private key), 비밀키(secret key)**
    - ✓ 사용자만이 알고 있는 키
    - ✓ 다른 사람에게 공개해서는 안되는 키
    - ✓ 개인키가 노출될 경우 심각한 보안 위협 발생
  - **공개키(public key)**
    - ✓ 다른 사람들에게 공개되는 키
  - **공개키에서 개인키를 추론해 내기는 거의 불가능**

공개키 암호 시스템(6)

- 동작 모드
  - 암호 모드(Encryption mode)
  - 인증 모드(Authentication mode)
- 암호 모드
  - 메시지의 내용을 메시지 수신자만 복원할 수 있도록
  - 메시지의 **비밀성 보호 목적**(confidentiality)
- 인증 모드
  - 메시지를 보낸 사람이 자신이 메시지를 보냈음을 확인
  - **메시지 출처 인증 목적**(data origin authentication)

공개키 암호 시스템(7)

- 암호 모드
  - **메시지 수신자의 공개키로 암호화**
  - **메시지 수신자의 개인키로만 복호화 가능**
  - 메시지 수신자만이 메시지 내용 복원(복호화) 가능
- 인증 모드
  - **메시지 발신자의 개인키로 암호화**
  - **메시지 수신자는 메시지 발신자의 공개키로 복호화**
  - 메시지 발신자의 공캐키로 내용이 복원되었다면
    메시지 발신자의 비밀키로 암호화되었음을 의미

공개키 암호 시스템(8)

- 암호 모드 - 지정된 수신자만이 복호화할 수 있도록

(상황) Alice가 Bob에게만 중요 문서(M)를 전달

Alice

$A_{개}$

$A_{공}$

Q1. 오직 Bob만이 복호화하도록 하는 복호키는 ?

Q2. 해당 복호키와 짝이 되는 암호키는?

Q3. Alice는 암호키를 어떻게 알아낼까? (키 분배 문제)

Q4. Charles는 암호문을 복호화할 수 있을까?

Bob

$B_{개}$

$B_{공}$

$C_{개}$

$C_{공}$

Charles

공개키 암호 시스템(9)

- 인증 모드 - 보낸 사용자가 누구인지 확인할 수 있도록

(상황) 중요 문서(M)를 Alice가 보낸 사실 증명 필요

Alice

$A_{개}$

$A_{공}$

Q1. 오직 Alice만이 알 수 있는 암호키?

Q2. 해당 암호키와 짝이 되는 복호키는?

Q3. Bob은 복호키를 어떻게 알아낼까? (키 분배 문제)

Q4. Charles는 암호문을 복호화할 수 있을까?

Bob

$B_{개}$

$B_{공}$

$C_{개}$

$C_{공}$

Charles

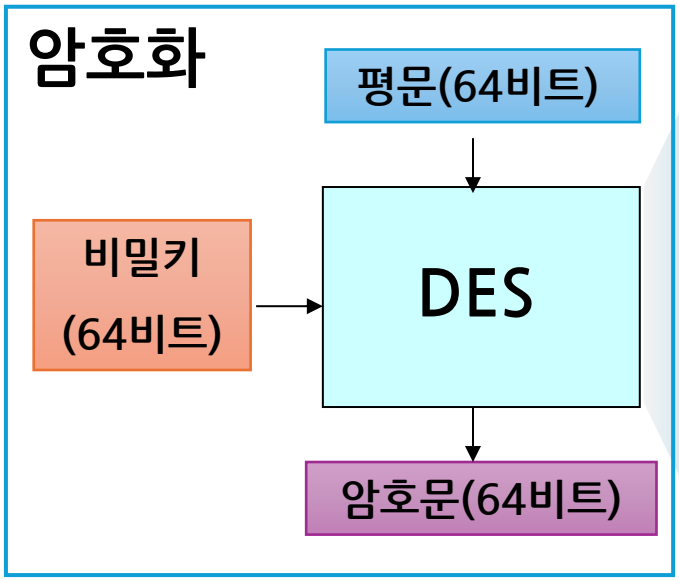
DES(Data Encryption Standard)(1)

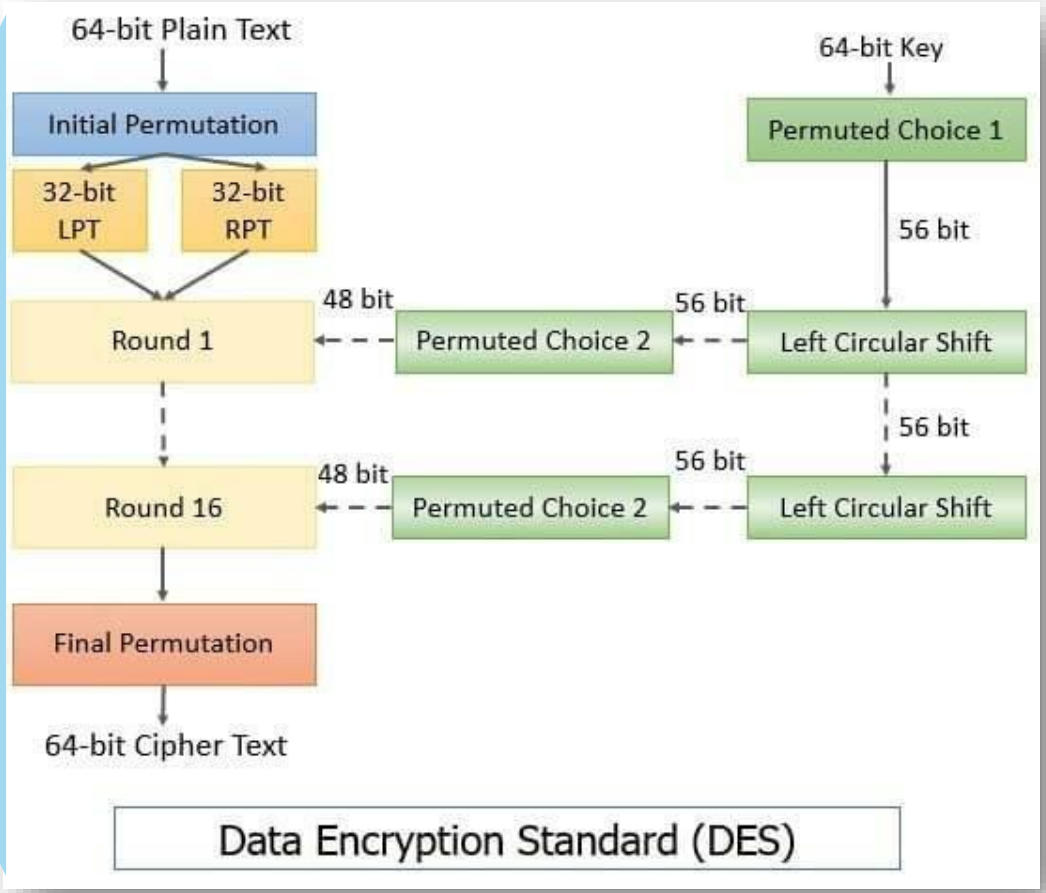
- **역 사**
  - 1972: 미국 NIST에 의해 표준 암호기술 개발 시작
  - 1977: DES를 표준 암호기술로 확정
- **특 징**
  - **56-bit** 길이의 암호 키 이용
    - ✓ 실제 암호 키의 길이 64-bit중 8-bit는 패리티로 사용
  - Feistel 방식의 **블록 암호 방식**
    - ✓ Substitution, transposition 기법 이용
  - IBM에서 제안한 Lucifer 시스템을 개량
    - ✓ 128-bit 길이의 암호 키

DES(Data Encryption Standard)(2)

- **문제점**
  - 56-bit 길이의 암호 키 채택과 trapdoor 존재에 대한 계속적인 논쟁
  - 1977년 이후 매 5년마다 DES 알고리즘에 대한 안전성 검토 절차 마련
    - ✓ 1982년, 1987년, 1992년
  - 1997년 DES의 후속 알고리즘 제안
    - ✓ AES(Advanced Encryption Standard)
  - 2000년 10월 Rijndael 암호 알고리즘을 DES 후속 암호 알고리즘으로 채택 (개발국: 벨기에)

DES(Data Encryption Standard)(3)





RSA(1)

- 1977년, MIT의 Rivest, Shamir, Adleman
- 소인수 분해의 어려움에 근거
- 시스템 구성
  - 공개키 : n(=p*q), e
  - 개안키 : n(=p*q), d
- 암호화 : $C = E(M) = M^e \pmod n$
- 복호화 : $M = D(E(M)) = (M^e)^d \bmod n = M$

RSA(2)

- **Encryption Speed**
  - 대칭키 암호시스템보다 상당히 느린 동작 속도 특징
- **키 크기**
  - 안전한 키 최소 길이 - 1024-bit
  - 키의 길이는 256-bit 배수로 증가
  - 현재 안전한 키 길이로 2048-bit 권장

RSA(3)

- **RSA 알고리즘 정리**
  - 키 생성
    - ✓ p, q 선택 (p, q는 솟수), n = p × q 계산
    - ✓ $\phi(n) = (p-1) \times (q-1)$ 계산
    - ✓ 정수 e 선택 ($\gcd(\phi(n),d) = 1$, $1 < d < \phi(n)$) (e와 $\phi(n)$ 서로 소)
    - ✓ d 계산 ($e \times d \mod \phi(n) = 1$ 관계 성립)
    - ✓ 공개키 (KU = {e, n})
    - ✓ 개인키 (KR = {d, n})
  - 암호화
    - ✓ $C = M^e \pmod n$
  - 복호화
    - ✓ $M = C^d \pmod n$

RSA(4)

- **RSA 알고리즘 사용 예**
  - 공개키와 개인키 생성

    1. 두 소수 p = 7, q = 17 을 선택
    2. n = pq = 7 × 17 = 119 계산
    3. ϕ(n) = (p-1) ×(q-1) = 96 계산
    4. ϕ(n) = 96과 서로 소이고 ϕ(n)보다 작은 e 선택 (e = 5)
    5. d × e mod 96 = 1 이고 d < 96 인 d를 결정 (d = 77)

    ⇒ 공개키 KU = {5, 119}, 개인키 KR = {77, 119}

RSA(5)

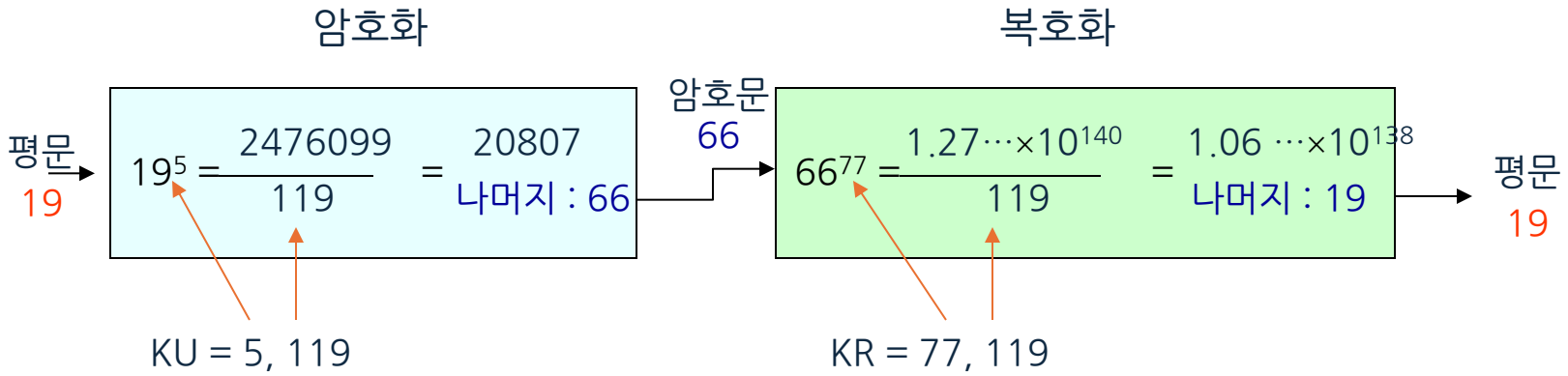
RSA 알고리즘 사용 예(계속)

- 암호화와 복호화

  : 평문 메시지 M = 19 일 경우

  - ✓ 암호문 : $19^5 \bmod 119 \Rightarrow 66$
  - ✓ 복호문 : $66^{77} \bmod 119 \Rightarrow 19$

- 공개키 KU = {5, 119}
- 개인키 KR = {77, 119}



대칭키, 공개키 암호 시스템 비교(1)

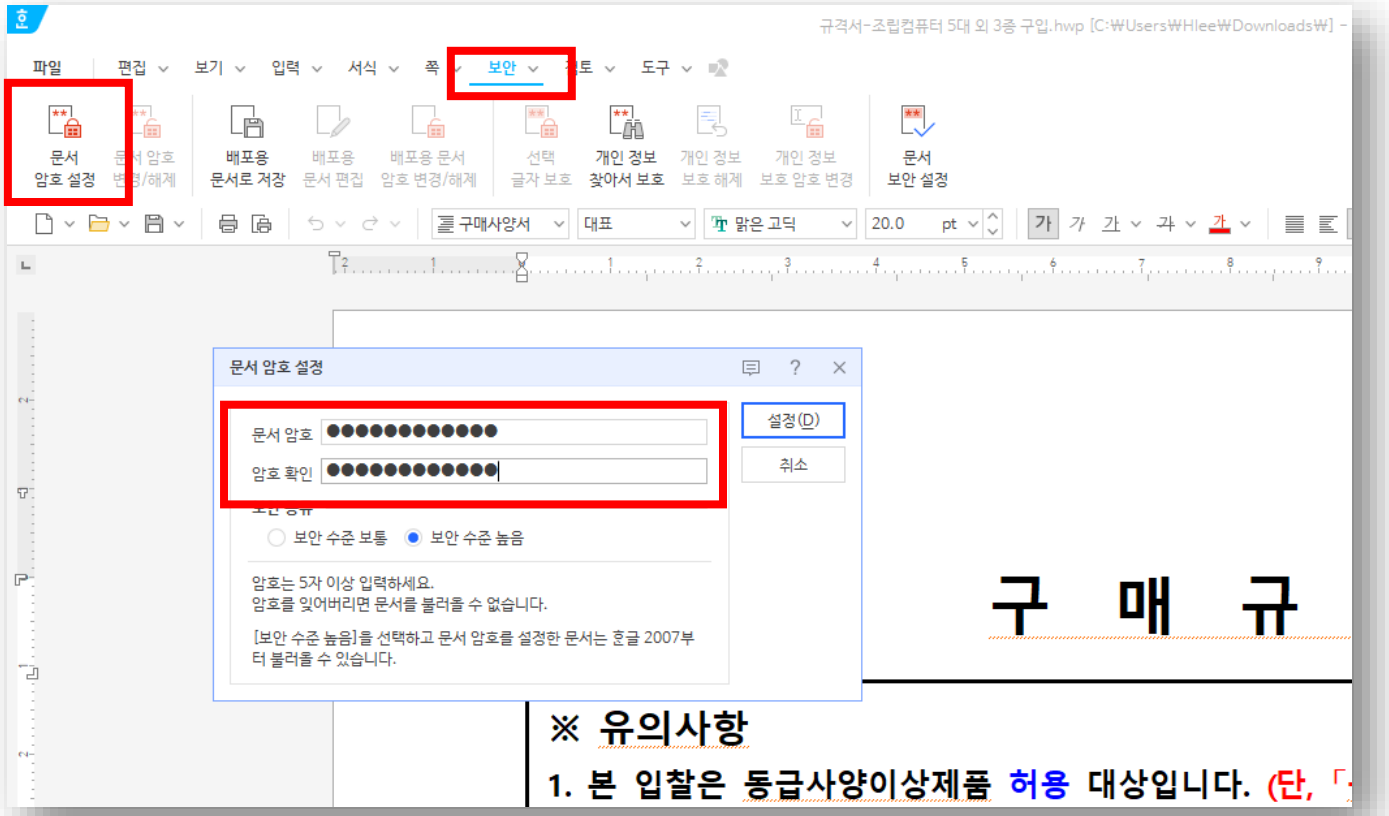
	대칭키 암호시스템	공개키 암호시스템
키의 상호관계	암호키 = 복호키	암호키 ≠복호키
암호키	대칭키	공개키 또는 개인키
복호키	대칭키	공개키 또는 개인키
대표적 예	DES/RC4/SEED/ARIA	RSA/DH/DSS/ECC
암호키 전송	필요	불필요
키 개수	n(n-1)/2	2n
안전한 인증	곤란	용이
암호화 속도	고속	저속
경제성	높음	낮음
전자서명 활용	복잡	간단

대칭키, 공개키 암호 시스템 비교(2)

- **SEED**
  - 1999년 한국인터넷진흥원(KISA) 개발 대칭키 암호 알고리즘
  - DES 암호화 방식 채택
  - 국제 표준 등재 (암호키 길이 128-bit 버전)
- **ARIA(Academy, Research Institute, Agency)**
  - 2003년 학계, 연구소, 정부기관 공동 개발
  - 경량 환경 및 하드웨어 구현 목적
  - 키 길이: 128/192/256비트
  - 국내 개발 보안 소프트웨어에 의무 사용

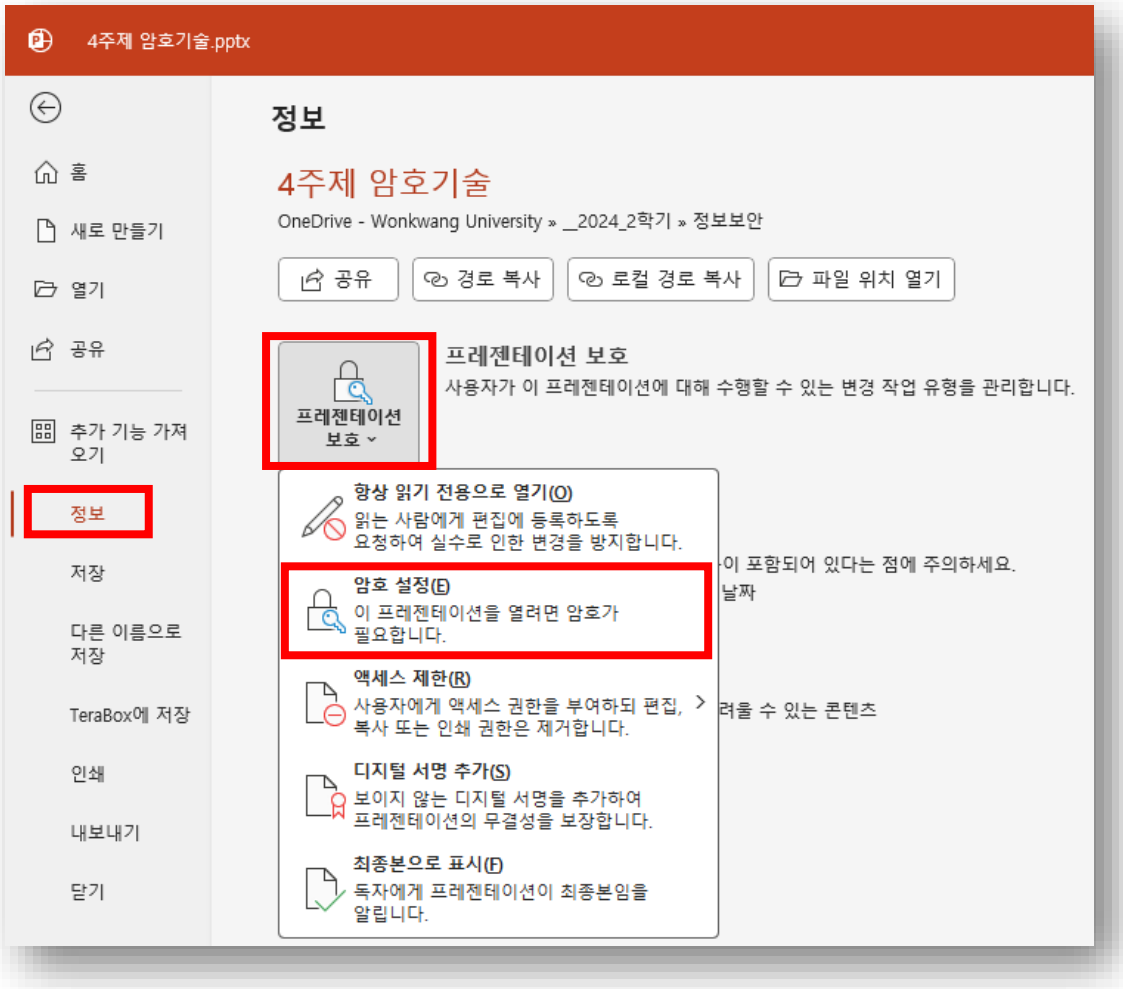
암호 사용 사례(1)

- 한글 워드프로세서 (ARIA 암호 알고리즘 사용)
  - [보안] - [문서 암호 설정]



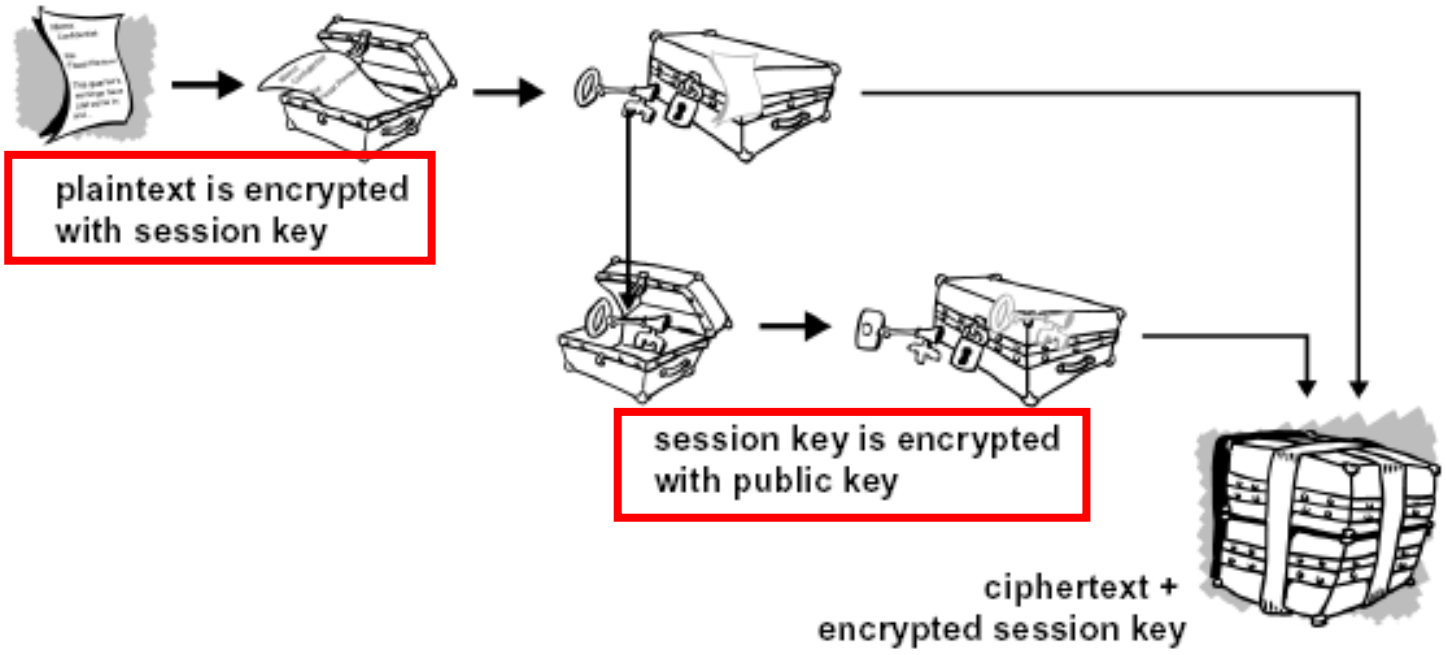
암호 사용 사례(2)

- MS Powerpoint
  - [파일] - [정보] - [프레젠테이션 보호] - [암호 설정]



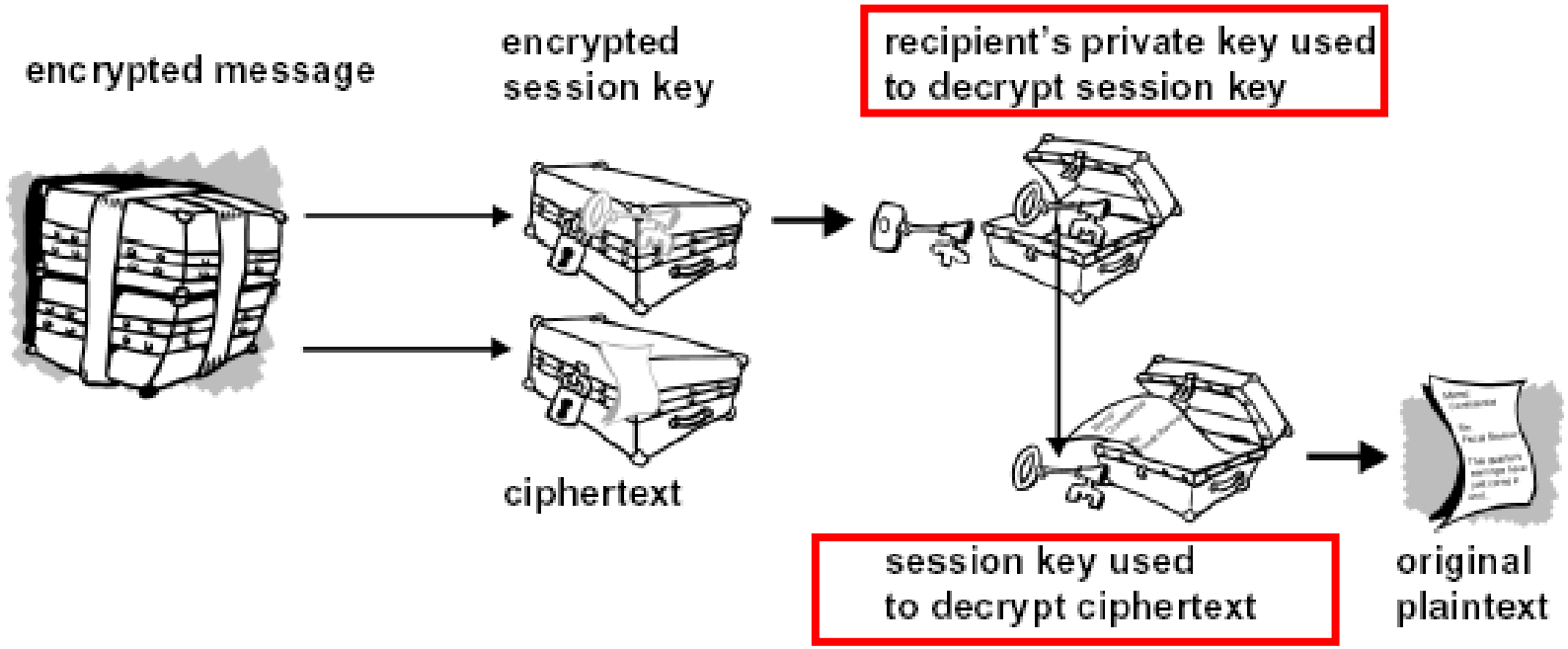
대칭키, 공개키 암호 시스템 활용 사례(1)

- **송신측(암호화 과정)**
  - 대칭키 암호시스템 - 평문 암호용 (빠른 동작 속도)
  - 공개키 암호시스템 - 세션키 암호용 (키 교환 문제 해결)



대칭키, 공개키 암호 시스템 활용 사례(2)

- **수신측(복호화 과정)**
  - 대칭키 암호시스템 - 암호문 복호용 (빠른 동작 속도)
  - 공개키 암호시스템 - 세션키 복호용 (키 교환 문제 해결)



기타 공개키 암호 시스템(1)

- DH
  - Diffie-Hellman
- ECC
  - Elliptic Curve Encryption
- DSS
  - Digital Signature Standard

기타 공개키 암호 시스템(2)

- **DH(Diffie-Hellman)**
  - 1976년 Diffie, Hellman에 의해 개발
  - **대칭키의 안전한 교환 절차** 정의
  - 메시지 암호화 기능 없음
  - 전자서명 기능 없음

기타 공개키 암호 시스템(3)

- **ECC(Elliptic Curve Cryptosystem)**
  - 1985년 Neil Koblitz, Victor Miller에 의해 개발
  - RSA나 DSA에 비해 보안성 우수
    - ✓ 10^{12} MIPS year의 경우
    - ✓ RSA, DSA: 1024 비트 요구
    - ✓ ECC: 160 비트 요구
  - 메시지 암호 기능 제공
  - 전자서명 기능 제공

기타 공개키 암호 시스템(4)

- **DSS(Digital Signature Standard)**
  - 1987년 미국의 NIST에 의해 제안
  - **전자서명** 목적의 공개키 암호 알고리즘
    - ✓ 전자문서 작성자의 신원 확인(authentication)
    - ✓ 전자문서의 변경여부 확인(integrity)
  - 메시지의 암호화 기능 없음
  - 키 교환 기능 없음