제3장. 공개키 암호와 메시지 인증

3.4 공개키 암호 원리

공개키 암호 구조

- 1976년에 Diffie 와 Hellman 에 의해 최초로 제안
- 수학적 함수에 근거
- 서로 다른 두 개의 키를 이용하는 비대칭 방식
- 기밀성, 키 분배, 인증에서 뛰어난 성능

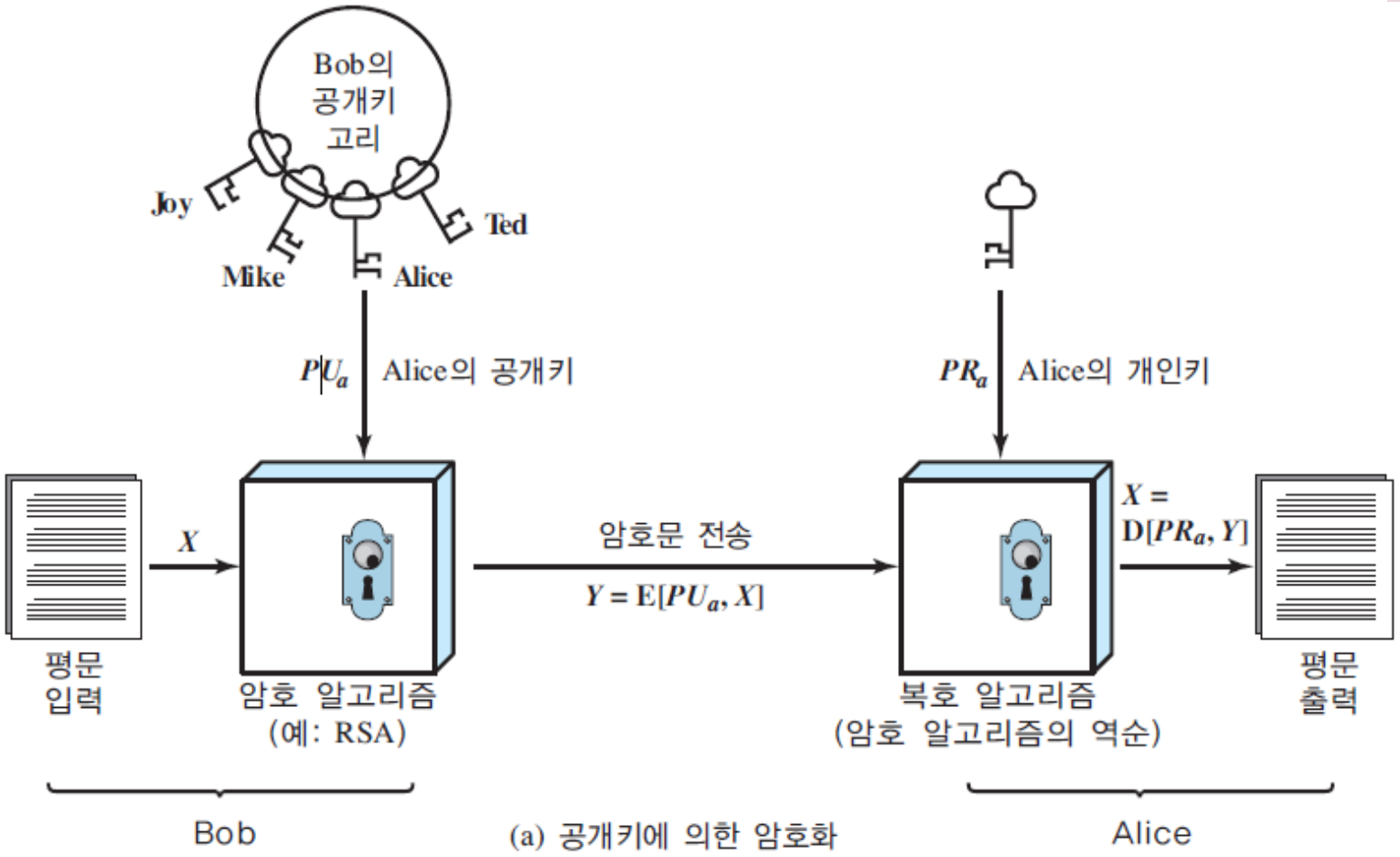
공개키 암호에 대한 오해

- 공개키 암호가 관용 암호보다 암호해독에 있어서 더 안전하다(X)
- 공개키 암호 기술이 일반화 되어 관용 암호를 더 이상 사용하지 않게 된다(X)
- 관용 암호의 키 분배보다 공개키를 사용하는 키 분배가 더 쉽다(X)

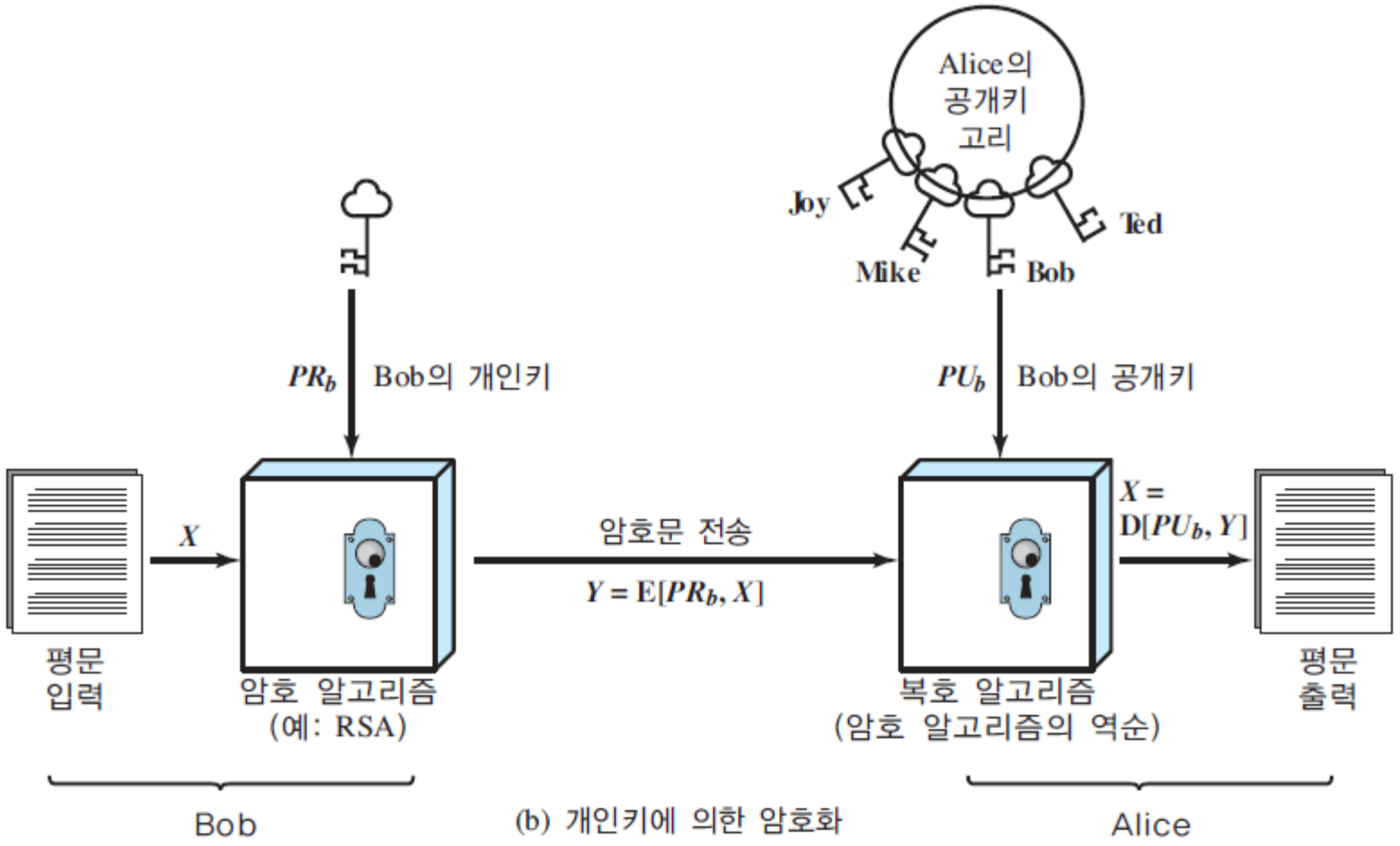
공개키 암호 핵심 요소

- 평문(Plaintext):
- 암호 알고리즘(Encryption algorithm):
- 공개키와 개인키(Public and private key):
- 암호문(Ciphertext):
- 복호 알고리즘(Decryption algorithm):

공개키로 암호화하기


Bob의
공개키
고리
Joy
Ted
Mike
Alice
PU_a
Alice의 공개키
PR_a
Alice의 개인키
X
암호문 전송
$Y = E[PU_a, X]$
$X = D[PR_a, Y]$
평문
입력
암호 알고리즘
(예: RSA)
복호 알고리즘
(암호 알고리즘의 역순)
평문
출력
Bob
(a) 공개키에 의한 암호화
Alice

개인키로 암호화하기



(b) 개인키에 의한 암호화

공개키 암호의 특성

- 한 쌍의 키 필요
  - 하나는 메시지 암호화에 사용하고 다른 하나는 복호화에 사용
- 공개키를 등록
  - 공개키와 한 쌍을 이루는 키는 개인키
- 메시지 암호화는 수신자 공개키로 암호화
- 암호문은 수신자의 개인키로 복호화

키 명칭

- 대칭암호(관용암호)
  - 비밀키(secret key)
- 공개키암호(비대칭 암호)
  - 공개키(public key)
  - 개인키(private key)

공개키 암호시스템 응용

알고리즘	암호/복호	디지털 서명	키 교환
RSA	Yes	Yes	Yes
Diffie-Hellman	No	No	Yes
DSS	No	Yes	No
타원 곡선	Yes	Yes	Yes

공개키 암호의 응용

- 암호화/복호화(Encryption/decryption):
  - 수신자의 공개키로 메시지 암호화
- 디지털 서명(Digital signature):
  - 송신자 자신의 개인키로 메시지 암호화(서명).
- 키 교환(Key exchange):
  - 세션 키를 교환(공유)한다

공개키 암호 요건

1. B가 한 쌍의 키(공개키: PU_b, 개인키: PR_b)를 생성하는 것은 계산적으로 쉬워야 한다.
2. 공개키와 평문 M을 알고 있는 송신자 A는 암호문을 계산적으로 쉽게 구할 수 있어야 한다.

$$C = E(PU_b, M)$$

3. 수신자 B가 암호문을 자신의 개인키를 이용해서 원문으로 복호화 하는 것이 계산적으로 쉬워야 한다.

$$M = D(PR_b, C) = D[PR_b, E(PU_b, M)]$$

4. 공개키 PU_b를 알고 있는 공격자가 개인키 PR_b를 알아내는 것이 계산적으로 불가능해야 한다.
5. 공개키 PU_b와 암호문 C를 알고 있는 공격자가 원문 M을 알아내는 것은 계산적으로 불가능해야 한다.

공개키 암호 요건

- 이 조건은 반드시 필요한 것은 아니다
- 2개의 키 중 어느 하나를 암호화에 사용하면 다른 하나는 복호화에 사용할 수 있다.

$$M = D\left[Pu_b, E(PR_b, M)\right]$$
$$= D\left[PR_b, E(Pu_b, M)\right]$$