9장. 공개키 암호와 RSA

박 종 혁

(jhpark1@snut.ackr)

http://www.parkjonghyuk.net

❑ 목 차

공개키 암호 시스템의 원리

❑ 공개키 암호 시스템의 원리

❖ 공개키 암호 시스템의 특징

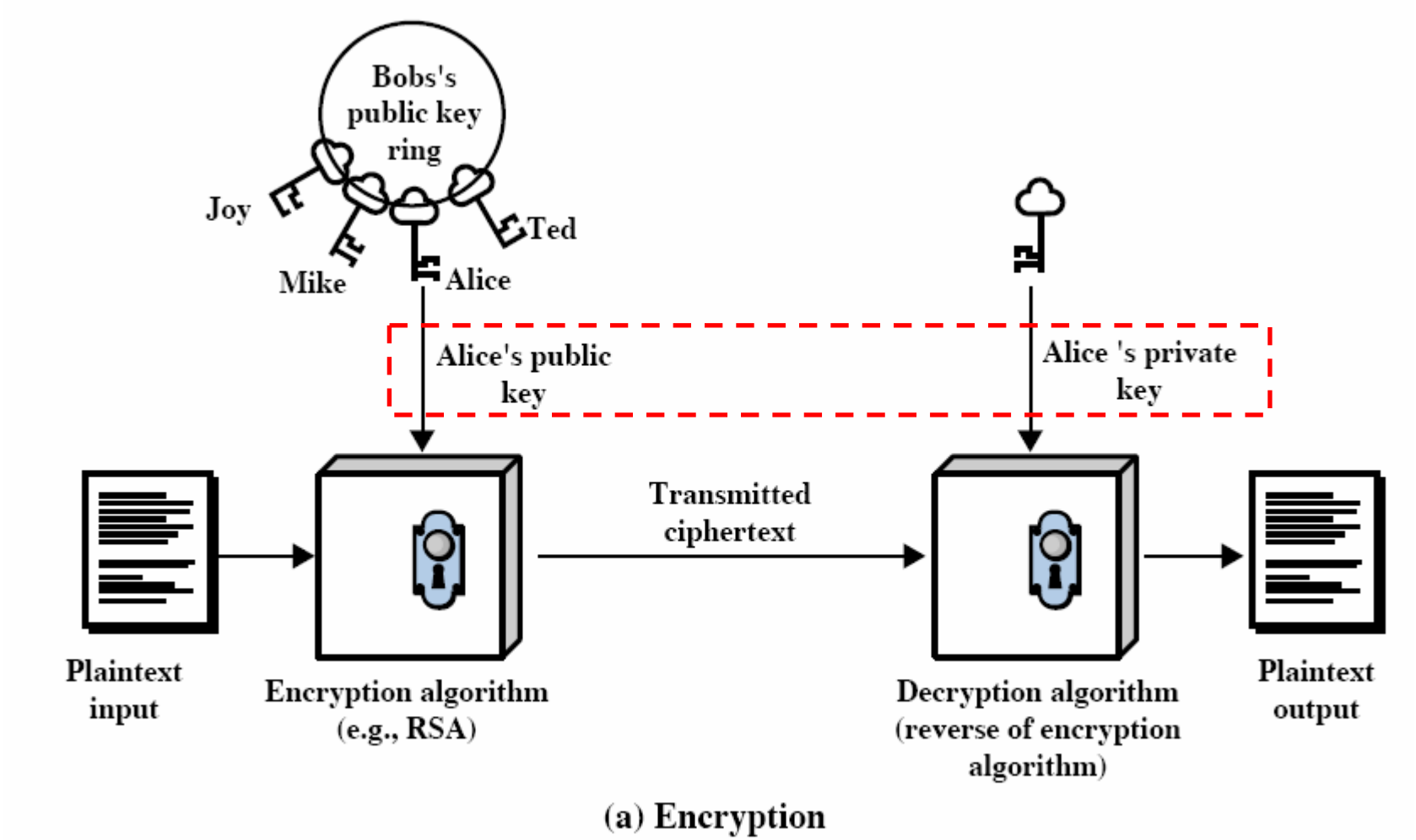
- ➢ 주어진 암호 알고리즘과 암호키를 알고 있더라도 복호키를 결정하는 것은 계산적으로 실행 불가능
- ➢ 두 개의 관련된 키에서 하나는 암호에 사용될 수 있고, 나머지는 복호에 사용됨

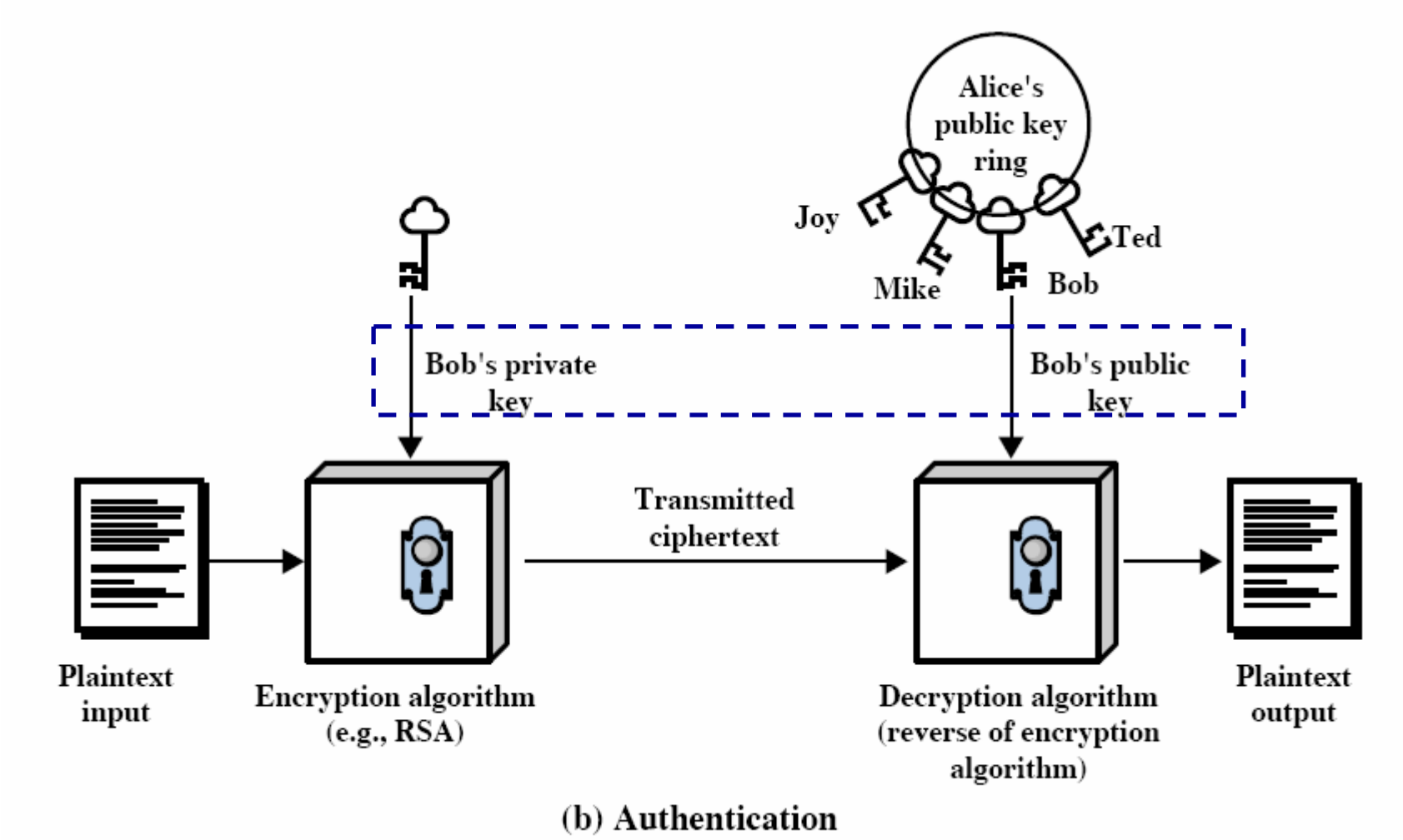
❖ 공개키 암호 구조의 구성 요소

- ➢ 평문 : 읽을 수 있는 평문 메시지 또는 데이터
- ➢ 암호 알고리즘 : 평문에 대하여 다양한 변형을 수행
- ➢ 공개키와 개인키 : 하나는 암호화를 위하여 사용되고 다른 하나는 복호화를 위하여 사용되도록 선택된 키의 쌍
- ➢ 암호문 : 출력으로써 변형된 메시지, 평문과 키에 의존적이며 주어진 하나의 메시지에 대하여 2개의 다른 키는 2개의 다른 암호문을 생성
- ➢ 복호 알고리즘 : 암호문과 대응하는 키를 받아서 본래의 평문을 생성

❑ 공개키의 처리 단계

1. 각 사용자는 메시지의 암호화와 복호화에 사용하기 위한 키 쌍을 생성
2. 각 사용자는 공개된 등록처나 또는 접근 가능한 파일에서 2개의 키 중에 하나를 설치(공개키), 대응되는 키는 비밀로 유지
3. 봅이 앨리스에게 비밀 메시지를 보내기 원하다면, 봅은 앨리스의 공개키를 사용하여 메시지를 암호화함
4. 앨리스가 메시지를 받았을 때, 앨리스는 자신의 개인키를 사용하여 복호화 함, 앨리스만의 개인키를 알기 때문에 다른 수신자는 메시지를 복호화할 수 없음


Bobs's public key ring
Joy
Ted
Mike
Alice
Alice's public key
Alice 's private key
Plaintext input
Encryption algorithm (e.g., RSA)
Transmitted ciphertext
Decryption algorithm (reverse of encryption algorithm)
Plaintext output
(a) Encryption



(b) Authentication

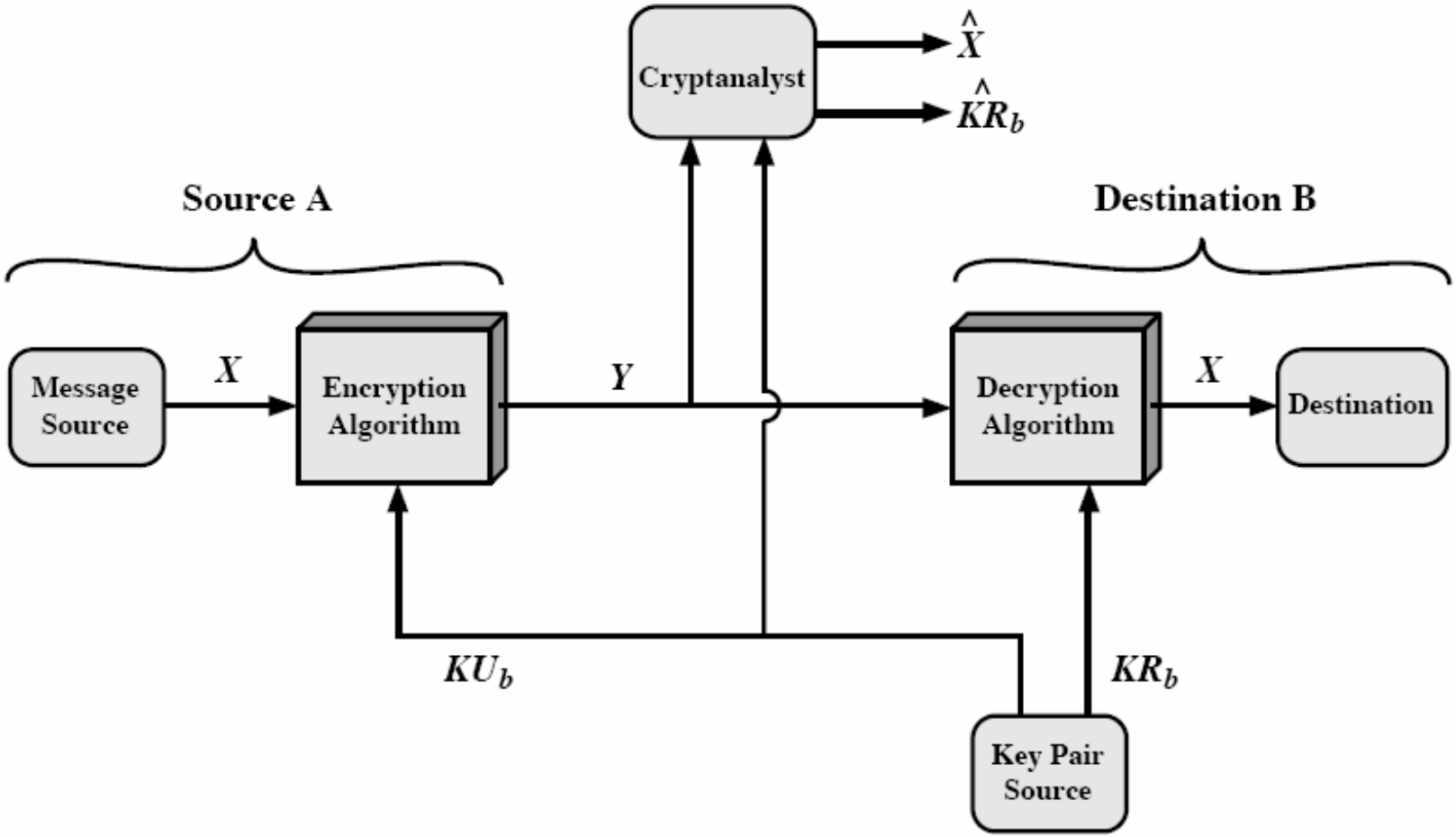
Chapter 9 공개키 암호와 RSA

❑ 관용 암호와 공개키 암호

관 용 암 호	공 개 키 암 호
작업을 위한 요구 사항 1.같은 키를 가지는 같은 알고리즘이 암호와 복호에 사용된다. 2.송신자와 수신자는 알고리즘과 키를 분배해야만 한다.	작업을 위한 요구 사항 1.하나의 알고리즘은 암호와 복호를 위한 키 쌍으로 암호와 복호에 사용된다. 2.송신자와 수신자는 대응되는(동일한 것이 아닌) 키의 쌍을 각각 가져야 한다.
안전성을 위한 요구 사항 1.키는 비밀로 유지되어야 한다. 2.만약 다른 정보가 이용되지 않는다면 메시지를 해독하는 것이 불가능하거나 적어도 비실용적이어야 한다. 3.알고리즘과 암호문 샘플의 지식이 키를 결정하지 못해야 한다.	안전성을 위한 요구사항 1.두 개의 키 중에서 하나는 비밀로 유지되어야 한다. 2.만약 다른 정보가 이용되지 않는다면 메시지를 해독하는 것이 불가능하거나 적어도 비실용적이어야 한다. 3.알고리즘과 하나의 키와 암호문 샘플의 지식이 키를 결정하지 못해야 한다.

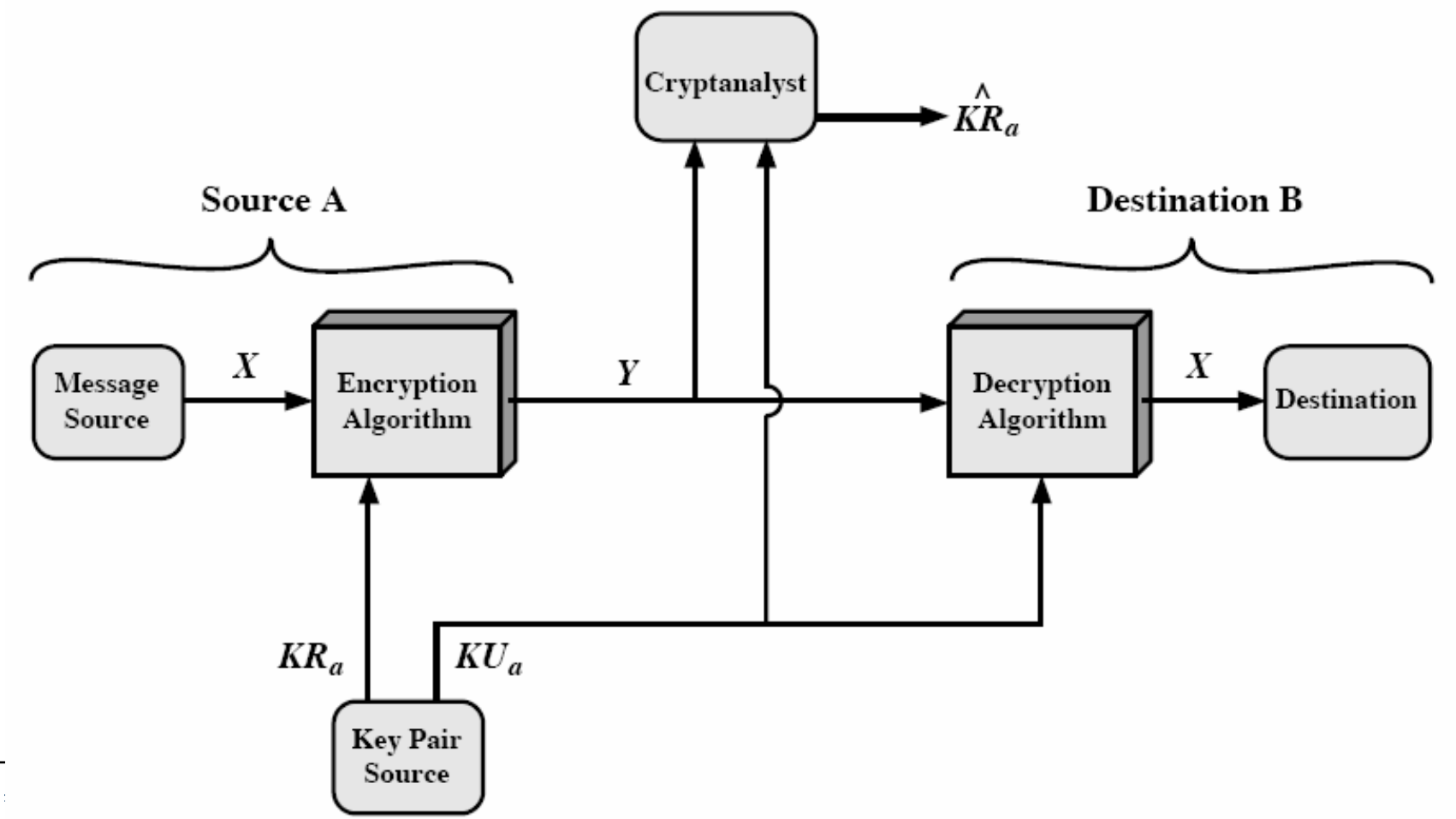
❑ 공개키 암호 시스템 : 기밀성

❖ X : 평문, Y : 암호문, KU_b: b의 공개키, KR_b: b의 개인키



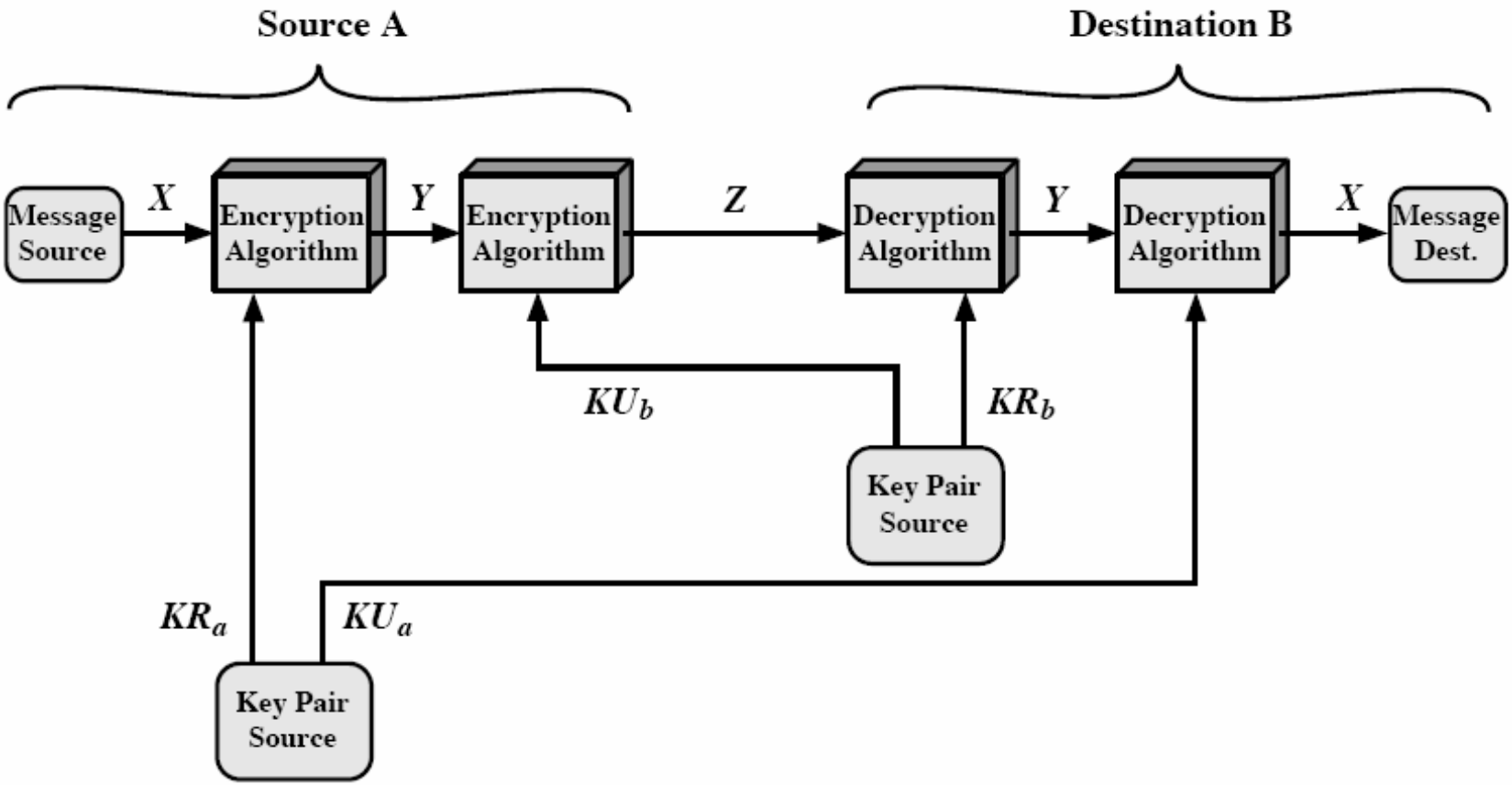
❑ 공개키 암호 시스템 : 인증

❖ X : 평문, Y : 암호문, KU_a: a의 공개키, KR_a: a의 개인키



❑ 공개키 암호 시스템 : 기밀과 인증

- ❖ X : 평문, Y : 암호문(인증), Z : 암호문(인증 + 기밀)
- ❖ KU_a: a의 공개키, KR_a: a의 개인키
- ❖ KU_b: b의 공개키, KR_b: b의 개인키



❑ 공개키 암호 시스템의 응용

- ❖ 암호/복호(Encryption/decryption)
  - ➢ 송신자는 수신자의 공개키로 메시지를 암호화 함
- ❖ 디지털 서명(Digital signature)
  - ➢ 송신자는 개인키로 메시지에 서명 함
- ❖ 키 교환(Key exchange)
  - ➢ 양쪽은 세션키를 교환하기 위하여 상호 협력 함

알고리즘	암호화/복호화	디지털 서명	키 교환
RSA	가능	가능	가능
타원 곡선	가능	가능	가능
Diffie-Hellman 키 교환	불가능	불가능	가능
DSS (전자 서명 표준)	불가능	가능	불가능

RSA 알고리즘

❑ RSA 알고리즘

- ❖ Ron Rivest, Adi Shamir and Len Adlema에 의해 1978년 공포

❑ 알고리즘의 기본 형태

$C = M^e \bmod n$

$M = C^d \bmod n = (M^e)^d \bmod n = M^{ed} \bmod n$

1. 모든 $M < n$ 에 대하여 $M^{ed} = M \bmod n$을 만족하는 e, d, n 값을 찾는 것이 가능하다.
2. $M < n$ 인 모든 값에 대하여 M^e, C^d를 계산하기 쉽다.
3. 주어진 e 와 n에 대하여 d를 결정하기 어렵다.

Chapter 9 공개키 암호와 RSA

❑ RSA의 알고리즘

Key Generation

Select p, q	p and q both prime, $p \quad q$
Calculate $n = p \times q$	
Calculate $\phi(n) = (p-1)(q-1)$	
Select integer e	$\gcd(\phi(n), e) = 1; \quad 1 < e < \phi(n)$
Calculate d	$d \equiv e^{-1} \bmod \phi(n)$
Public key	$KU = \{e, n\}$
Private key	$KR = \{d, n\}$

Encryption

Plaintext:	$M < n$
Ciphertext:	$C = M^e \pmod{n}$

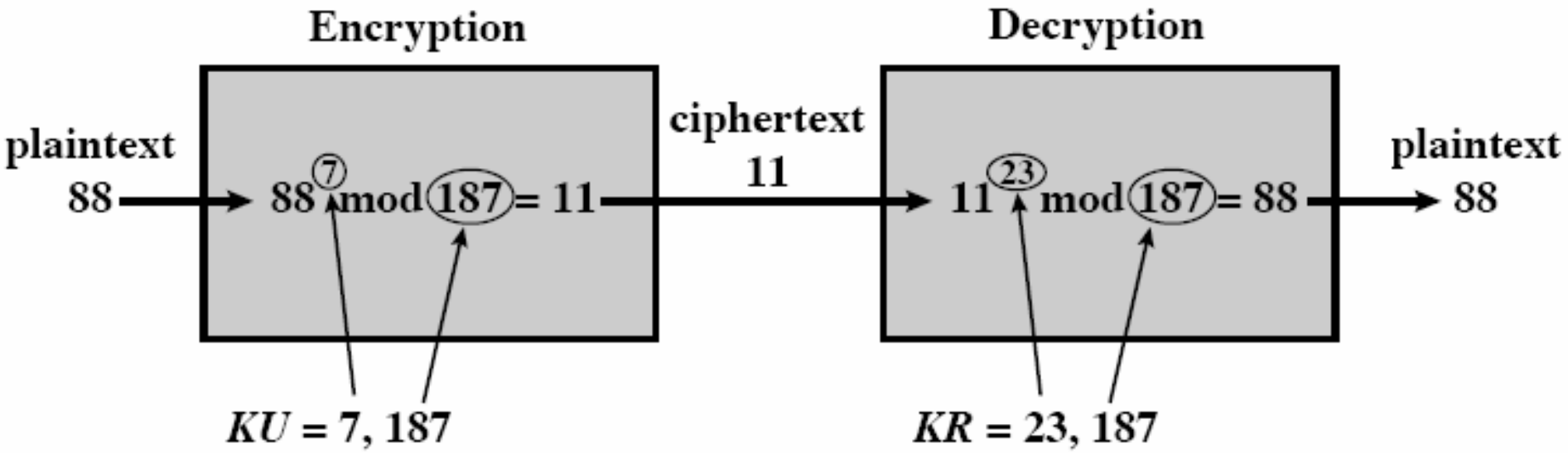
Decryption

Ciphertext:	C
Plaintext:	$M = C^d \pmod{n}$

Chapter 9 공개키 암호와 RSA

❑ RSA 알고리즘의 예(책 pp.275)

1. 두 솟수 p = 17, q = 11을 선택
2. n = pq = 17 * 11 = 187을 계산
3. φ(n)=(p−1)(q−1) = 16 * 10 = 160을 계산
4. φ(n)=160 과 서로소이고 φ(n) 보다 작은 e를 선택함, 예 e = 7
5. de = 1 mod 160이고 d < 160 인 d를 결정함. 23 * 7 = 161 = 10 * 160 +1 이기 때문에 정확한 값은 d = 23임.



Chapter 9 공개키 암호와 RSA

❑ RSA의 안전성

❖ RSA알고리즘의 공격

- ➢ 전사적 공격
  - ▪ 모든 가능한 개인키로서 시도함
- ➢ 시간적인 공격
  - ▪ 복호 알고리즘의 실행시간에 의존함
- ➢ 수학적인 공격
  - ▪ 두 솟수의 곱을 인수분해 하는 몇 가지 접근
  - ▪ 인수분해 문제
    - » 3가지 접근법(책 pp.279)

1. n을 두 개의 솟수로 인수분해 할 수 있는 경우
2. p와 q를 결정하지 않고 직접 φ(n)을 결정
3. 먼저 φ(n)을 결정하지 않고 직접 d를 결정

Thanks

Q & A