Section 01
키 배송 문제

1.1 키 배송 문제란?

- **키 배송 문제**(key distribution problem)
  - 대칭 암호를 사용하려면 송신자와 수신자가 대칭키를 사전에 공유해야 하는 문제
  - 대칭 키를 보내지 않으면 밥은 복호화할 수 없다
  - 안전하게 키를 보내는 방법은?

키 배송 문제를 해결하기 위한 방법

- 키의 사전 공유에 의한 해결
- 키 배포 센터에 의한 해결
- Diffie-Hellman 키 교환
- 공개 키 암호에 의한 해결

키를 보내 버리면 도청자 이브도 복호화 가능

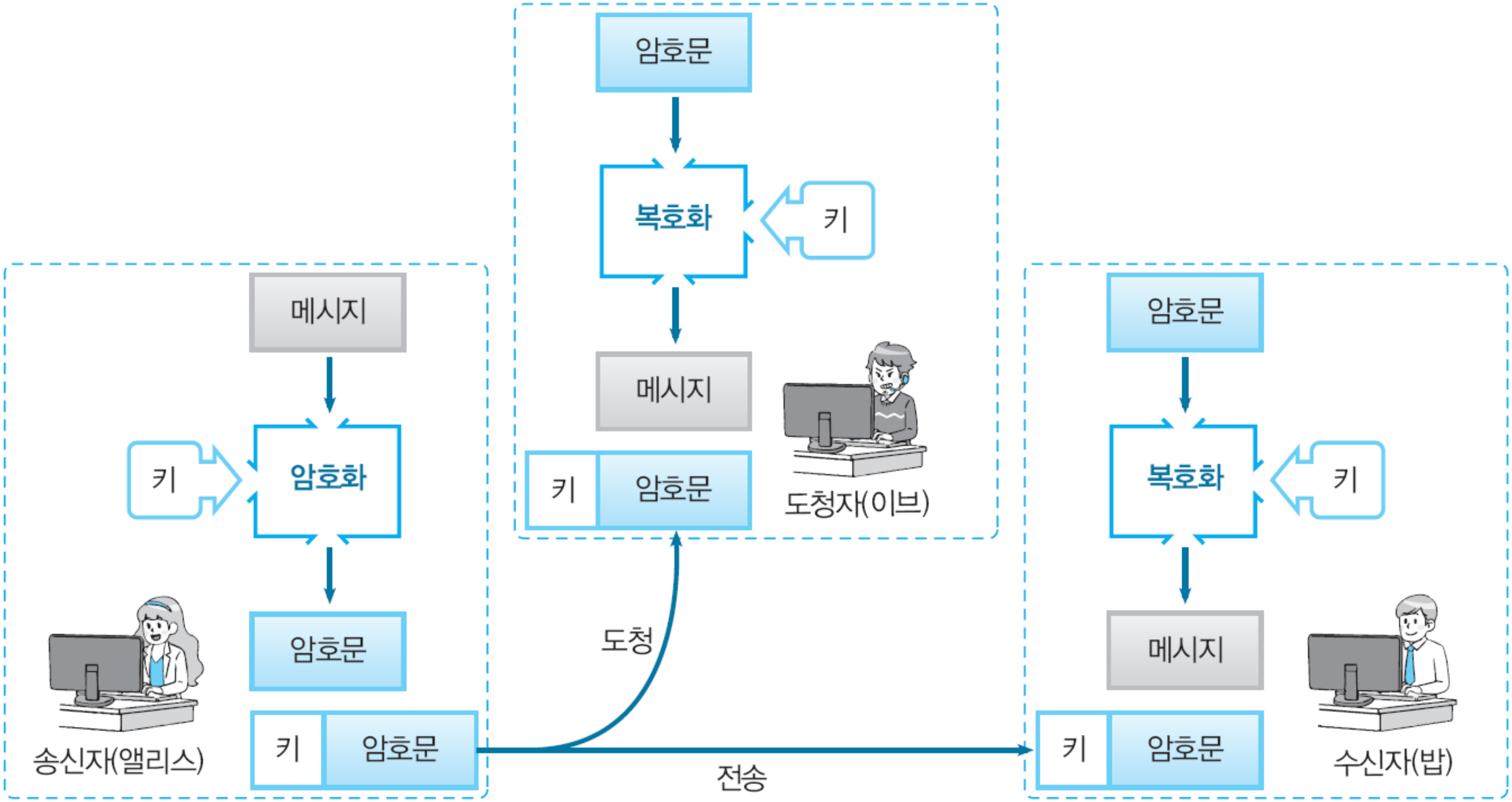


그림 6-1 • 키를 함께 보내면 도청자 이브도 복호화할 수 있다(키 배송 문제)

1.2 키 사전 공유에 의한 키 배송 문제 해결

- 키 사전 공유
  - 「안전한 방법으로 키를 사전에 건네주는」것
  - 직접전달은 안전
  - 이메일/일반메일 등은 위험
  - 인원이 많아지면 관리 해야 할 키 수 증가

사원 1000명 회사

- 1000명의 사원 한 사람 한 사람이 자신 이외의 999명과 통신할 가능성이 있다고 하면, 통신용 키는 1인당 999개가 필요
- 회사 전체로 필요한 키의 수

1000 × 999 ÷ 2 = 49만 9500개

- 현실적이지 못하다

1.3 키 배포 센터에 의한 키 배송 문제 해결

- **키 배포 센터**(key distribution center; KDC)
  - 암호 통신 때마다 통신용의 키를 키 배포 센터에 의뢰해서 개인과 키 배포 센터 사이에서만 키를 사전에 공유
  - 키 배포 센터의 역할을 하는 컴퓨터를 지정
  - 구성원 전원의 키를 보존

키 배포센터의 문제점

- 구성원 수 증가시 키 배포 센터의 부하
- 키 배포 센터의 컴퓨터가 고장시 조직 전체의 암호 통신 마비
- 키 배포센터가 공격의 대상이 될 수 있다

1.4 Diffie-Hellman 키 교환에 의한 키 배송 문제의 해결

- **Diffie-Hellman 키 교환**
  - 암호 통신을 원하는 두 사람이 있다면 어떤 정보를 교환한다
    - 이 정보는 도청자 이브에게 노출 되어도 무방
  - 두 사람은 교환한 정보를 가지고 동일한 키를 각각 생성할 수 있다
    - 하지만 도청자 이브는 같은 키를 만들 수 없다

1.5 공개 키 암호에 의한 키 배송 문제의 해결

- **공개 키 암호**
  - 대칭 암호
    - 「암호화 키」와 「복호화 키」 동일
  - 공개 키 암호
    - 「암호화의 키」와 「복호화 키」 다르다
    - 「암호화 키」를 가지고 있는 사람이라면 누구든지 암호화 할 수 있음
    - 하지만 「암호화 키」를 가지고 있어도 복호화할 수는 없다
    - 복호화 할 수 있는 것은 「복호화 키」를 가지고 있는 사람 뿐임

- 수신자는 미리「암호화 키」를 송신자에게 알려 준다.
  - 이「암호화 키」는 도청자에게 알려져도 무방
- 송신자는 그「암호화 키」로 암호화해서 수신자에게 전송
- 암호문을 복호화할 수 있는 자는「복호화 키」를 가지고 있는 사람(수신자)뿐
- 이렇게 하면「복호화 키」를 수신자에게 배송할 필요가 없음

공개 키 암호를 이용한 키 배송

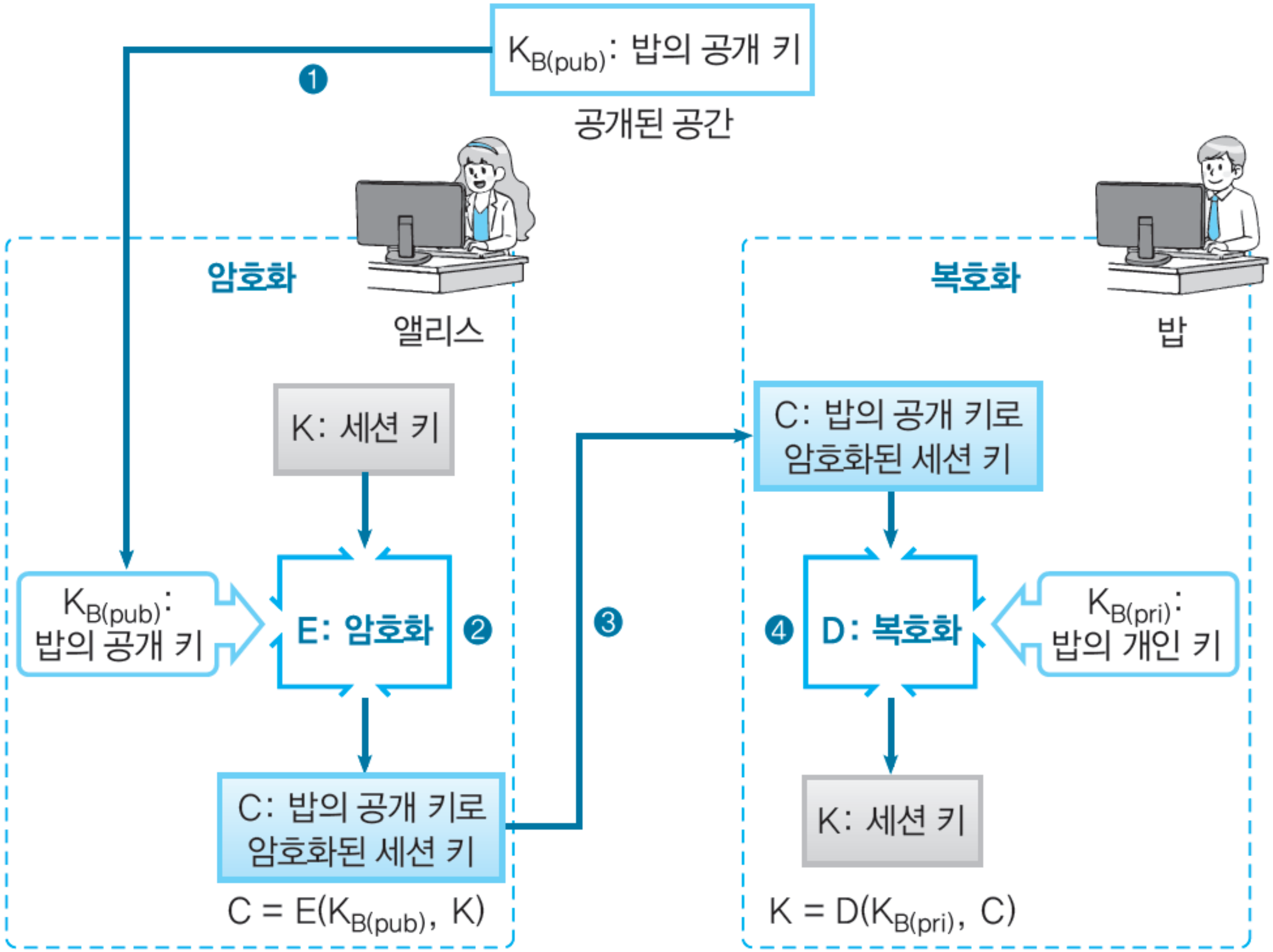


그림 6-3 • 공개 키 암호를 이용한 키 배송

Section 02
공개 키 암호

2.1 공개 키 암호란?

- **공개 키 암호**(public-key cryptography)
  - 「암호화 키」와 「복호화 키」가 분리
  - 송신자는 「암호화 키」를 써서 메시지를 암호화하고, 수신자는 「복호화 키」를 써서 암호문을 복호화

공개키 암호의 암호화

- 송신자가 필요한 것은 「암호화 키」뿐
- 수신자가 필요한 것은 「복호화 키」뿐
- 도청자에게 알려지면 곤란한 것은 「복호화 키」
- 「암호화 키」는 도청자에게 알려져도 무방

공개키의 의미

- **공개 키(public key)**
  - 「암호화 키」는 일반에게 공개해도 무방
  - 수신자에게 메일로 전달해도 무방
  - 신문의 광고란에 실어도 무방
  - 간판으로 해서 길가에 세워도 무방
  - Web 페이지를 통하여 전 세계에서 읽을 수 있도록 해도 무방
  - 도청자 이브에게 공개 키가 도청되는 것을 신경 쓸 필요가 없다

개인키의 의미

- **개인 키(private key)**
- 「복호화 키」는 미공개
- 이 키는 본인만 사용
- 개인 키는 다른 사람에게 보이거나, 건네주거나 해서는 안 됨
- 개인 키는 자신의 통신 상대에게도 보여서는 안 됨

공개키-개인키 쌍

- **키 쌍(key pair)**
- 공개 키와 개인 키는 둘이 한 쌍
  - 공개 키로 암호화한 암호문은 그 공개 키와 쌍이 되는 개인 키가 아니면 복호화 할 수 없다
- 수학적인 관계
  - 키 쌍을 이루고 있는 2개의 키는 서로 밀접한 관계
  - 공개 키와 개인 키 쌍은 별개로 만들 수 없음

공개키 암호의 역사

- Whitfield Diffie 와 Martin Hellman(1976)
  - 공개 키 암호의 아이디어를 발표
  - 암호화 키와 복호화 키의 분리성
  - 공개 키가 어떠한 특성을 갖추고 있어야 하는지를 제시
- Ralph Merkle 와 Martin Hellman(1977)
  - 배낭(napsack) 암호
- Ron Rivest, Adi Shamir, Leonard Adleman(1978)
  - 공개 키 암호 알고리즘 **RSA** 발표

2.2 공개 키를 사용한 통신 흐름

- 앨리스가 밥에게 메시지 보내기
  - (1) 밥은 공개 키/개인 키로 이루어진 한 쌍의 키($K_{B(pub)}$/$K_{B(pri)}$)생성
  - (2) 밥은 자신의 공개 키($K_{B(pub)}$)를 앨리스에게 전송
  - (3) 앨리스는 밥의 공개 키를 써서 메시지(P)를 암호화($C=E(K_{B(pub)},P)$)
  - (4) 앨리스는 암호문(C)을 밥에게 전송
  - (5) 밥은 자신의 개인 키($K_{B(pri)}$)를 써서 암호문을 복호화($P=D(K_{B(pri)},C)$)

공개 키를 사용한 메시지 전송

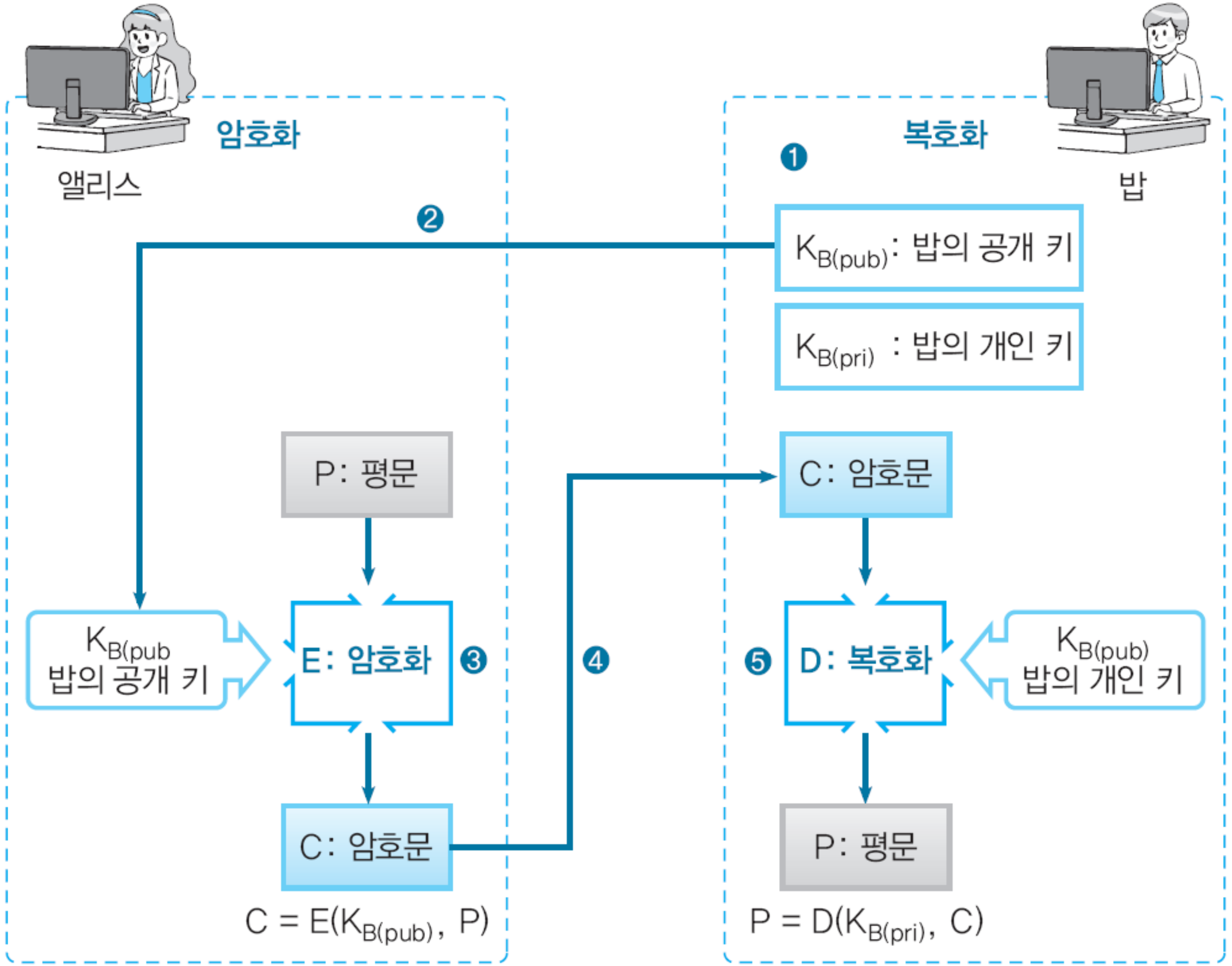


그림 6-4 • 공개 키를 사용해서 앨리스가 밥에게 메시지를 보낸다

Section 04

RSA

4.1 RSA란 무엇인가?

- **RSA**는 공개 키 암호 알고리즘의 하나
  - RSA 이름
    - 개발자 3명의 이름
    - Ron Rivest, Adi Shamir, Leonard Adleman의 이니셜(**R**ivest-**S**hamir-**A**dleman)
  - 응용
    - 공개 키 암호
    - 디지털 서명
    - 키 교환

4.2 RSA에 의한 암호화

- RSA에서 평문도 키도 암호문도 숫자로 변환한 뒤 실행
- RSA의 암호화는 다음 식으로 표현

암호문 = (평문)^{E} mod N

(RSA에 의한 암호화)

E와 N은 무엇일까?

- **(E, N): 공개 키**
  - E와 N이라는 한 쌍의 수를 알면 누구라도 암호화를 행할 수 있다
  - E와 N이 RSA 암호화에 사용되는 키
  - E와 N은 면밀한 계산을 통해 생성

4.3 RSA에 의한 복호화

- 복호화도 간단하다

$$평문 = (암호문)^{D} \bmod N$$

(RSA의 복호화)

D와 N은 무엇일까?

- **(D, N): 개인 키**
  - D와 N이라는 한 쌍의 수를 알면 누구라도 복호화를 행할 수 있다
  - D와 N이 RSA 복호화에 사용되는 키
  - D와 N도 면밀한 계산을 통해 생성
  - E와 D는 밀접한 연관관계

RSA의 암호화 · 복호화

키 쌍	공개 키	수 E와 수 N
	개인 키	수 D와 수 N
암호화		암호문 = (평 문)^{E} mod N (평문을 E제곱해서 N으로 나눈 나머지)
복호화		평 문 = (암호문)^{D} mod N (암호문을 D제곱해서 N으로 나눈 나머지)

RSA의 암호화와 복호화

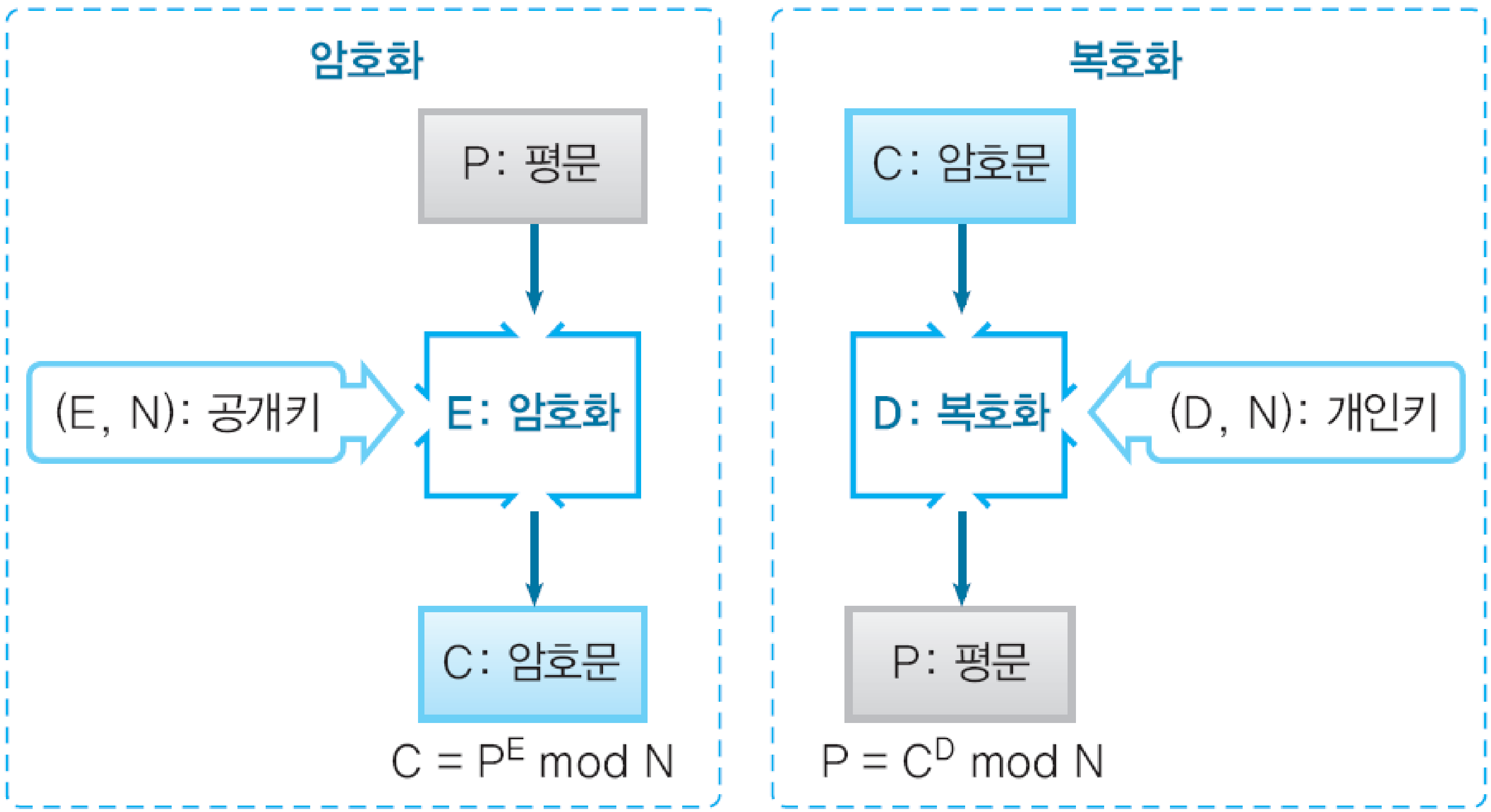


그림 6-6 • RSA 암호화와 복호화

4.4 키 쌍의 생성

1) N을 구한다

2) L을 구한다

(L은 키 쌍을 생성할 때만 등장하는 수이다)

3) E를 구한다

4) D를 구한다

N 구하기

1024비트 이상의 소수여야 함

- 큰 소수를 2개 준비(p와 q)
- N = p × q (p, q는 소수)

ex) p=11, q= 3, N=33

L 구하기

- L 은 RSA의 암호화나 복호화에 사용안함
- 키 쌍을 만들 때 임시로 사용
- L = lcm(p-1, q-1)

  (L은 p-1 과 q-1의 최소공배수)

E 구하기

- 다음 두 식을 만족하는 수 E를 하나 찾아 낸다
- 1 < E < L
- gcd(E, L) = 1 (E와 L은 서로 소)

GCD(e,10)=1
e = 3

D 구하기

E->D(수정)

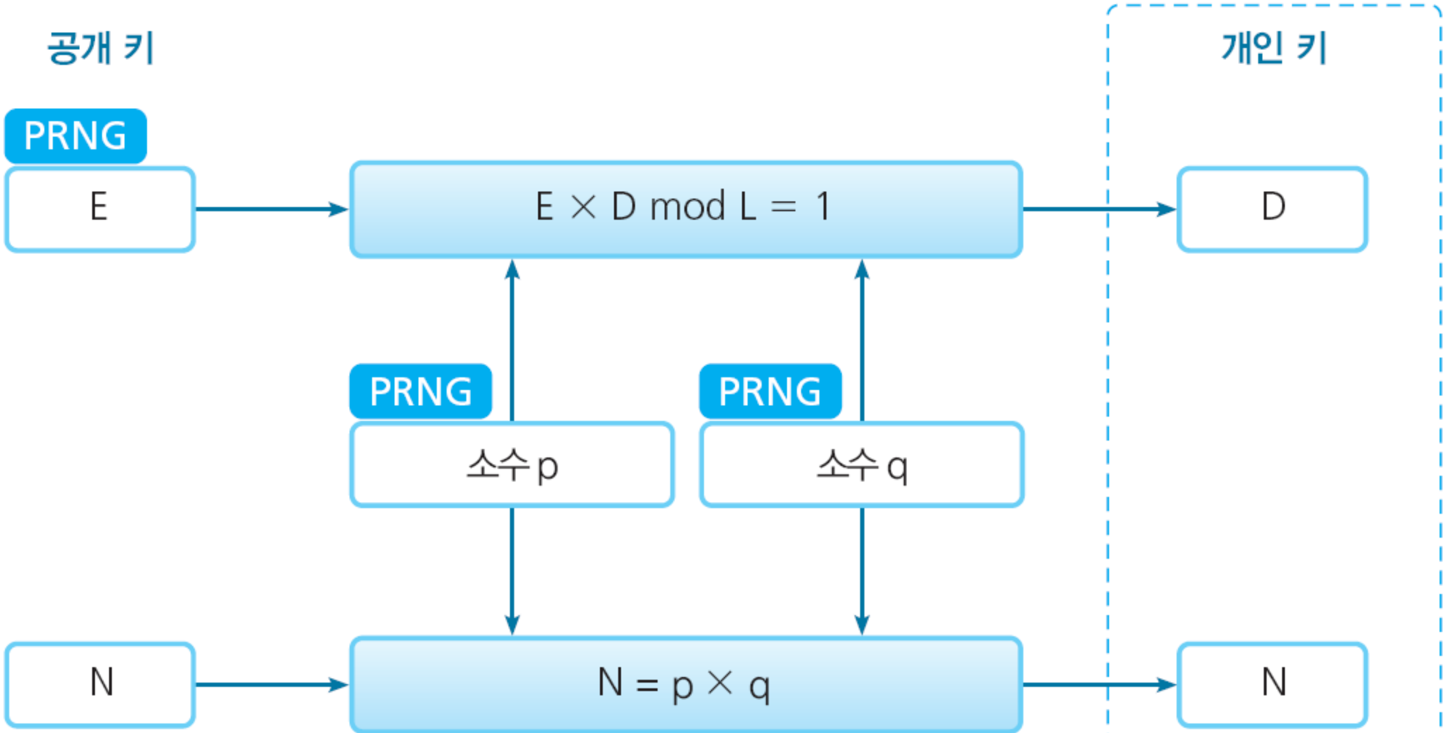
- 다음 두 식을 만족하는 수 E를 하나 찾아 낸다
- $1 < D < L$
- $E \times D \bmod L = 1$

d = 7

RSA 키 쌍 생성

(1) N을 구한다 의사난수 생성기로 p와 q를 구한다 p와 q는 소수 $N = p \times q$
(2) L을 구한다 $L = lcm(p-1, q-1)$ L은 p-1과 q-1의 최소공배수
(3) E를 구한다 $1 < E < L$ $gcd(E, L) = 1$ E와 L과의 최대공약수는 1(E와 L은 서로 소)
(4) D를 구한다 $1 < D < L$ $E \times D \bmod L = 1$

RSA 키 쌍



PRNG = 의사난수 생성기

$L = \mathrm{lcm}(p-1, q-1)$

$\gcd(E, L) = 1$

$1 < E < L$

$1 < D < L$

e=3, d=7, n=33

public key = (3,33)
private key = (7,33)

그림 6-7 • RSA의 키 쌍

4.5 구체적 계산

- 구체적인 수를 써서 RSA의 키 쌍 생성 · 암호화 · 복호화를 실제로 구현
- 너무 큰 수(p와 q)를 사용하면 계산이 힘들기 때문에 작은 수를 이용하여 계산

RSA 예

- p 와 q 선택하기
  - 2개의 소수 p=17, q=19 선택
- N 구하기
  - N = p × q = 17 × 19 = 323
- L 구하기
  - L = lcm(p-1, q-1) = lcm(16, 18) = 144 (16과 18의 최소공배수)
- E 구하기(선택하기)
  - gcd(E, L) = 1 이 되는 수 E 를 선택하자.
  - E가 될 수 있는 수는 다음과 같은 수이다.
  - 5, 7, 11, 13, 17, 19, 23, 25, 29, 31, ...
  - 우리는 E=5를 선택(다른 수를 선택해도 무방)
- D 구하기
  - E × D mod L = 5 × 29 mod 144 = 145 mod 144 = 1 이므로 D=29

RSA 예

- 공개 키: (E, N) = (5, 323)
- 개인 키: (D, N) = (29, 323)

암호화

- 평문은 N=323 보다 작은수
- 예로 평문=123이라 하고 암호화를 해보자

$$평문^E \bmod N = 123^5 \bmod 323$$
$$= 225$$

M(메세지)는 8인 경우
이때 M은 N보다 작아여 함(M M B)

C=M^e mod N
8^3 mod 33 = 512 mod 33 = 17

복호화

$$암호문^{D} \bmod N = 225^{29} \bmod 323$$

$$= 123$$

8 -> c( ) -> 17
M = c^d mod N =17^7 mod 33
= 410338673 mod 33
= 8

보통 AES 키를 담아서 보낼 때 많이 사용함

225^{29} mod 323의 계산

- $29=10+10+9$
- $225^{29} = 225^{10+10+9} = 225^{10} \times 225^{10} \times 225^{9}$
  - $225^{10} = 3325256730079650878906 25$
  - $225^{9} = 1477891880035400390625$
  - $225^{10} \bmod 323 = 332525673007965087890625 \bmod 323 = 16$ ...... (1)
  - $225^{9} \bmod 323 = 1477891880035400390625 \bmod 323 = 191$ ...... (2)

$225^{29} \bmod 323 = 225^{10} \times 225^{10} \times 225^{9} \bmod 323$
$= \underline{(225^{10} \bmod 323)} \times \underline{(225^{10} \bmod 323)} \times \underline{(225^{9} \bmod 323)} \bmod 323$
$= 16 \times 16 \times 191 \bmod 323$
$= 48896 \bmod 323$
$= 123$

- 따라서 $225^{29} \bmod 323 = 123$