정보보안개론

박 종 혁 교수

UCS Lab

Tel: 970-6702

Email: jhpark1@seoultech.ac.kr

목차

1. 정보사회 특징

- 돋은 사회의 변화추세가 어디로 가는지를 나타내는 지표
  - 디지털과 사이버 세계의 새로운 지식산업이 높은 부가가치 창출
- 탈산업 사회화의 추세
  - 물적 자원시대에서 지식기반 자원시대로 전환
  - 컴퓨터와 통신기술의 발달로 사회생활 양식의 변화
- 정보통신 기술의 발달
  - 정보 유통에 필요한 비용을 현저하게 낮추어 비약적인 생산성 향상
- 지식과 정보량의 폭발적 증가
  - 2050년 현재 지식의 1%만 사용
- 세계화의 진전
  - 세계적 대응이 불가피(판매/지식확산/이익, 경쟁/질병/환경)

지식사회 혁명

- 거대한 새로운 변화의 물결
- 지식 혁명
- 디지털 혁명
- 기술정보 혁명
- 인터넷 혁명
- **.com ism**(닷컴이즘)

➔ 지식과 정보의 활용을 극대화하고 체계적으로 관리하지 않는 조직은 생존 불가

지식사회 의식의 혁명

- 지식사회 특징
  - 부가가치 재료의 변화
  - 지역적/시간적 한계극복
  - 글로벌 네트워크를 통한 실시간 거래
  - 정보의 획득, 판단, 행동의 속도혁신이 성공 요인

➔ 사고, 행동, 의식의 혁명 필요

➔ 인터넷을 이용한 빛의 속도로 상거래

(CALS: Commerce At Light Speed)

인터넷 상거래 특성

구분	전통적 상거래	전통적 EC	인터넷 EC
유통채널	기업→도매상→소매상→소비자	기업-대-기업	기업-대-고객, 기업-대-기업, 기업-대-행정, 사용자-대-사용자
거래지역	일부 특정 지역	특정 분야 폐쇄모임	시장 개방, 세계적 규모
고객상대	시장 방문자	제한된 조직의 상대방	무제한의 상대방
마케팅활동	직접 방문	폐쇄된 전용 네트웍	개방된 네트웍
고객신뢰	실물 인증	신뢰된 상대방	다수의 불확실한 상대방
보안기술	필요 없음	가입자간 보안 설계	보안 및 인증의 필요성
판매거점	물리적 판매 공간	가입자 네트웍	가상 상점 공간

2. 정보보안 개요

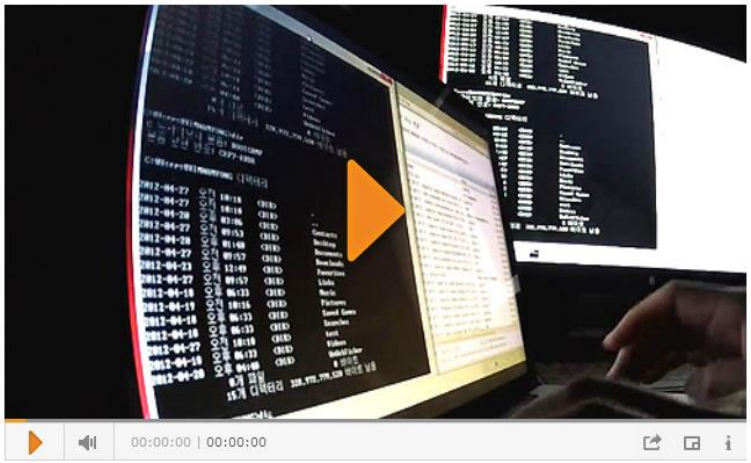
2014년 정보의 위협

- 해킹 및 인터넷 시스템 위협

"국방과학연구소 해킹으로 군 기밀 대량 유출"

김수형 기자 416 0 공유하기

입력 : 2014.04.10 11:25 | 수정 : 2014.04.10 12:37



국방과학연구소가 해킹을 당해서 군사기밀이 대량 유출됐다고 새정치민주연합 김영주 의원이 밝혔습니다.

김 의원은 중국과 북한 조직으로 추정되는 해커들이 프로그램의 중앙 배포 서버에 악성코드를 침투시켜 내부의 전체 PC와 서버를 장악해 군사기밀 자료가 유출됐다고 주장했습니다.

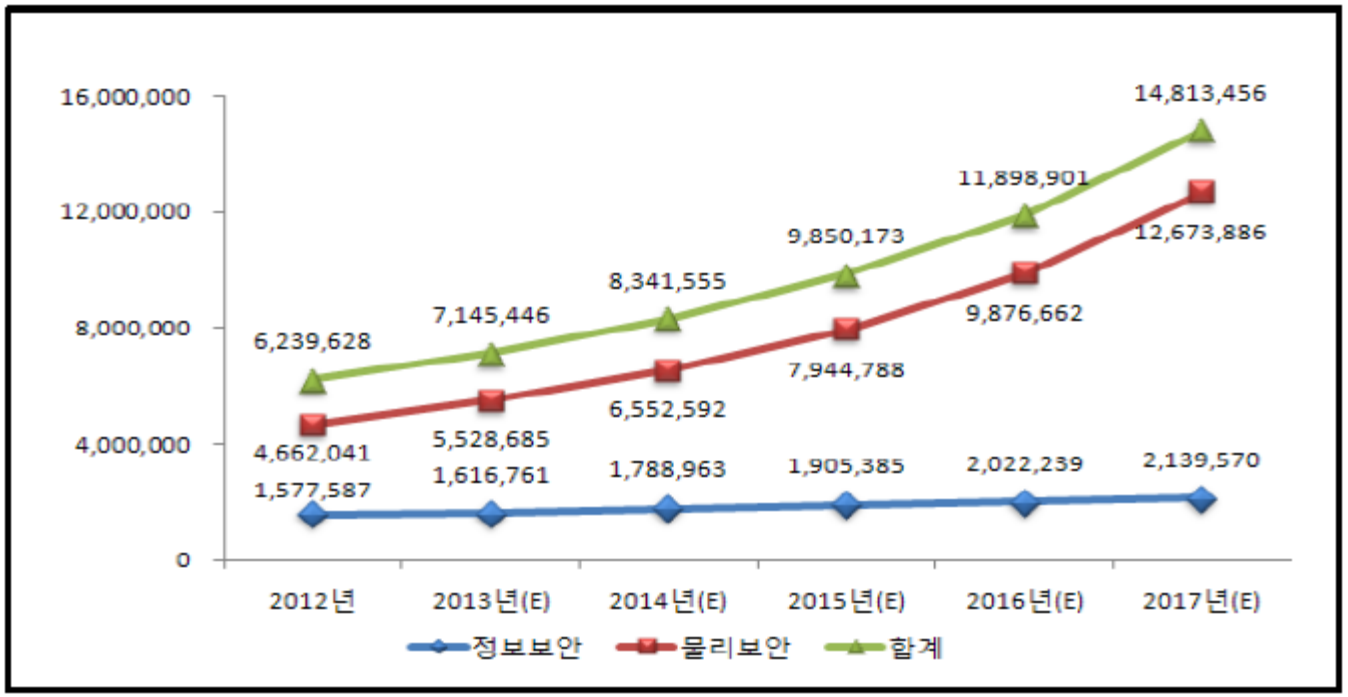
해킹에 신한·국민·농협카드 10 여만명 정보유출

경찰청이 확인한 사고액만 268건에 1억2천만원에 달한다. 카드사 중에서는 국민카드의 사고액이 가장 많은 것으로 알려졌다.

신한카드 관계자는 "이번 포스단말기 유출과 관련해 사고 가맹점의 정보유출 고객에 대해 지난 1월 소비자보호 사전안내를 통해 재발급 등 필요한 조치를 완료했다"면서 "기존 조치 완료 고객을 제외한 나머지 고객의 피해를 예방하고자 카드 재발급 안내 및 24시간 FDS 모니터링을 강화하고 있다"고 말했다.

정보보호 시장 가능성

[그림] 정보보호산업 규모 전망 (단위 : 백만원)



KISIA, 2013 국내정보보호산업 실태조사

개인 정보 유출 흐름도


>>개인정보 유출 흐름도
개인정보 Source
전기통신 사업자
호텔, 백화점
은행, 카드사
의료기관, 동호회
Website
개인정보 유출
내부자
외부 위탁점
해커
관리 부주의
개인정보 축적·거래
온라인
인터넷 카페 등을 통한 거래(1천만명 이상의 개인정보 유통 추정)
개인정보 1건당 1원
오프라인
CD 등 저장 매체를 통한 직접 판매
개인정보 오남용
타인명의 인터넷 회원가입
불법 대포폰 개설
신용카드 명의도용
ARS 결제요금 전가
인터넷서비스 가입권유 TM

개인 정보보호 강화 대책 추진현황

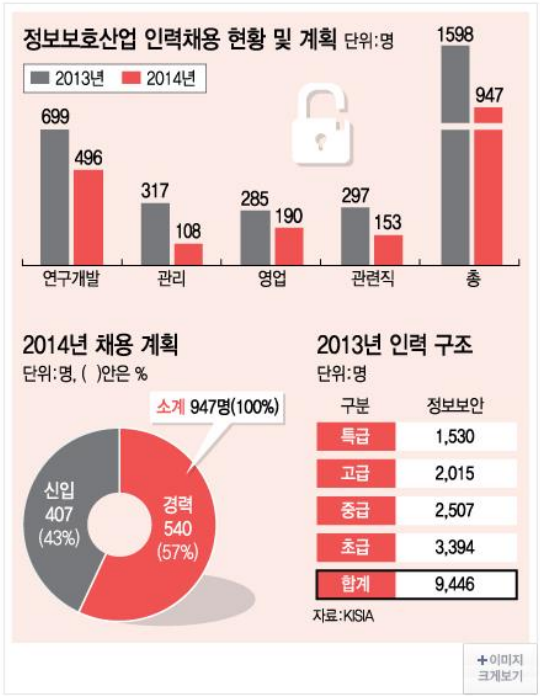
정보보호 인력 필요

- 정보보호 인력 필요

보안솔루션 개발자 어디에? "인재 찾기 어렵네"

갈수록 다양해지는 보안솔루션 분야, 적합한 인재 찾기 쉽지 않아

머니투데이 진달래 기자 | 입력 : 2014.07.03 05:41



보안업계가 우수한 개발 인력을 찾는데 여전히 어려움을 겪고 있다. 갈수록 보안솔루션 영역이 다양해지면서 인력난도 심화되는 추세라고 인사담당자들은 전했다. 솔루션 품질을 높이는데 가장 중요한 요소인 인재 확보가 힘든 상황에서는 국내 보안업체 경쟁력 강화도 요원하다는 우려가 나온다.

정보보호 인력 채용 활기

행문기사 이기사 번역의뢰하기

정보보호 기업과 관련 기관들이 잇따라 신규채용에 나서면서 인력 시장이 활기를 띠고 있다.

19일 관련 업계에 따르면 한국정보보호진흥원과 금융보안연구원이 신규 채용을 시작한 것은 물론 민간 정보보호 평가기관을 비롯해 주요 보안 기업이 컨설턴트와 영업, 개발 등 다양한 분야에서 직원을 채용하고 있다. 또 11월 중에는 한국정보보호산업협회와 한국정보보호학회가 '제1회 정보보호 인력 채용 박람회'를 여는 등 어느 때보다 인력 채용 움직임이 활발해 질 전망이다.

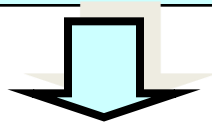
가장 먼저 채용에 나선 곳은 금융보안연구원(원장 정성순)이다. 금융보안연구원은 이달 말 일회용비밀번호(OTP) 통합인증센터 운영에 들어가는 것은 물론 전자금융거래에 대한 위협에 적극 대처하기 위해 인력 수급에 나섰다.

모집분야는 △금융정보보호 대책 수립 및 연구 개발 △금융부분 정보보호 제품 적합성 테스트 및 취약성 분석 △피싱, 해킹 등 금융부분 전자적 침해에 대한 사전 취약성 점검 및 대응 등에 신입과 경력, 인턴 사원을 채용한다.

- 컴퓨터에 저장된 파일 및 통신망 유통정보를 보호하기 위해 도구 필요
- 공용시스템의 경우(시분할 시스템)
- 데이터 네트워크를 통해서 접근하는 시스템

컴퓨터 보안 (Computer security)
데이터를 보호하고 해커를 막기 위한 도구의 집합을 총칭

- 분산 시스템의 등장
- 사용자와 컴퓨터간의 데이터전송을 위한 네트워크 및 통신시설의 이용



네트워크 보안 (Network security)
전송중인 자료를 보호

인터네트워크 보안 (Internetwork security)
상호연결된 네트워크 집합을 보호

- 정보 보안 (Information Security)
- 컴퓨터 보안 (Computer Security)
- 네트워크 보안 (Network Security)
- 인터네트워크 보안 (Internetwork security)
- 인터넷 보안 (Internet Security)
- 보안
- 정보보호

3. 보안 공격

보안 공격 (Security Attack)
조직에 의하여 소유된 정보의 안전성을
위태롭게 하는 어떠한 행위

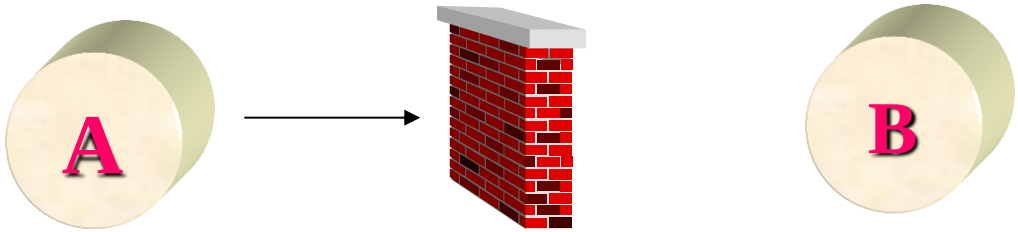
보안 메커니즘 (Security Mechanism)
보안 공격을 예방, 탐지, 복구하기 위하여
설계된 메커니즘

보안 서비스 (Security Service)
조직의 데이터 처리 시스템과 정보의 전송에 대한
안전성을 수행하기 위한 서비스

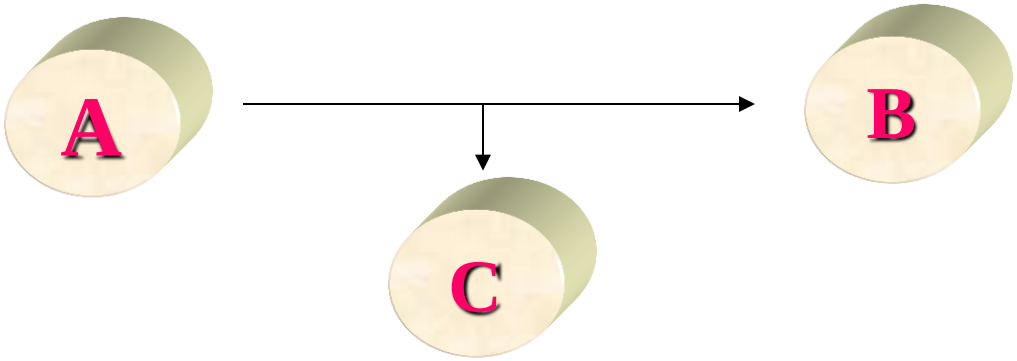
보안 공격

- 보안 공격 (Security Attack)
  - 조직의 정보보호를 저해하는 제반행위

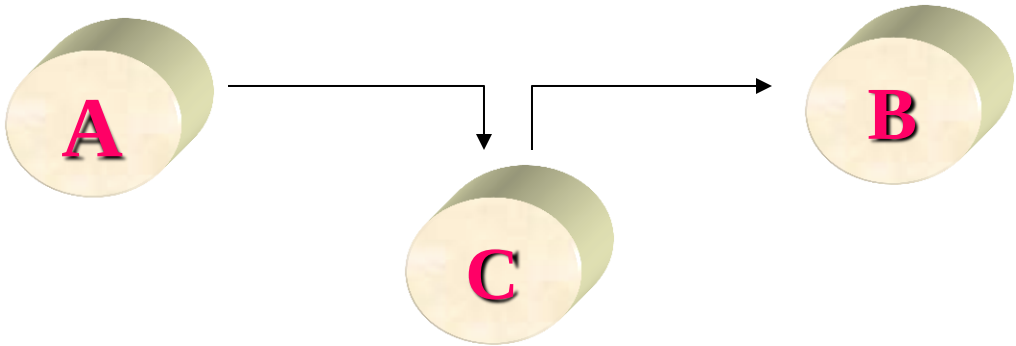
- 보안 공격의 유형(그림 1.1)
  - 방해 (Interruption)
    - 시스템의 일부가 파괴되거나 사용할 수 없는 경우로 가용성에 대한 공격



– 가로채기 (Interception)
  - 비인가자들의 불법적인 접근에 의한 신뢰성에 대한 공격

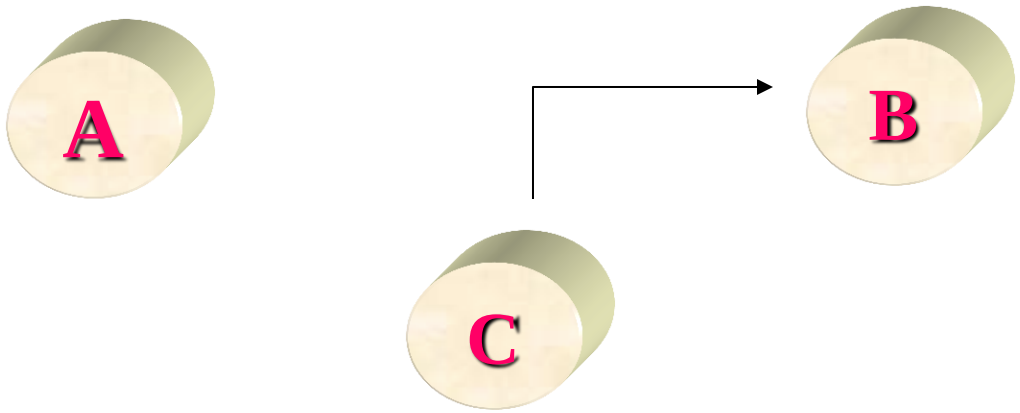


❖ 불법수정 (Modification)
  - ➢ 비인가자들의 불법적인 접근 뿐만 아니라 불법적인 변경에 의한 무결성에 대한 공격



❖ 위조 (Fabrication)

➢ 비인가자들의 시스템에 대한 위조물 삽입에 의한 인증에 대한 공격



- 자연적 위협 요소
  - 자연적 재앙, 에러 및 손실, 정보관리 부실
  - 네트워크 장애, 시스템 장애
- 고의적 위협 요소
  - 내부의 적, 컴퓨터 해킹, 위장(Masquerade)
  - 메시지 순서 변조 (Modification of Message Sequence)
  - 정보 변조 (Modification of Information)
  - 서비스 거부 (Denial of Service), 부인 (Repudiation)
  - 정보노출 (Leakage of Information)
  - 신분 레이블 변조 (Modification of Identification Label)

보안 공격

소극적 공격

철 수

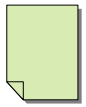
전송 파일 및 내용
공개
트래픽 분석을 통
한 추측

영희

적극적 공격

가로채기

재전송, 메시지 수정



철수로 위장

- 소극적 공격 (passive attack)
  - 가로채기
  - 도청
  - 트래픽 분석: 송수신자 신분, 통신시간 , 주기관찰
  - 변화가 없으므로 검출 곤란
  - 검출보다 예방 필요
- 적극적 공격 (active attack)
  - 방해: 가용성 침해
  - 불법적 수정: 무결성 침해
  - 재전송 : 데이터 단위 수동적 획득 -> 다시 전송
  - 서비스 부인 (서비스 거부 공격) : 특정 목표물을 대상으로 무력화, 성능저하 유발
  - 예방하기가 대단히 어려움: 모든 자원과 시간 보호불가능
  - 예방, 탐지, 복구 필요

4.보안 서비스

- 보안 서비스 (Security Service)
  - 조직의 데이터 처리 시스템 및 정보 전송에 대한 보안을 강화하기 위한 제반 서비스

- 보안 서비스의 종류
  - 기밀성 서비스 (Confidentiality, 비밀성, 비밀유지)
    - 합법적인 실체만 읽을 수 있도록 보호하는 서비스
    - 메시지 내용 공개, 트래픽 흐름 분석, 도청으로부터 전송 메시지 보호
    - 접속 구간 기밀성, 내용 기밀성, 메시지 흐름 기밀성
    - 암호 알고리즘 이용

- 무결성 서비스 (Integrity, 온전성)
  - 합법적인 실체만 수정할 수 있도록 보호하는 서비스
  - 연결형 무결성 서비스, 비연결형 무결성 서비스
    - 연결형 : 메시지 스트림을 대상, 불법변경 보호와 서비스 부인 방지
    - 비연결형 : 개인 메시지들만을 대상, 불법변경 보호
  - 해쉬 함수, 디지털 서명, 암호 알고리즘 이용

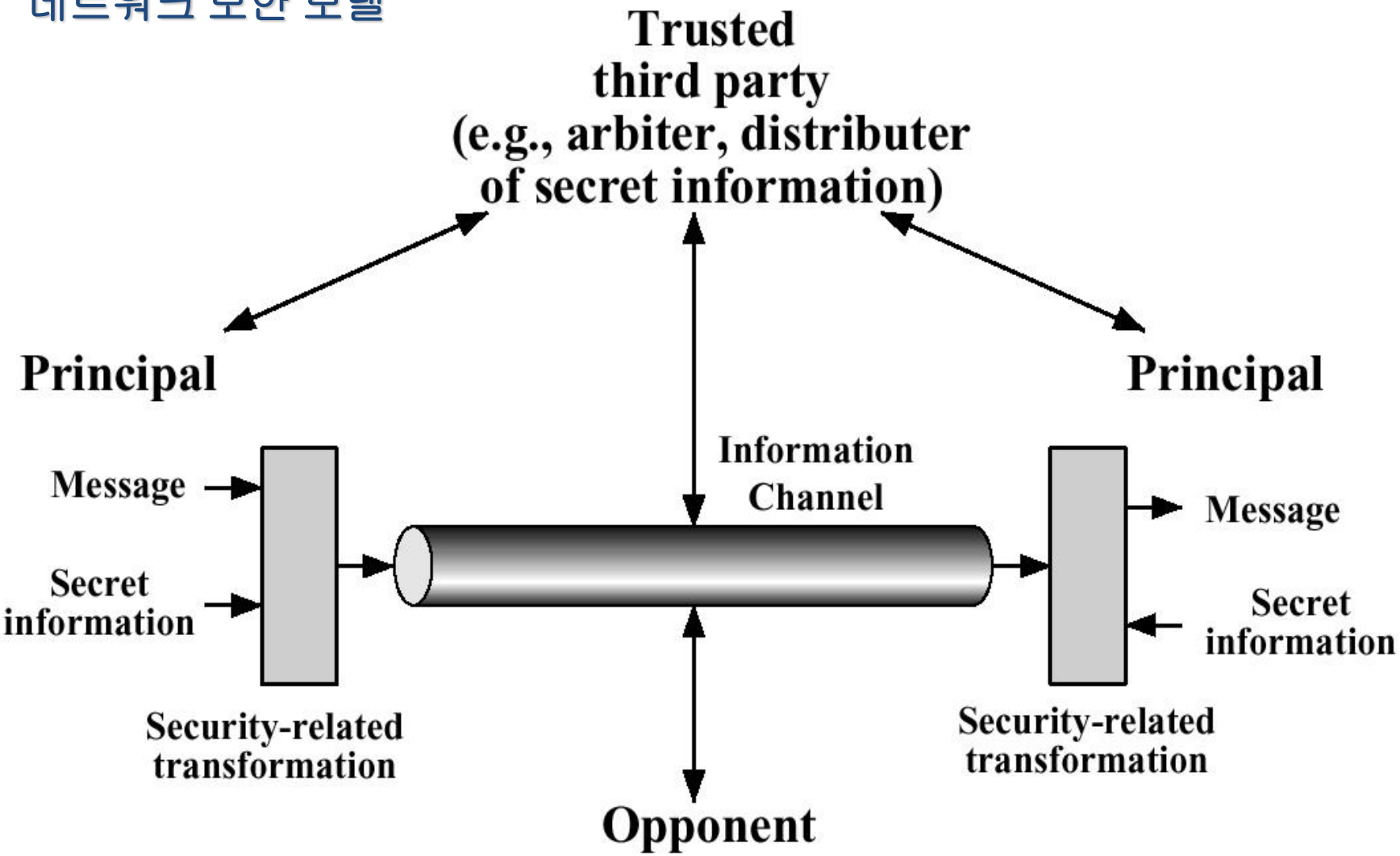
- 인증 서비스 (authentication, 보증)
  - 정보 및 시스템의 자원을 사용하는 정당한 사용자임을 확인할 수 있도록 보호하는 서비스
  - 연결된 송수신자 확인, 제 3자의 위장 확인
  - 발신처 인증, 메시지 인증, 실체 인증

- 부인봉쇄 서비스 (non-repudiation, 부인방지)
  - 송수신자가 송수신 사실에 대한 부인을 하지 못하게 하는 것
  - 송신자 부인 봉쇄, 수신자 부인봉쇄, 배달증명, 의뢰증명
- 접근 제어 서비스 (access control, 접근통제)
  - 사용자가 시스템 혹은 특정 자원에 접근 하고자 할 때 인가 받은 사용자만 접근을 허락하도록 제어하는 서비스
- 가용성 서비스 (Availability)
  - 컴퓨터 시스템이 인가 당사자가 필요로 할 때 이용할 수 있게 보호하는 서비스

**** 보안의 3대 서비스: C I A**

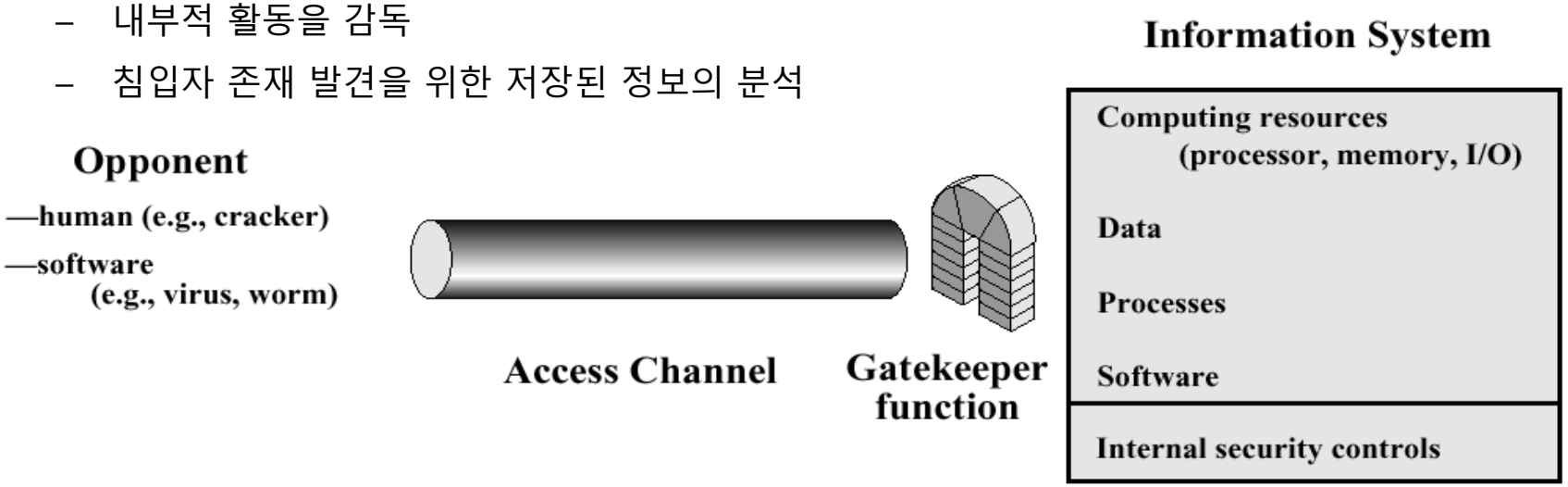
5. 보안 모델

네트워크 보안 모델



네트워크 접근 보안모델

- 1차 방어: gatekeeper function
  - 패스워드 기반 로그인 절차: 사용자 인증, 접근 통제
  - 감독 및 심사 구조: 웜, 바이러스 등의 검출과 거부
- 2차 방어: monitoring function
  - 원하지 않는 침입자를 검출하기 위한 내부적 보안 제어
  - 내부적 활동을 감독
  - 침입자 존재 발견을 위한 저장된 정보의 분석



보안 서비스 설계

- 보안을 위한 모든 기술의 2가지 요소
  - 보안을 위한 암호화 또는 특정 코드의 추가
  - 암호화 키와 같은 어떤 비밀 정보
- 일반 모델로부터 특정 보안 서비스 설계의 기본 사항
  - 보안 관련 변환 알고리즘의 설계
    - 공격자가 변환을 파악할 수 없는 것이어야 함
  - 변환 알고리즘과 병용될 비밀 정보의 생성
  - 비밀정보의 분배 및 공유 방법의 개발
  - 특정 보안 서비스를 위한 보안 알고리즘 및 비밀정보를 사용할 통신주체간의 프로토콜 지정

공개키 암호 시스템의 원리

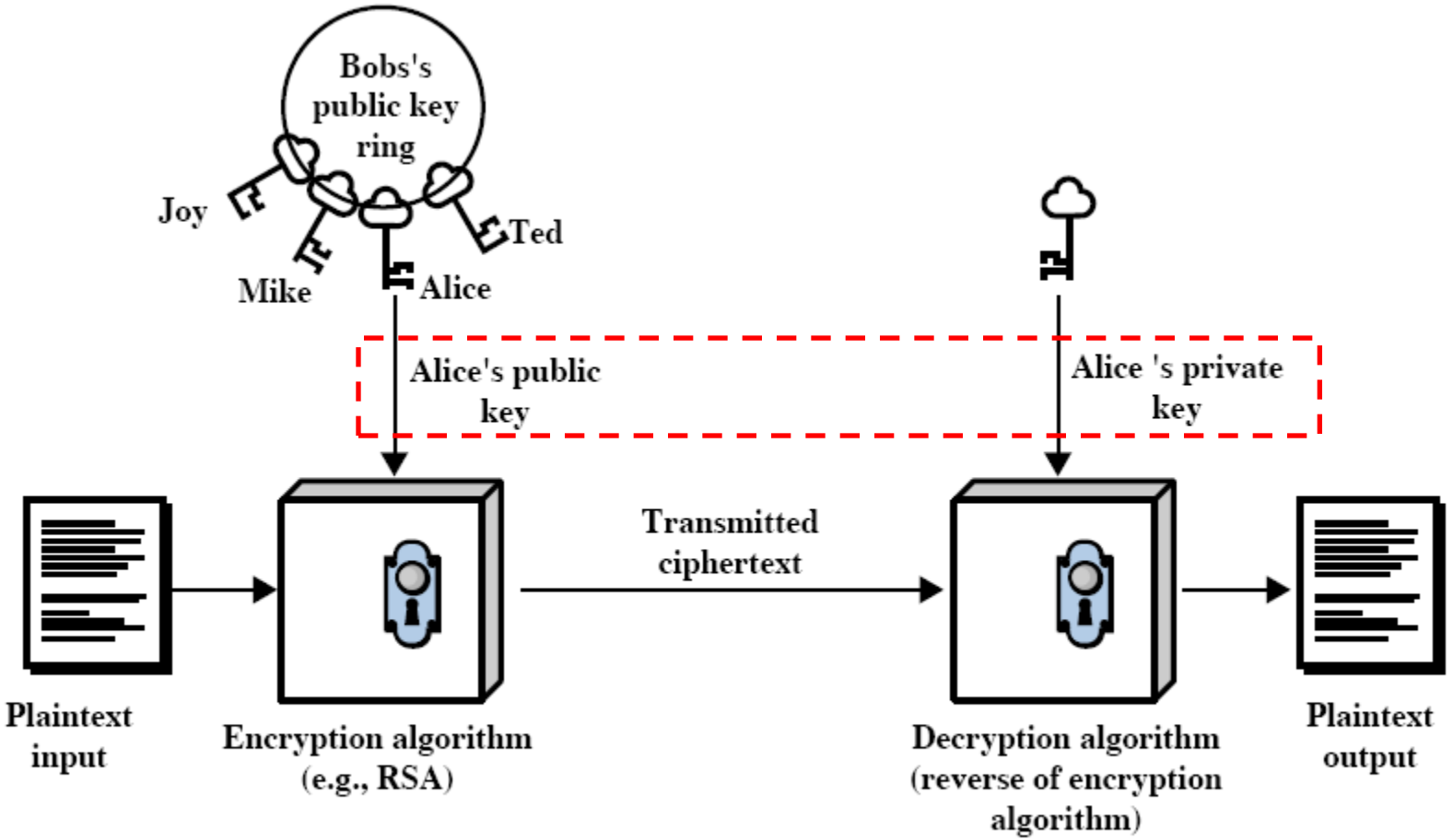
- 공개키 암호 시스템의 원리
  - 공개키 암호 시스템의 특징
    - 주어진 암호 알고리즘과 암호키를 알고 있더라도 복호키를 결정하는 것은 계산적으로 실행 불가능
    - 두 개의 관련된 키에서 하나는 암호에 사용될 수 있고, 나머지는 복호에 사용됨
  - 공개키 암호 구조의 구성 요소
    - 평문 : 읽을 수 있는 평문 메시지 또는 데이터
    - 암호 알고리즘 : 평문에 대하여 다양한 변형을 수행
    - 공개키와 개인키 : 하나는 암호화를 위하여 사용되고 다른 하나는 복호화를 위하여 사용되도록 선택된 키의 쌍
    - 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

공개키 암호 시스템의 원리

- 공개키의 처리 단계

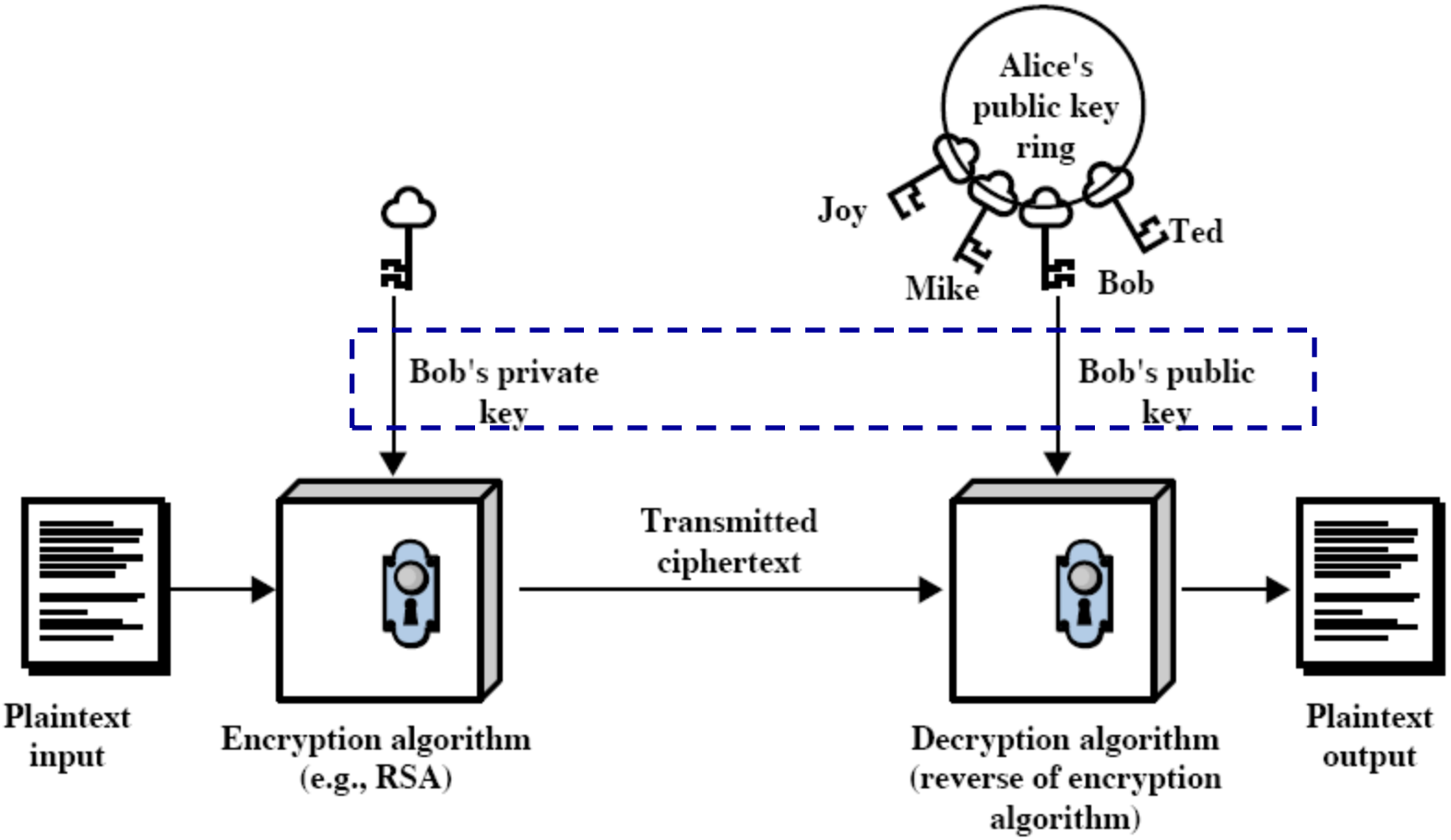
1. 각 사용자는 메시지의 암호화와 복호화에 사용하기 위한 키 쌍을 생성
2. 각 사용자는 공개된 등록처나 또는 접근 가능한 파일에서 2개의 키 중에 하나를 설치(공개키), 대응되는 키는 비밀로 유지
3. 봅이 앨리스에게 비밀 메시지를 보내기 원하다면, 봅은 앨리스의 공개키를 사용하여 메시지를 암호화함
4. 앨리스가 메시지를 받았을 때, 앨리스는 자신의 개인키를 사용하여 복호화 함, 앨리스만의 개인키를 알기 때문에 다른 수신자는 메시지를 복호화할 수 없음

공개키 암호 시스템의 원리



(a) Encryption

공개키 암호 시스템의 원리



(b) Authentication

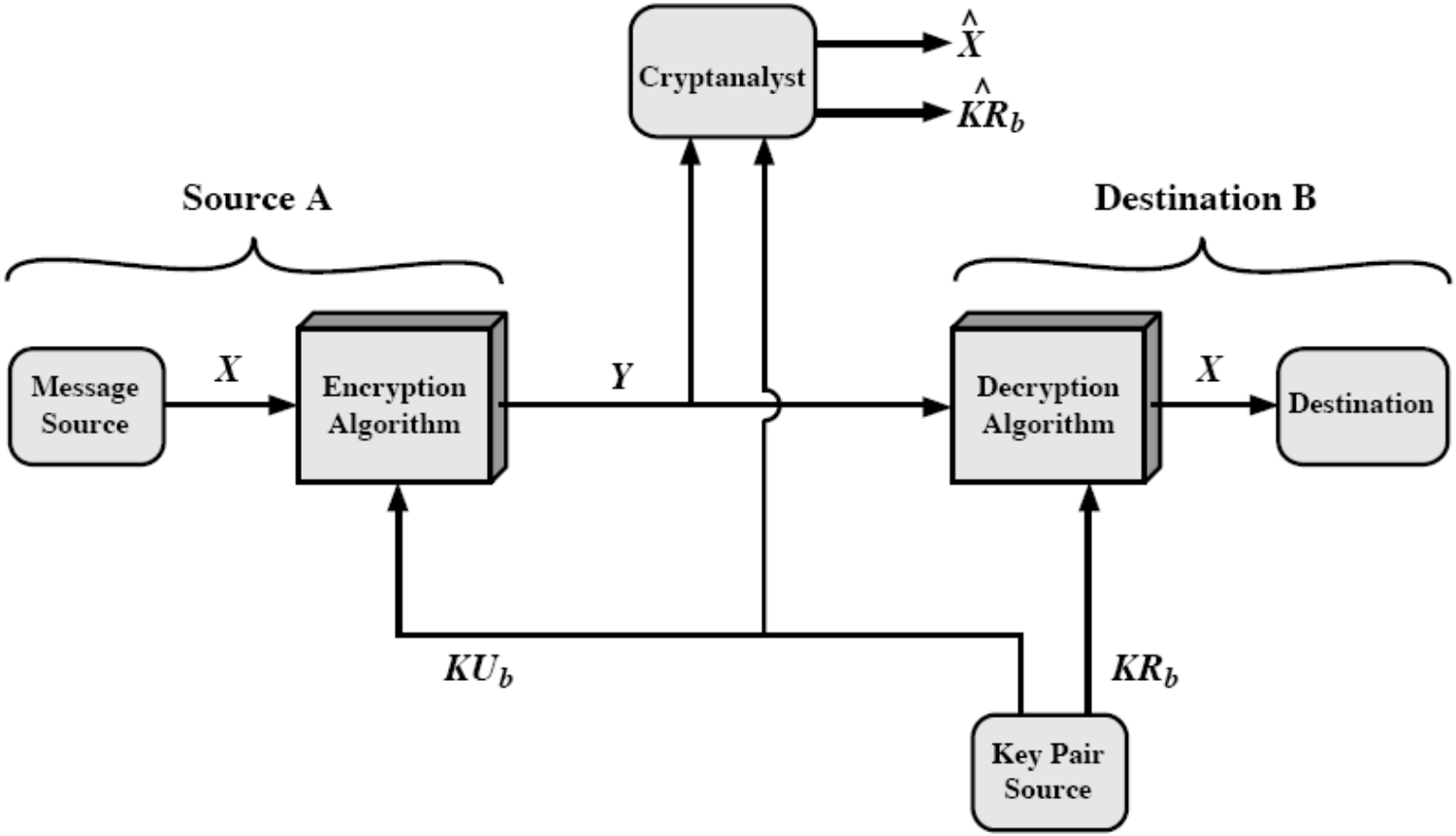
공개키 암호와 RSA

- 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.

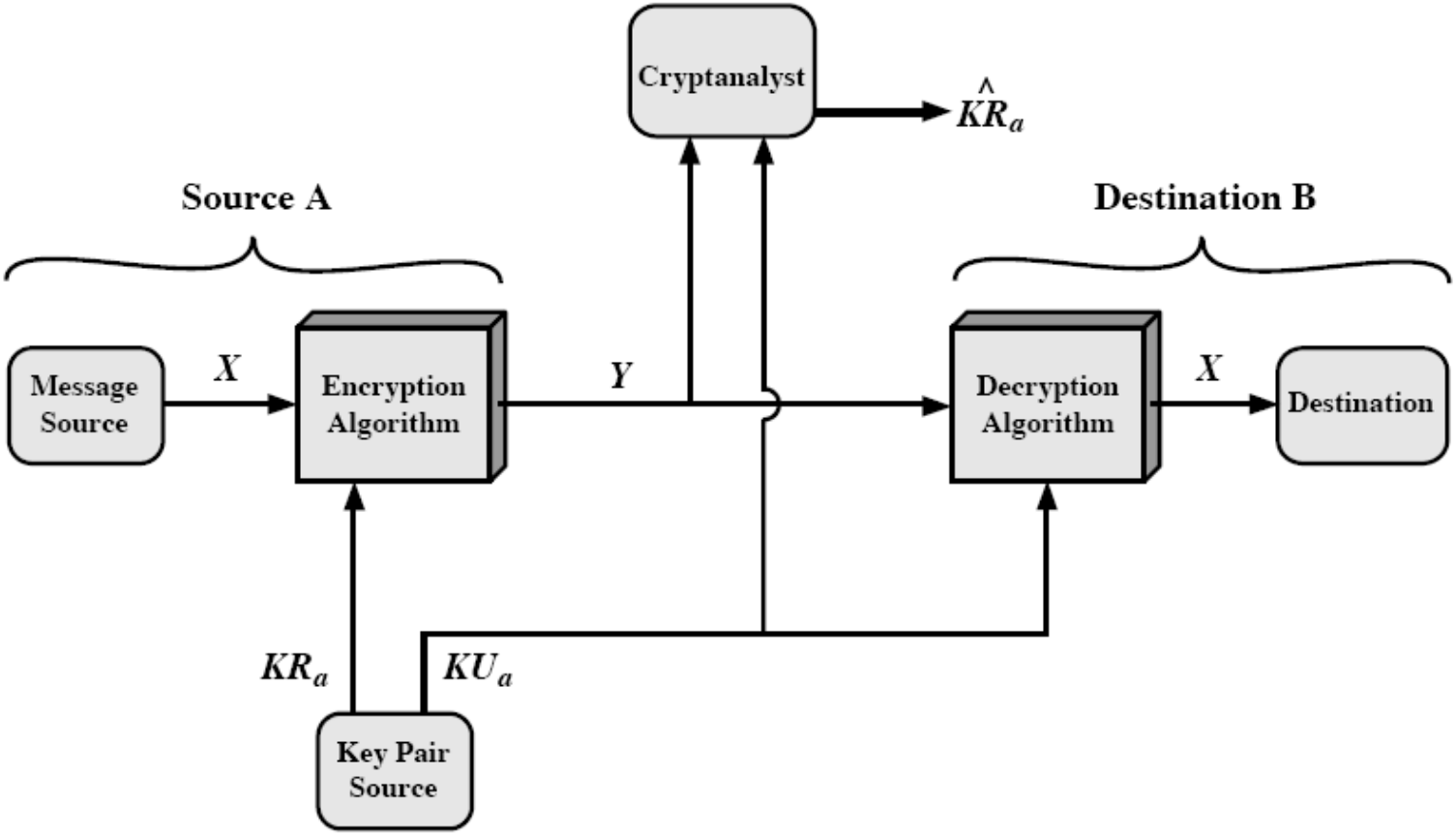
공개키 암호와 RSA

- 공개키 암호 시스템 : 기밀성
  - X : 평문, Y : 암호문, KU_b: b의 공개키, KR_b: b의 개인키



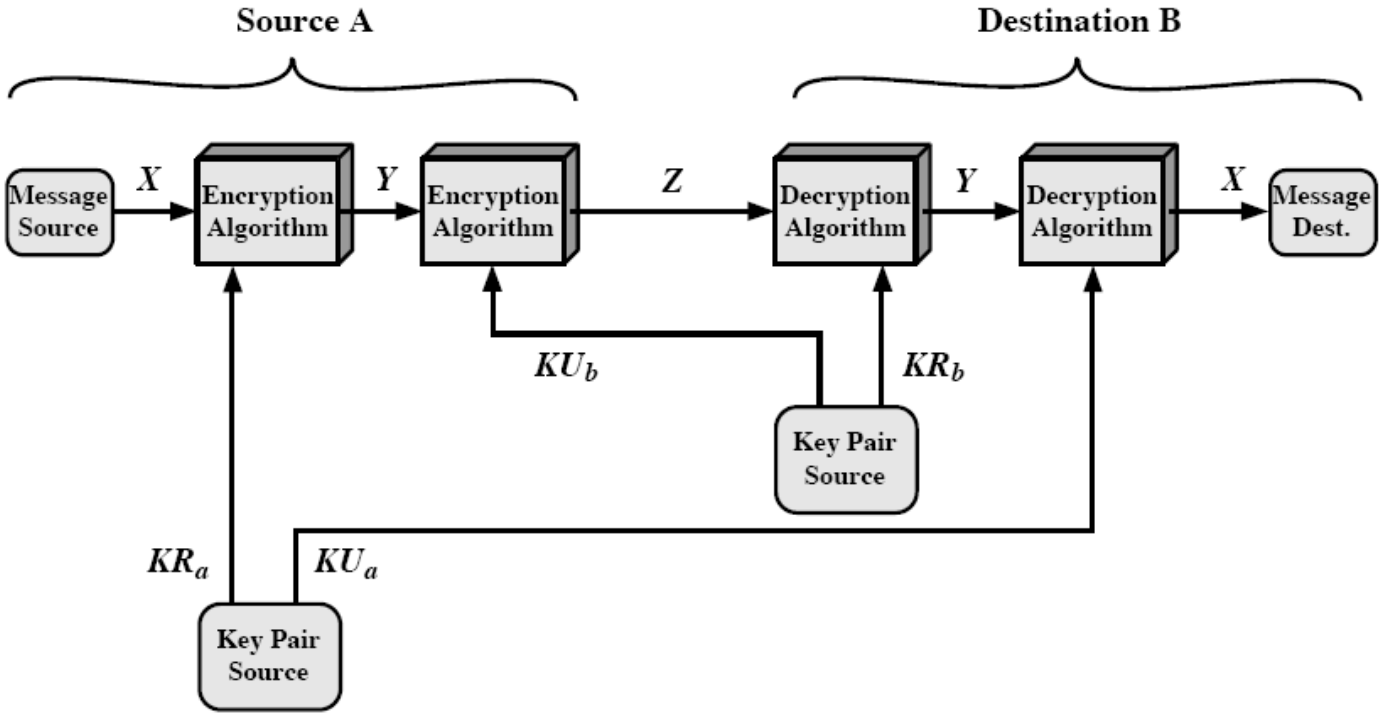
공개키 암호와 RSA

- 공개키 암호 시스템 : 인증
  - X : 평문, Y : 암호문, KU_a: a의 공개키, KR_a: a의 개인키



공개키 암호와 RSA

- 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 암호와 RSA

- 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.

RSA 알고리즘

- 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

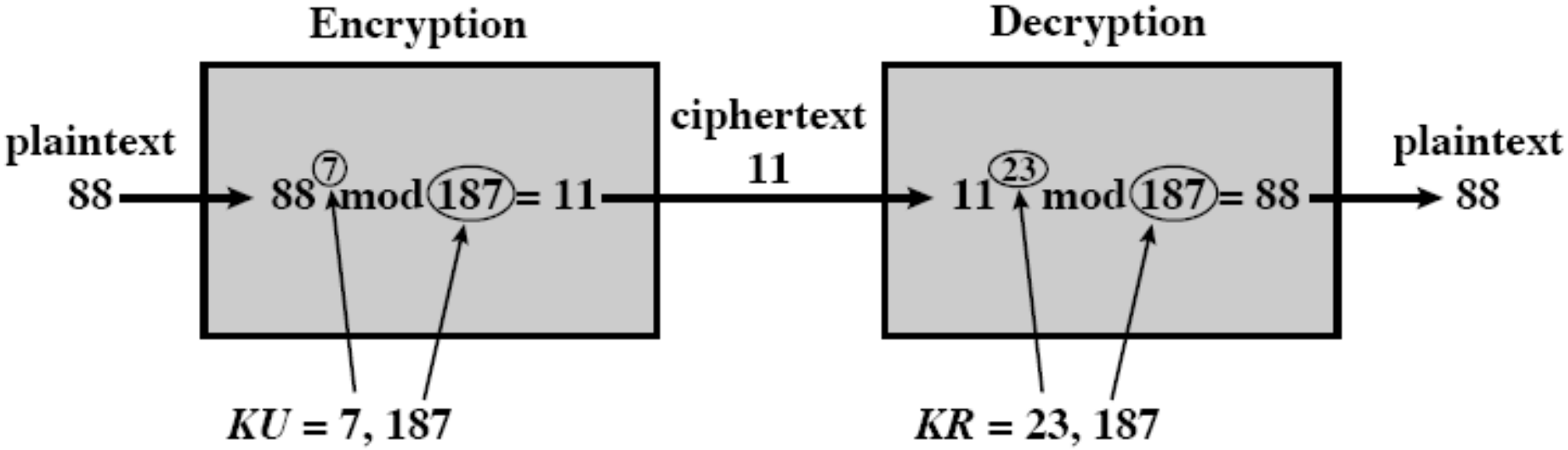
Plaintext:	$M < n$
Ciphertext:	$C = M^e \pmod{n}$

Decryption

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

RSA 알고리즘

- RSA 알고리즘의 예
  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.



RSA 알고리즘

- 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

Q & A