

15장: 정보보안

정보보안

- 개요
- 암호화
- 인터넷 보안
- 악성 소프트웨어
- 컴퓨터 범죄

학습내용

- 정보보안 개요
- 암호화
- 인터넷 보안
- 악성 소프트웨어
- 컴퓨터 범죄

15.1 정보보안 개요

정보 보안

□ 정보의 수집, 가공, 저장, 검색, 송신, 수신 도중에 발생할 수 있는 ‘정보의(변조, 훼손, 유출)등을 방지하기 위한 방법’을 의미


□ 정보 보안의 방법

□ 관리적, 물리적인 방법

▶ 예) 자물쇠, 경비원

□ 기술적, 비물리적 방법

▶ 예) 암호학 기술

공부하세요 :) 

정보 보안의 주요 목표

기밀성, 무결성, 가용성

□ 기밀성

- 정보를 저장하거나 전송하는 과정에서 정보 원본을 권한이 없는 사용자에게 노출되지 않도록 보장하는 것
- 즉, 정보의 비밀 보장

□ 무결성

- 정보를 주고받는 과정에서 불법적으로 (생성, 변경, 삭제되지 않도록 원본을 유지하는 것;
- 허락되지 않은 사용자가 정보를 수정 할 수 없도록 하는 것

□ 가용성

- (권한이 있는 사용자가) 필요로 하는 정보는 필요한 시점에 접근하거나 사용할 수 있도록 보장하는 것

(기밀성, 무결성, 가용성)

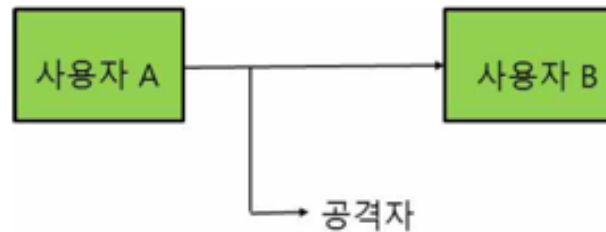
보안 위협

□ 보안 목표, 즉 기밀성, 무결성, 가용성을 위협하는 제반 행위를 의미

□ 기밀성에 대한 위협: (스누핑, 트래픽 분석)

□ 스누핑 = ~~스누핑~~

▶ 공격자가 다른 사람 데이터를 몰래 훑쳐보는 행위



□ 트래픽 분석

▶ "특정 시스템이나 네트워크에서 전송되고 있는 트래픽을) 관찰하고 분석하여 의미 있는 정보를 얻는 행위"

보안 위협

□ 무결성에 대한 위협: 변경, 위장, 재연 공격

□ 변경 공격

- ▶ 원본 메시지를 변조

변경, 위장, 재연



□ 위장 공격

- ▶ 공격자가 처음부터 네트워크에서 '특정 사람'으로 가장하여 수신자를 속이는 행위
- ▶ ARP 스누핑 등 속이기
- ▶ DNS 해킹하여 은행인 척하기

(Mac 주소를 속이는 것)



□ 재연 공격

- ▶ (권한이 있는 사용자가) 사용한 메시지 원본을 공격자가 어떤 방법으로 획득하고 그 메시지를 다시 사용하는 방법

보안 위협

□ 가용성에 대한 위협: 서비스 거부 공격

- 권한 있는 사용자가 사용하고자 할 때는 언제든지 정보에 접근 가능해야 함
- 서비스 거부 공격(또는 DDoS 공격)
 - ▶ 시스템을 공격해 해당 시스템의 자원을 부족하게 해서, 사용자가 자원에 대한 서비스를 받지 못하게 함
 - ▶ 예를 들어, 특정 서버에 대해서 수많은 접속 시도를 만들어 다른 사용자가 정상적으로 서비스 이용을 하지 못하게 함
 - ▶ 인터넷 사이트 또는 서비스의 기능을 일시적 또는 무기한으로 방해/중단을 초래

보안 서비스

데이터 기밀성
디지털 서명
인증
접근 제어
무인 방지
항복화

트래픽 패싱
구동 제어
무인-

- 데이터 기밀성
 - (스누핑과 트래픽 분석 공격) 같은 데이터 노출 공격으로 부터 데이터를 보호하는 서비스
- 데이터 무결성 - 디지털 서명(전자서명)
 - 공격자의 불법적인 (데이터 변경, 데이터 삽입, 데이터 삭제) 등으로 부터 데이터를 보호하는 서비스
- 인증
 - (연결을 중심으로 하는 통신에서는) 통신을 연결할 때, (송신자나 수신자에 대하여 인증).
 - 연결을 중심으로 하지 않는 통신에서는 데이터의 출처를 인증
- 접근 제어
 - 권한이 없는 사용자의 접근으로부터 데이터를 보호
- 부인 방지
 - 데이터를 주고받는 (송·수신자가 송수신 사실에 대해서) 부인 못하게 하는 보안 서비스

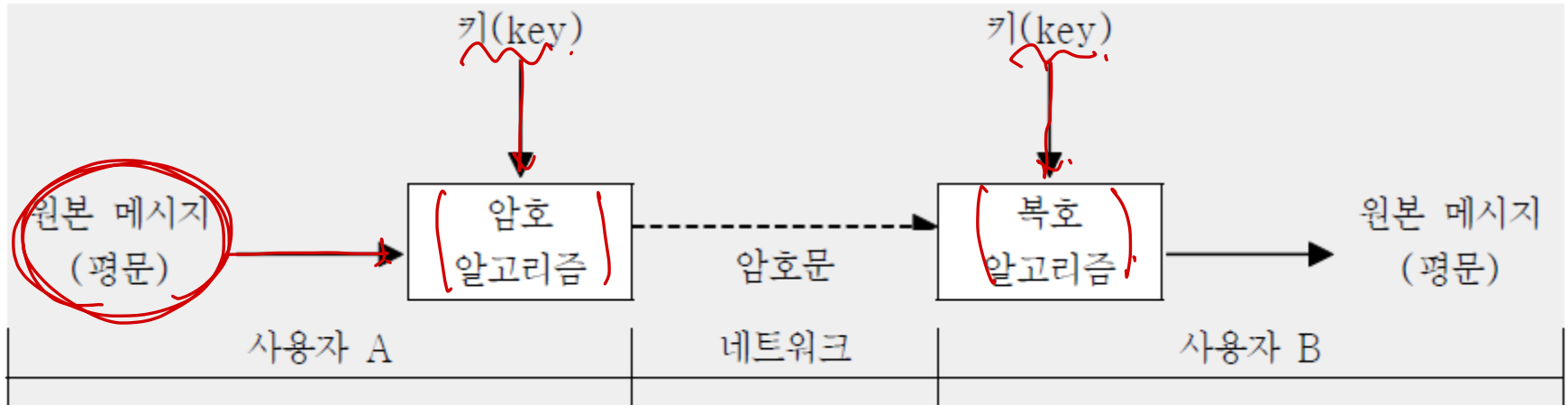
보안 기법

- 암호화.
- 데이터 무결성
 - 디지털 서명
- 인증.
- 트래픽 패딩 → 실제 데이터가 아닌 임의의 데이터를 네트워크에 흘림
- 라우팅 제어
- 공증
- 접근제어

15.2 암호화

암호 개요

□ 일반적인 암호 체계



□ 암호의 목적?

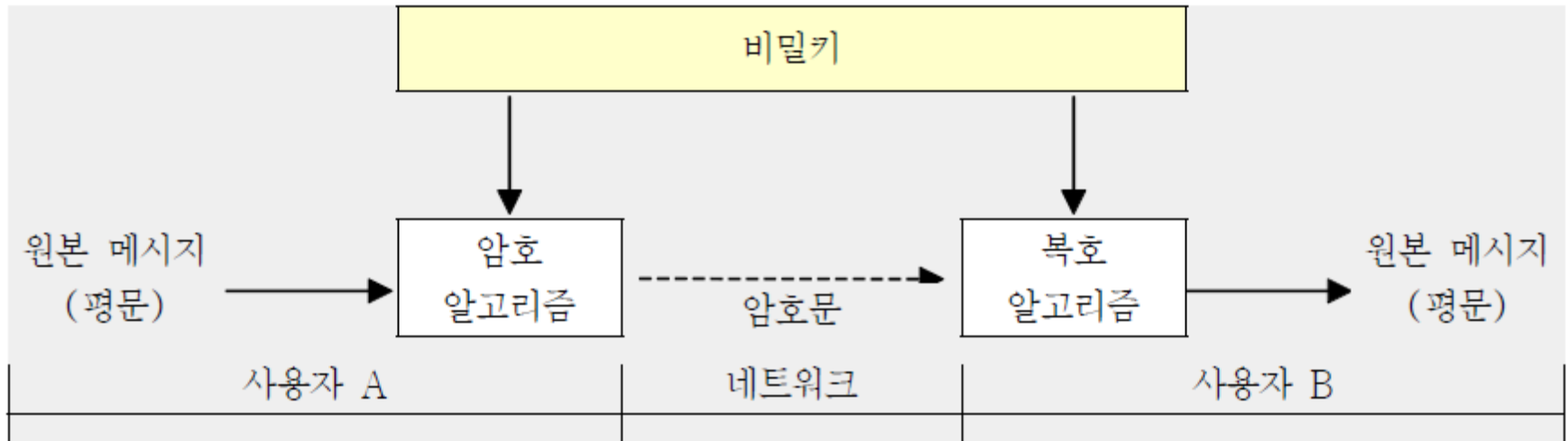
□ ...

□ 암호의 분류: (대칭키^①(symmetric) 암호), (공개키 암호^②)

비밀키 *공개키 + 비밀키*

비밀키 암호

- 송신자와 수신자는 **동일한 비밀키 공유** (**대칭키**, **비밀키**, 공유키, 동일키, 싱글키, 공통키 등등으로 불림)
- 비밀키 암호의 개념



예제: 덧셈을 활용한 비밀 키 암호

□ 암호 알고리즘: 암호문 = (평문 + 키) mod 26

□ 예) 송신자: 메시지 “korea”를 비밀키 k로 암호화

□ 영문자 a는 정수 0, b는 정수 1,..., z는 정수 25로 표현

원본 문자:	k (→ 10)	암호화:	<u>(10 + 10)</u> mod 26	암호문:	20 → u
원본 문자:	o (→ 14)	암호화:	(14 + 10) mod 26	암호문:	24 → y
원본 문자:	r (→ 17)	암호화:	(17 + 10) mod 26	암호문:	01 → b
원본 문자:	e (→ 04)	암호화:	(04 + 10) mod 26	암호문:	14 → o
원본 문자:	a (→ 00)	암호화:	(00 + 10) mod 26	암호문:	10 → k

예제: 덧셈을 활용한 비밀 키 암호

- 복호 알고리즘: $\text{평문} = (\text{암호문} - \text{키}) \bmod 26$
- 수신자: 암호문 “uybok”를 비밀키 k (10)로 복호화
 - 영문자 a는 정수 0, b는 정수 1,..., z는 정수 25로 표현

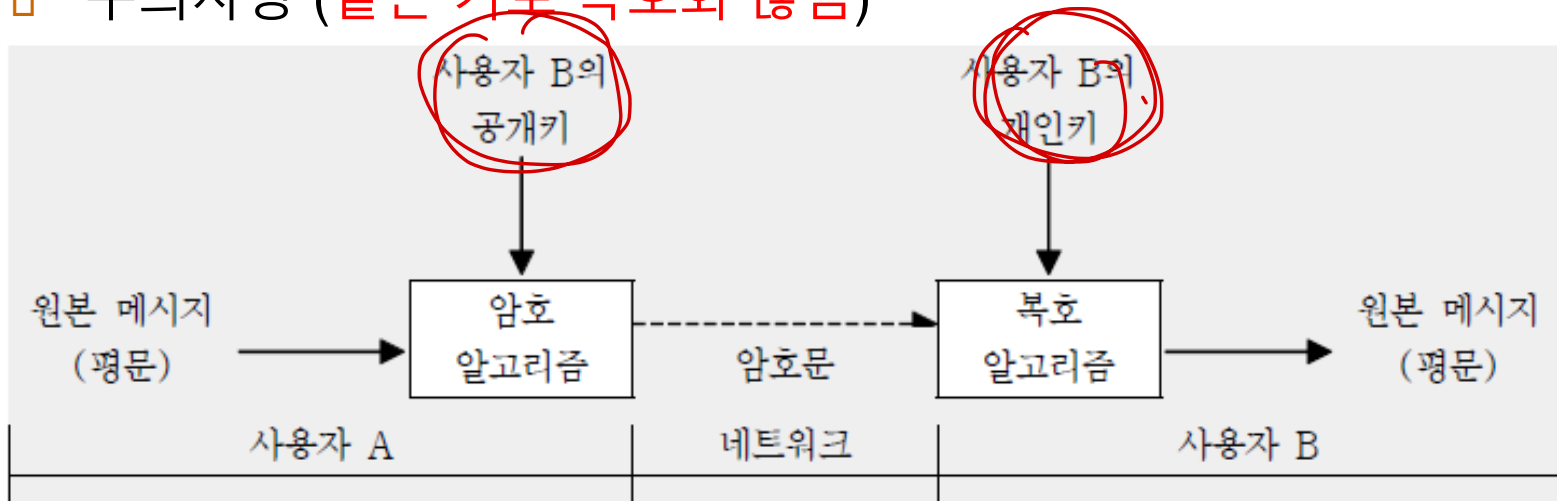
암호문:	u ($\rightarrow 20$)	복호화:	$(20 - 10) \bmod 26$	원본:	10 \rightarrow k
암호문:	y ($\rightarrow 24$)	복호화:	$(24 - 10) \bmod 26$	원본:	14 \rightarrow o
암호문:	b ($\rightarrow 01$)	복호화:	$(01 - 10) \bmod 26$	원본:	17 \rightarrow r
암호문:	o ($\rightarrow 14$)	복호화:	$(14 - 10) \bmod 26$	원본:	04 \rightarrow e
암호문:	k ($\rightarrow 10$)	복호화:	$(10 - 10) \bmod 26$	원본:	00 \rightarrow a

비밀키 암호의 유형

- 비밀키 암호는 스트림 암호 또는 블록 암호로 구현됨
- 스트림 암호
 - (비트 또는 바이트 크기로 암호화)
 - (하드웨어 구현이 용이, 속도가 빠르다는 장점 때문에 무선통신에서 많이 사용됨).
 - Ex) RC4, ARIA (한국)
- 블록 암호
 - 데이터를 일정한 크기 128bit, 256bit 등의 블록 단위로 암호화
 - Ex) AES
- 비밀키 장점 : 빠르다, 안전하다
- "비밀키 문제점" : 송수신자가 동일한 키를 가지고 있어야 함
→ 유통이 어렵다

공개키 암호

- 비대칭키 암호라고도 함
- 암호화, 복호화에 서로 다른 키(공개키, 개인키)가 각각 사용됨
- 공개키 암호의 개념
 - 송신자는 메시지 수신자의 공개키로 평문을 암호화
 - 수신자는 수신된 암호문을 자신의 개인키로 복호화
 - 주의사항 (같은 키로 복호화 않됨)



예제: RSA 알고리즘

□ 대표적인 공개키 암호 알고리즘

□ (키생성, 암호화, 복호화 과정)으로 구성

□ 키 생성 : 공개키 : (n, e), 개인키 : (n, d)

(1) 두 개의 소수 p, q를 선택

(2) p와 q의 곱 $n(=p \times q)$ 을 계산

(3) e 와 d를 생성, 이때 e와 d는 역수의 관계를 가짐;

$$e \cdot d \equiv 1 \pmod{(p-1)(q-1)}$$

$$e \cdot d \pmod{(p-1)(q-1)} = 1$$

$e = 1$

$e \cdot d \equiv 1$
 $e \cdot d \pmod{(p-1)(q-1)} = 1$

$n = 33$
 $p = 3 \quad q = 11$
 $\phi(n) = 2 \times 10 = 20$
 $\forall e \in \phi(n) \quad e = 3, 7, 9, 11, \dots$
 $e \cdot d \pmod{\phi(n)} = 1$
 $d = 7$

□ RSA 암호화 : 암호문 = 메시지^e (mod n)

□ RSA 복호화 : 메시지 = 암호문^d (mod n)

예제: RSA 알고리즘

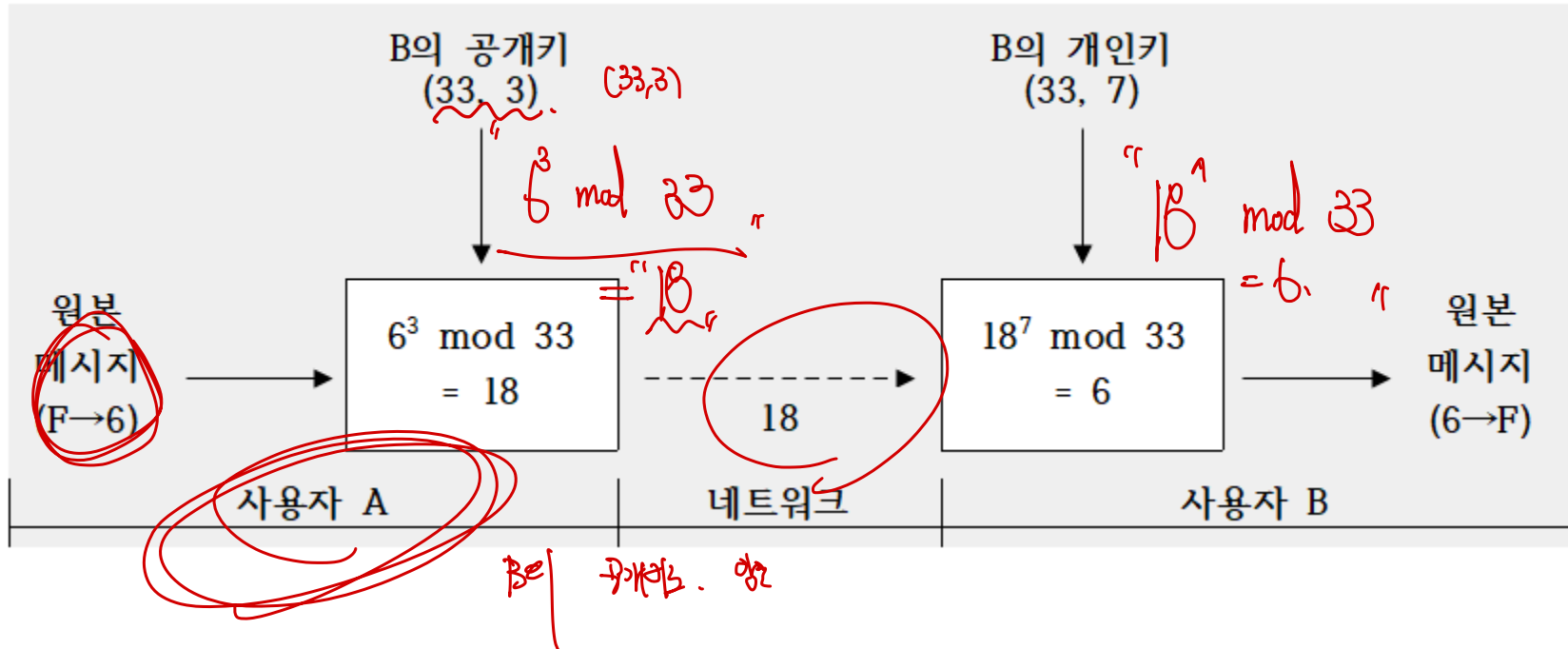
□ 키생성 : 공개키 : $(n=33, e=3)$, 개인키 : $d=(33, 7)$

(1) $p=11, q=3$ 를 선택 (2) $n=p \times q=33$ 을 계산

(3) 오일러 피 함수에 해당되는 $\phi(N) = (P-1)(Q-1) = 20$

(4) $0 < e < \phi(N)$ 이며 $\phi(N)$ 와 '서로소'가 되는 e 선택, $e = 3, 7, 9, 11, 13$

(3) $e=3$ 와 $d=7$ 를 생성 $e * d \bmod (\phi(N)) = 1$ 이 되는 수 $d=7$ 선택



비밀키 암호 vs 공개키 암호

□ 비밀키 암호 방식

- (암호화, 복호화)에 사용되는 키가 동일
- 계산속도 빠름, 심지어 hw로 가능해.
- 송신자와 수신자가 동일한 비밀키를 어떻게 공유할 것인가?
(키분배 문제) 공개키 암호 방식을 해결하자!

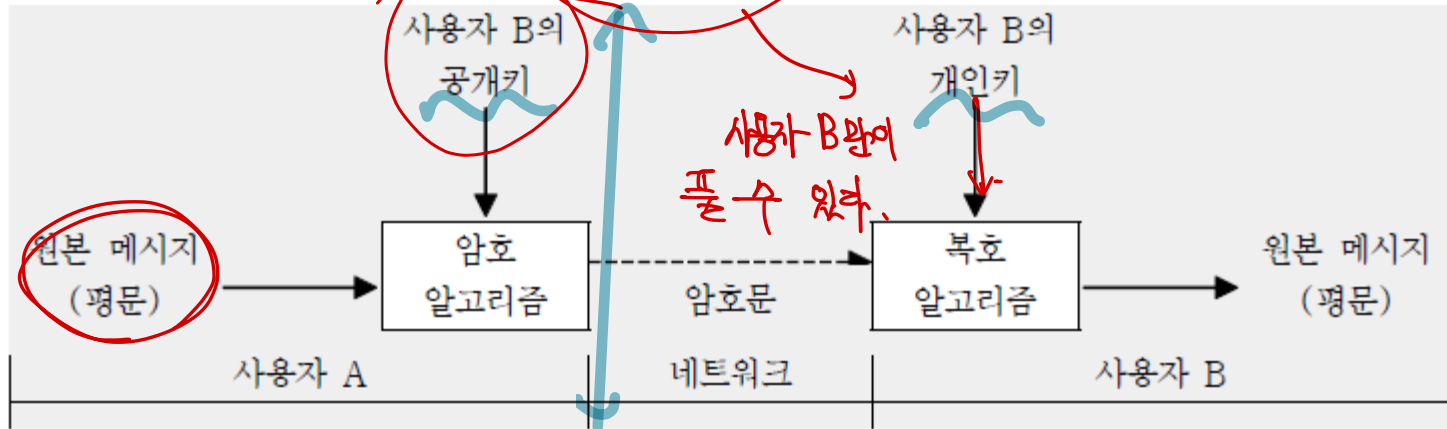
□ 공개키 암호 방식

- (암호화, 복호화)에 사용되는 키가 다름.
- 계산속도 느림
- 사전에 암호키 공유 불필요

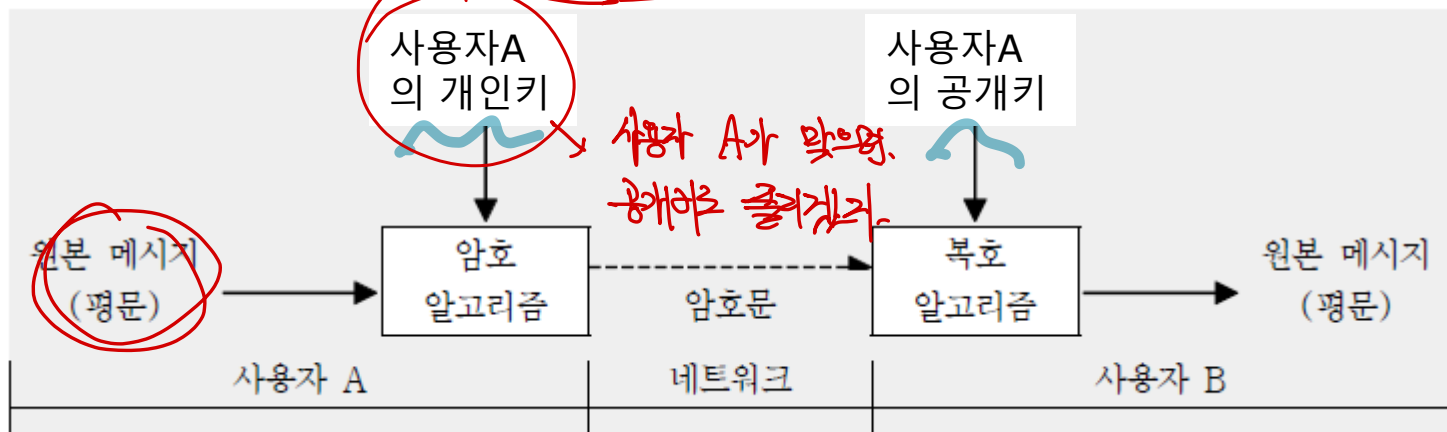
□ 공개키 암호방식을 통하여 비밀키를 교환하면 되겠네..

공개키

비밀키 암호 방식 - 수신자 인증



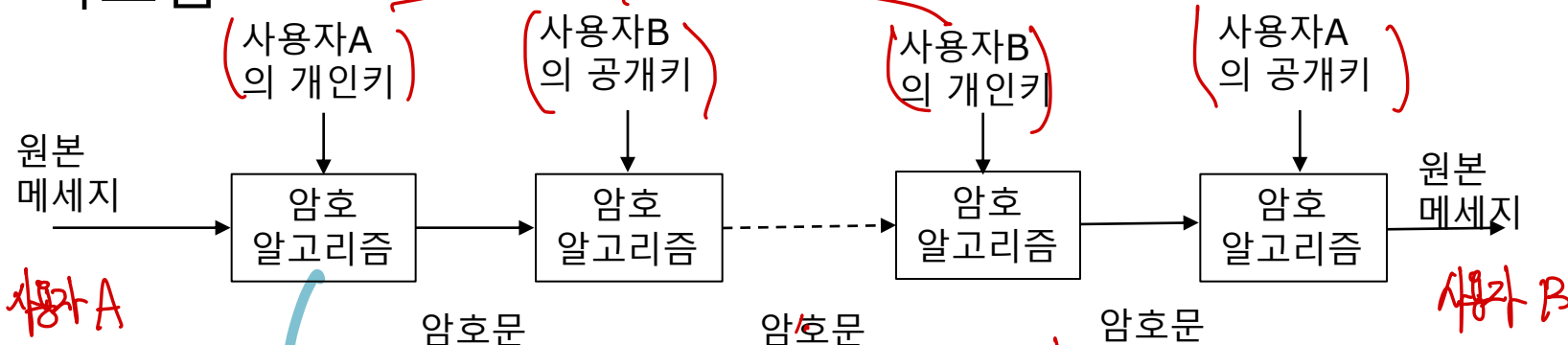
비밀키 암호 방식 - 송신자 인증



송수신자 인증된 통신

A (A의 개인키) → B의 공개키 → (B의 개인키) → A의 공개키 B

- 통신의 기밀성, 무결성, 상호인증, 통신사실 부인방지 확보됨



- 이제 (동일한 대칭키)를 생성해서 비밀리에 송신하여 공유하면 되겠네 - 대칭키의 키 공유 문제 해결

- 대량 통신은 비밀키 통신으로

“대칭키 문제” = 하이브리드형

⇒ “한계점은 십자 깨달음”

공개키 통신에서

□ 통신의 (기밀성, 무결성, 상호인증, 통신사실 부인방지) 확보됨

□ 그런데....

□ ~~내가 통신한 것은 맞는데.... 그 계약서는 내가 보낸 것이 아니야~~~~

□ 네이버가 끝내 주는 자료를 공개했다. 내가 보내줄게

□ 그런데 보낸 자료가 원본 맞니?/주요자료는 원 저작자 사인해서 보내라

→ 인증이 필요..!

원 저작자 사인 → 인증.

디지털 서명

- 공개키 암호에서만 제공할 수 있는 기능

- 디지털 서명의 용도

- '메시지(를 보낸 사람이 A가 확실한가?)' 또는

- 메시지가 '전송 도중에 변경되지 않았는가?' 와 같은 검증이 필요할 때 사용될 수 있는 기술

- 디지털 서명 과정

- 자료 생성자는 생성 자료의 지문을 개인키를 사용해서 암호화한 값(서명값) 자료와 묶음(서명)

- 자료 사용자는 (생성자의 공개키로) 서명값 복호화 문서지문 획득

- 원본 자료의 지문과 복호화한 지문의 일치 여부 검사



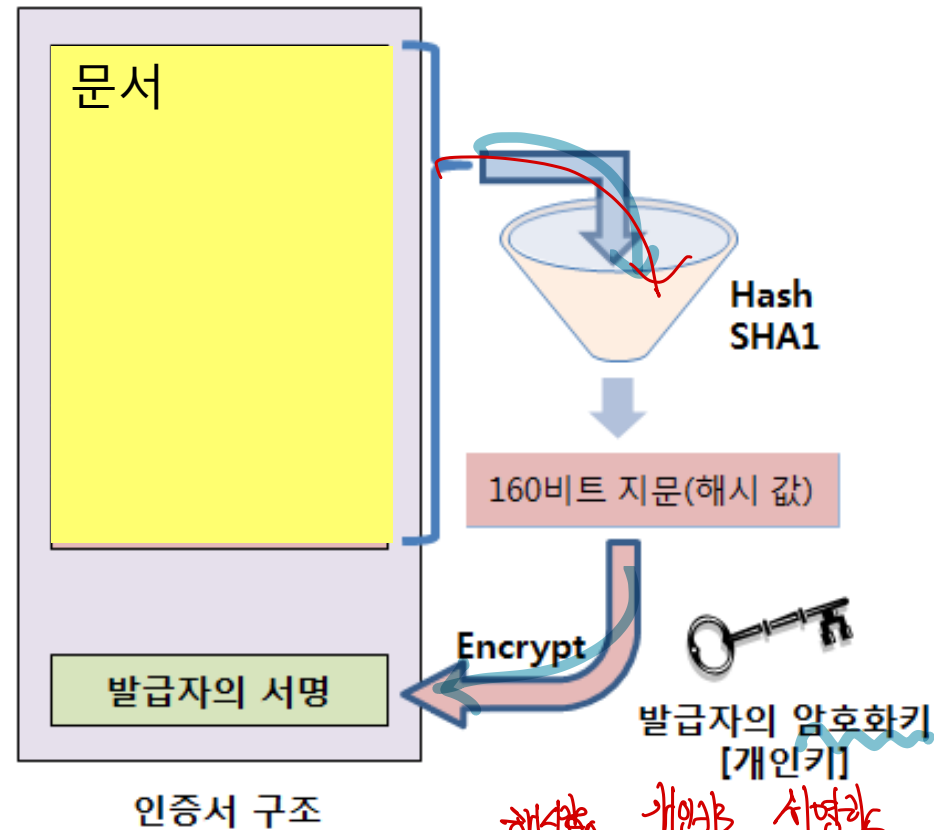
← 해커는 서명을 볼 수 있음

디지털 서명 - 문서의 지문(문서의 해시 값)



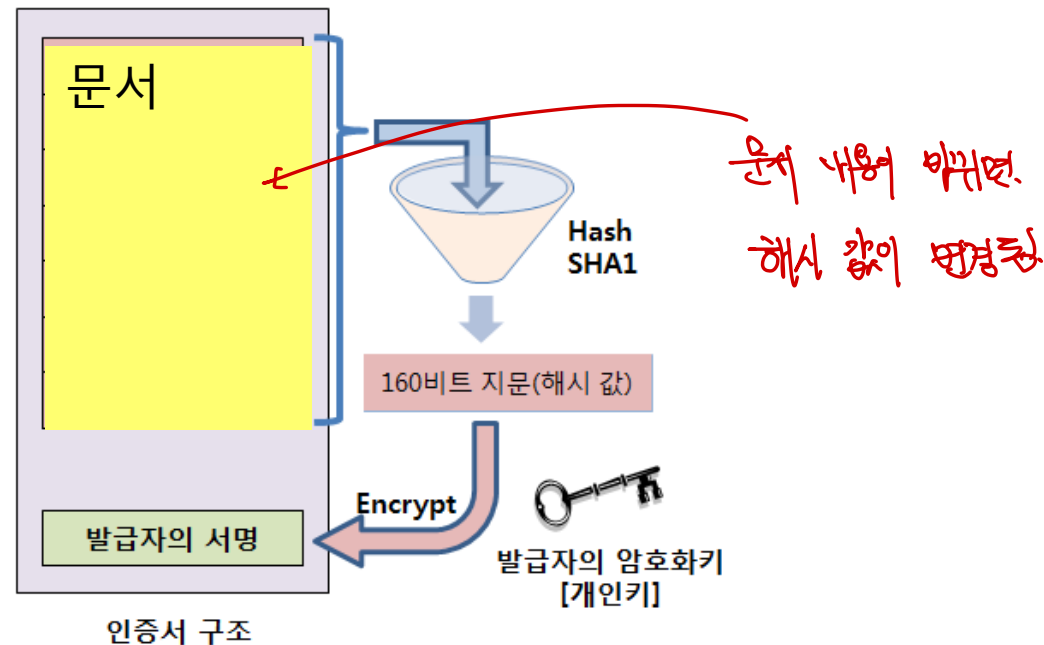
- 문서와 문서의 지문을 같이 묶음
- 해커 :문서를 바꾸고 지문도 다시 바꾸면 되겠네.....

전자서명



- 문서의 지문을 문서생성자의 개인키로 암호화하여 묶음

전자서명



- 문서생성자가 아닌 사람이
- 문서의 내용을 변경하면 해시 값이 변경됨,
- 변경된 해시 값을 개인키로 암호화해야 하지만
- 개인 키가 없음.

서명의 필요성

홍길동

국민은행

통신합시다. 공개키 주세요, 내건 여깁어요 ~~~

홍길동 ^{상인가 응답} 공개키 받았어, 내건 여기있어 ~ 뭐해줄까?

네.. 100억만 대출해주시 ~~~

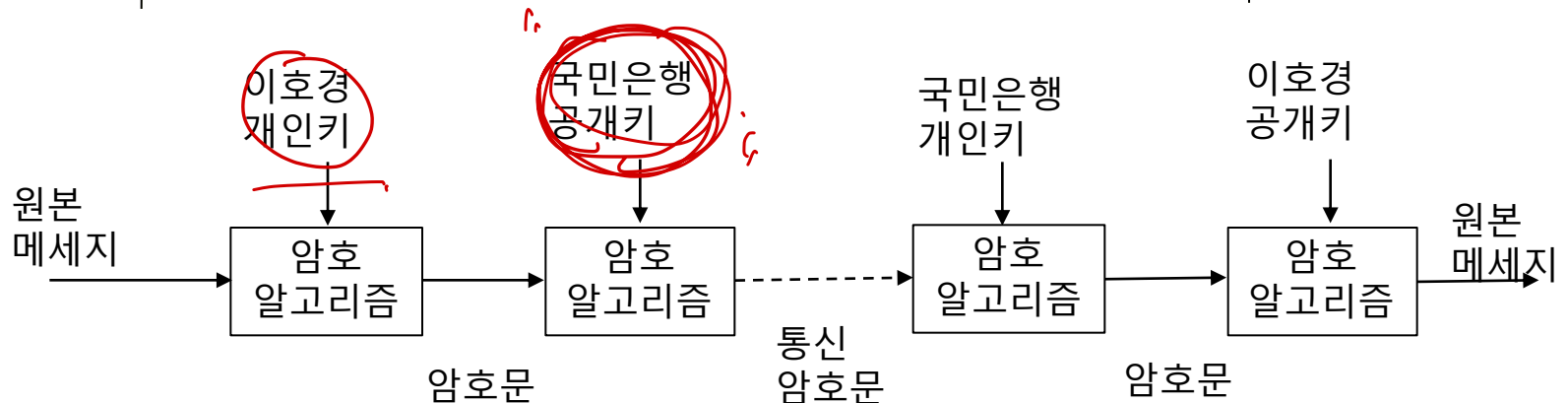
차용증 문서 작성해서 보내줘 ~

차용증 문서 여기있다 돈 줘 ~

옛다 돈 머니~

차용증 기한 다 됐다. 돈 갚아라 !!

차용증? 내가 쓴것 아니야 무슨돈?? 그 때 통신한 것은 맞는데 차용증은 쓴 적 없어 도둑놈아 !!!



서명의 필요성

홍길동

국민은행

통신합시다. 공개키 주세요, 내건 여깁어요 ~~~

홍길동 공개키 받았어, 내건 여기있어 ~ 뭐해줄까?

네.. 100억만 대출해주셔 ~~

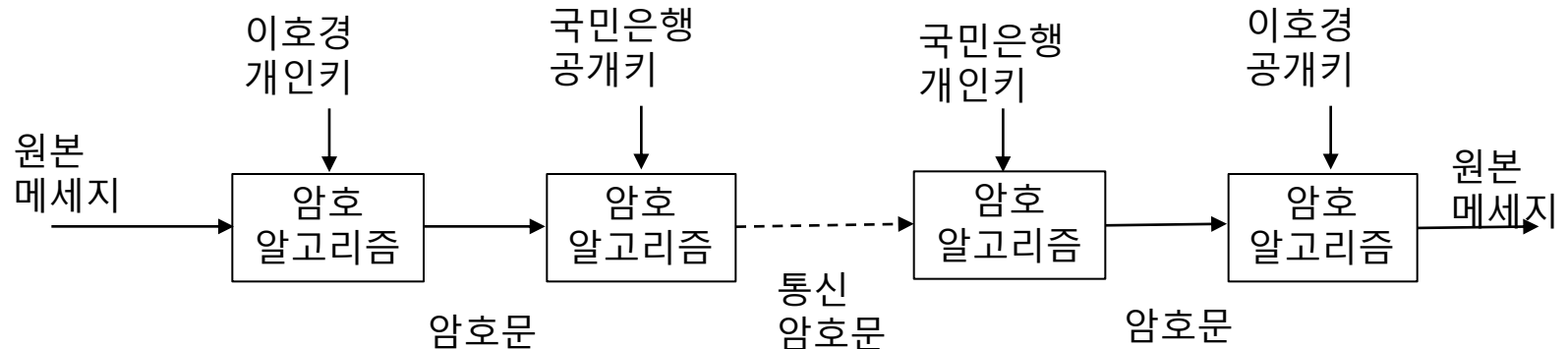
차용증 문서 작성해서 전자서명 해서 보내줘 ~

서명한 차용증 문서 여기있다 돈 줘 ~

옛다 돈 머니~

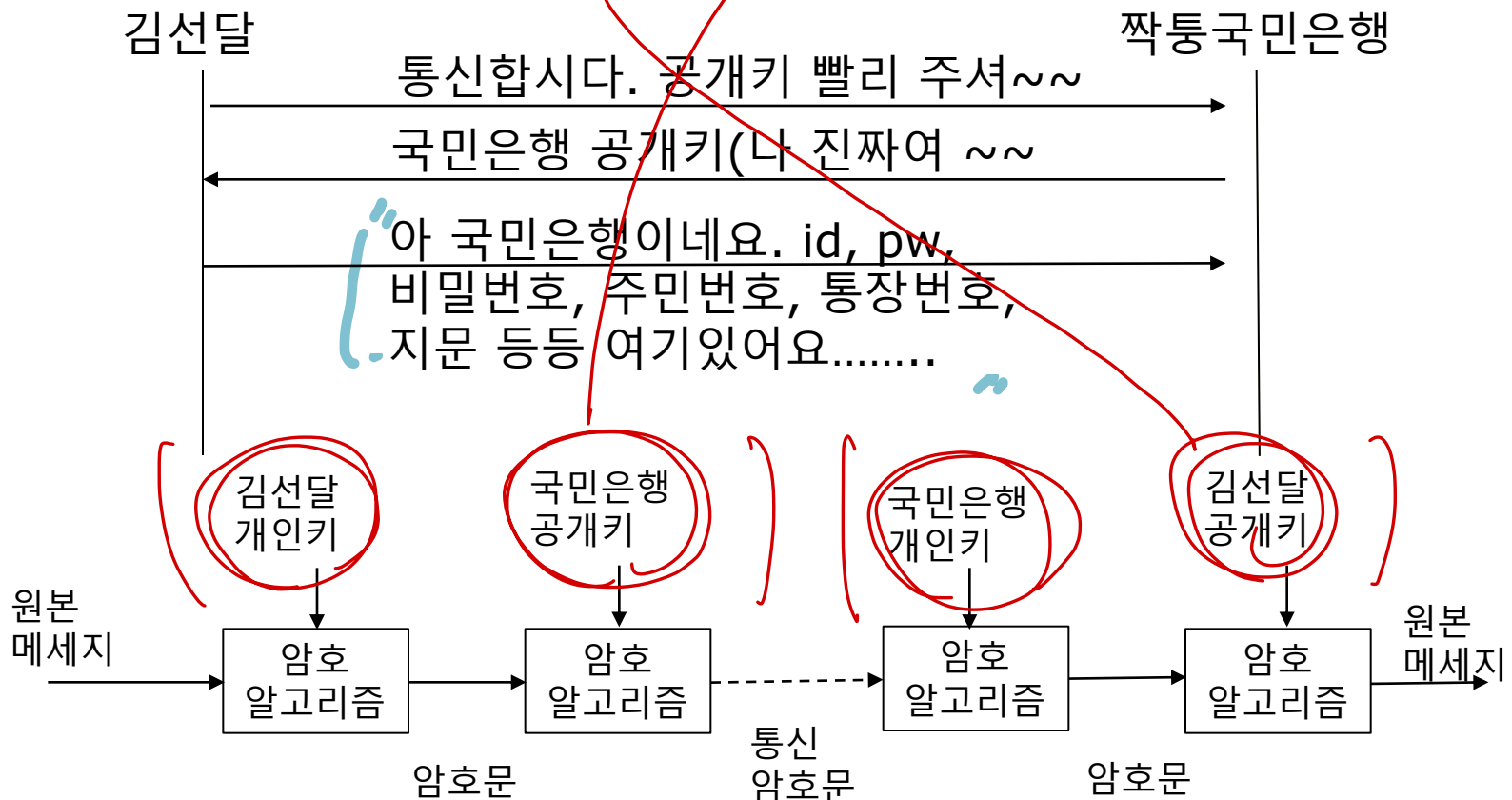
차용증 기한 다 됐다. 돈 갚아라 !!

헐 내 공개키로 풀리니 내가 작성한 문서 맞네..갚을게요



공증의 필요성

- 국민은행에 접속하기 위해 은행의 공개키를 알아야함
- 국민은행은 김선달의 공개키를 알아야 함



공증의 필요성

봉이 김선달

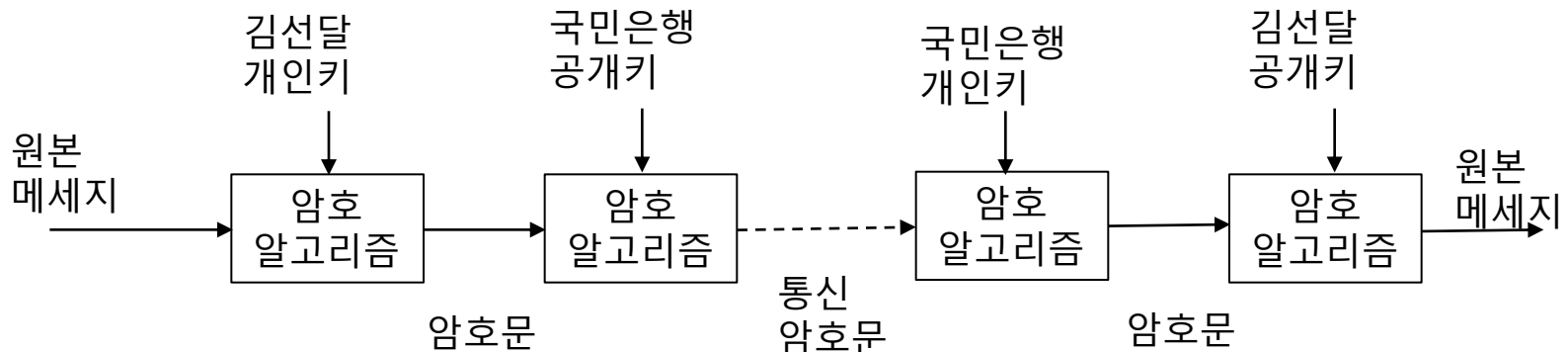
국민은행

통신합니다. 공개키 주세요, 내건 여깁어요 ~~~

김선달 공개키 받았어, 내건 여기있어 ~ 뭐해줄까?

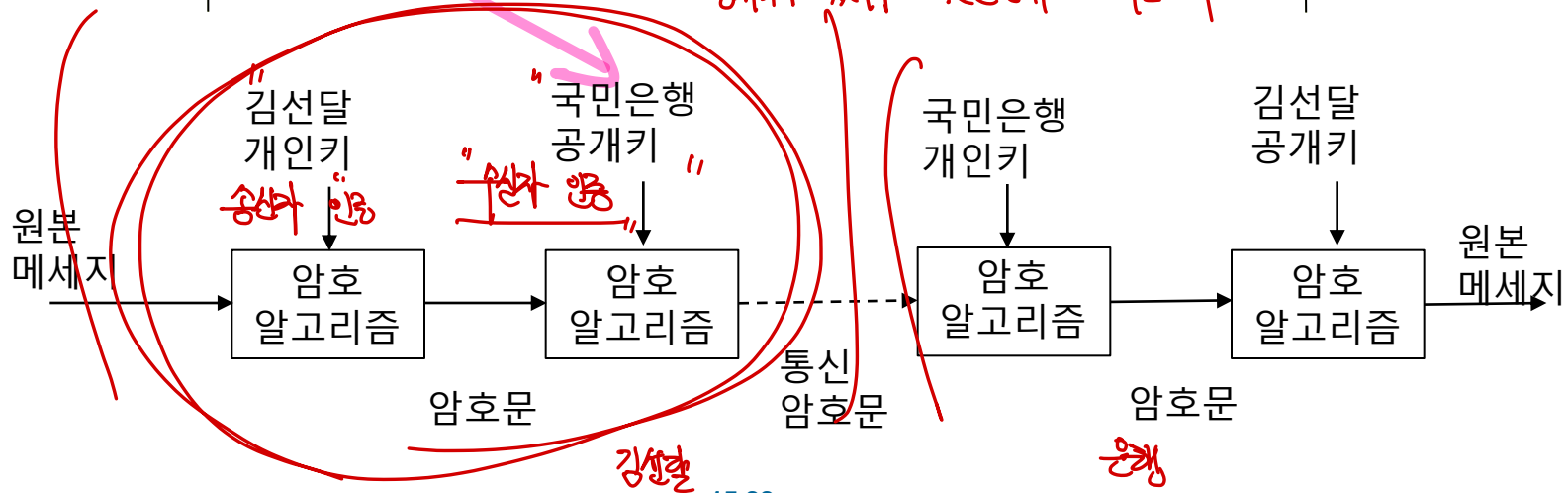
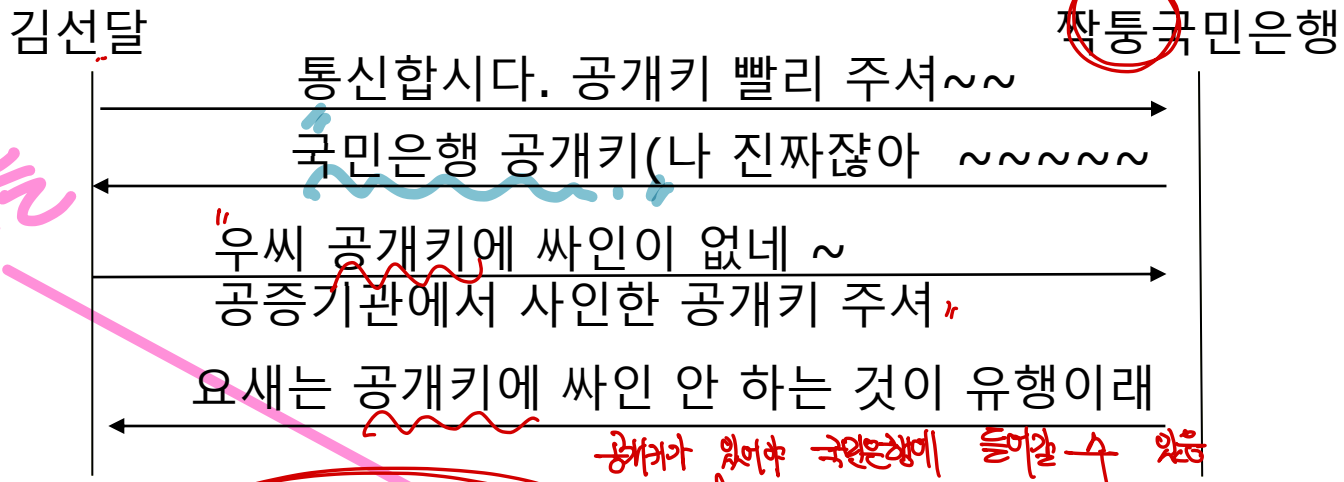
네.. 100억만 대출해서 이쪽 대포통장계좌로 입금해주셔 ~~

그래 어차피 이 통신은 홍길동이 확실하니까~~~
입금했당 ~~

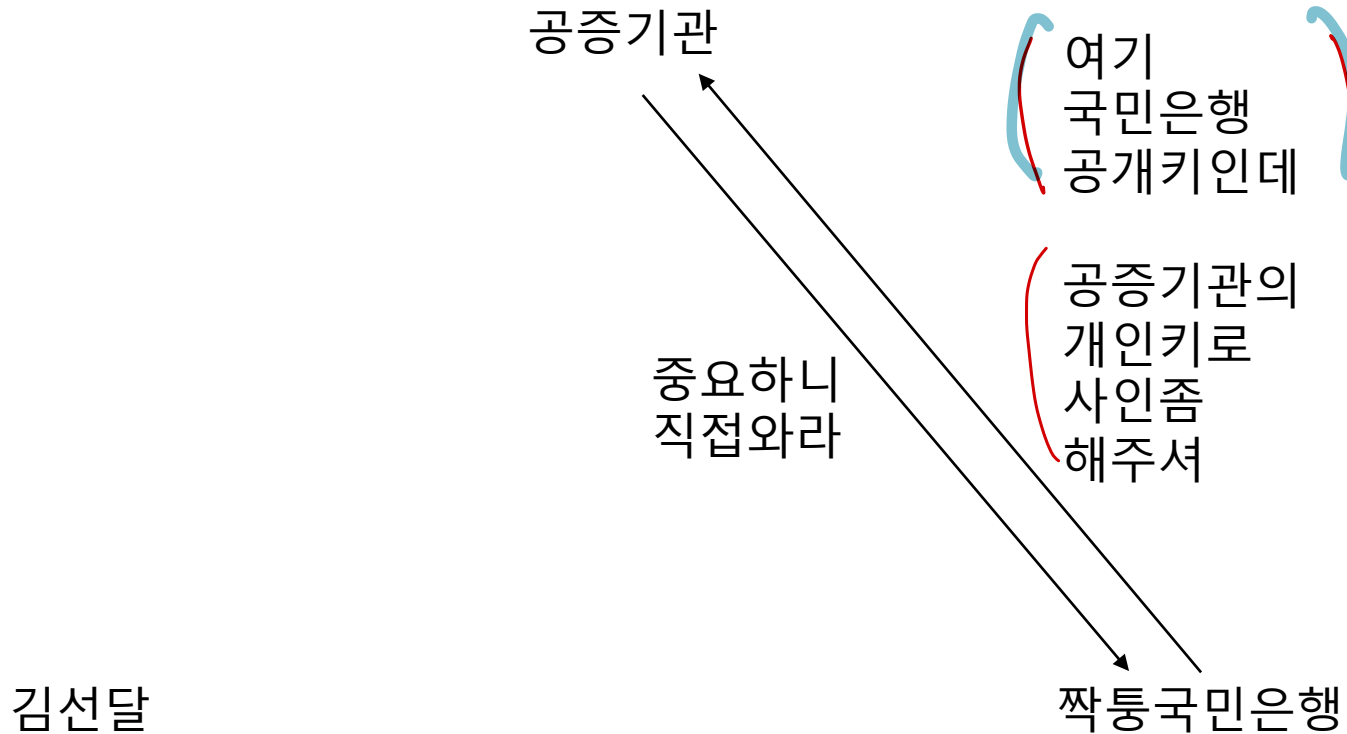


공증의 필요성

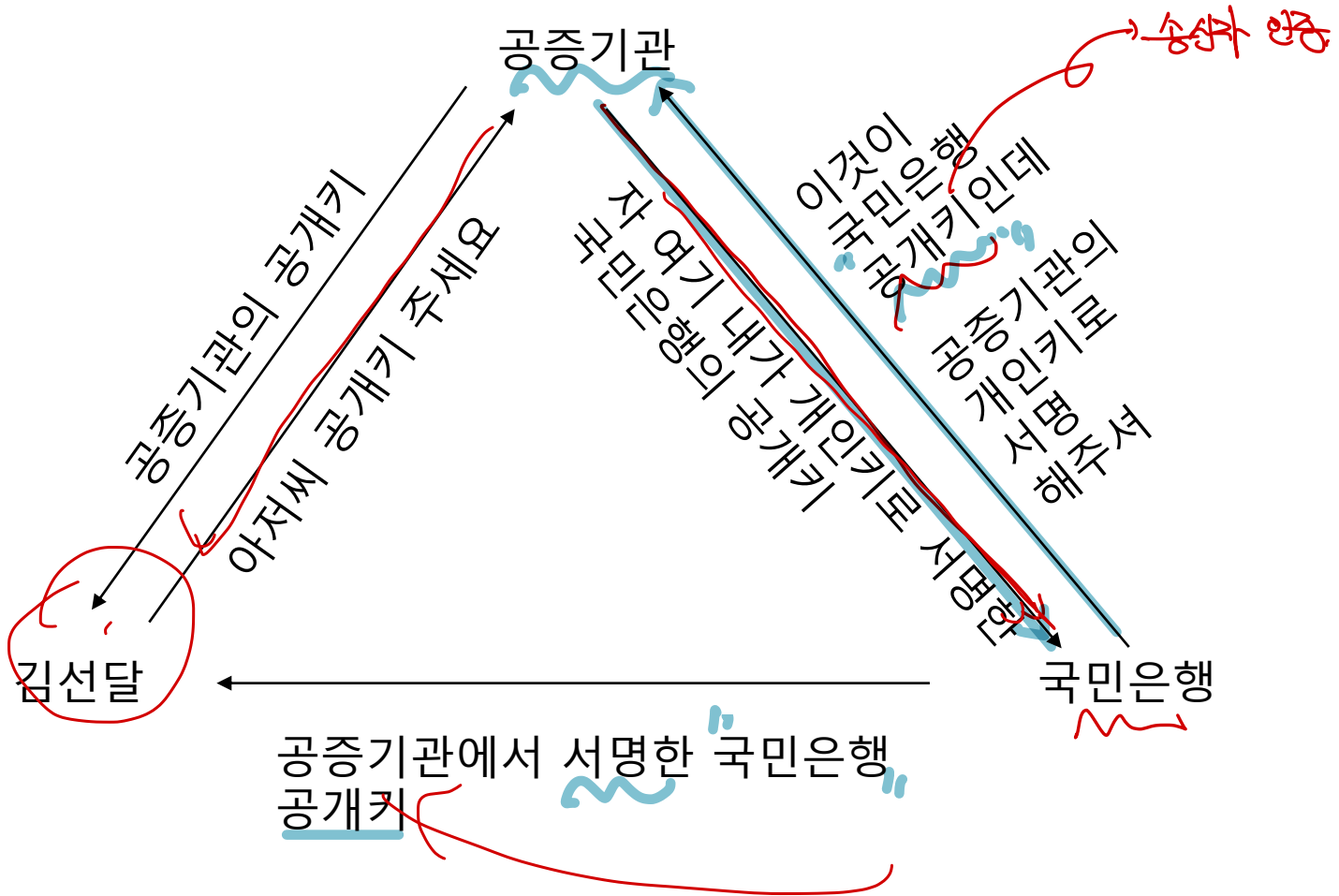
- 국민은행에 접속하기 위해 (은행의 공개키)를 알아야함
- 국민은행은 이호경의 공개키를 알아야 함



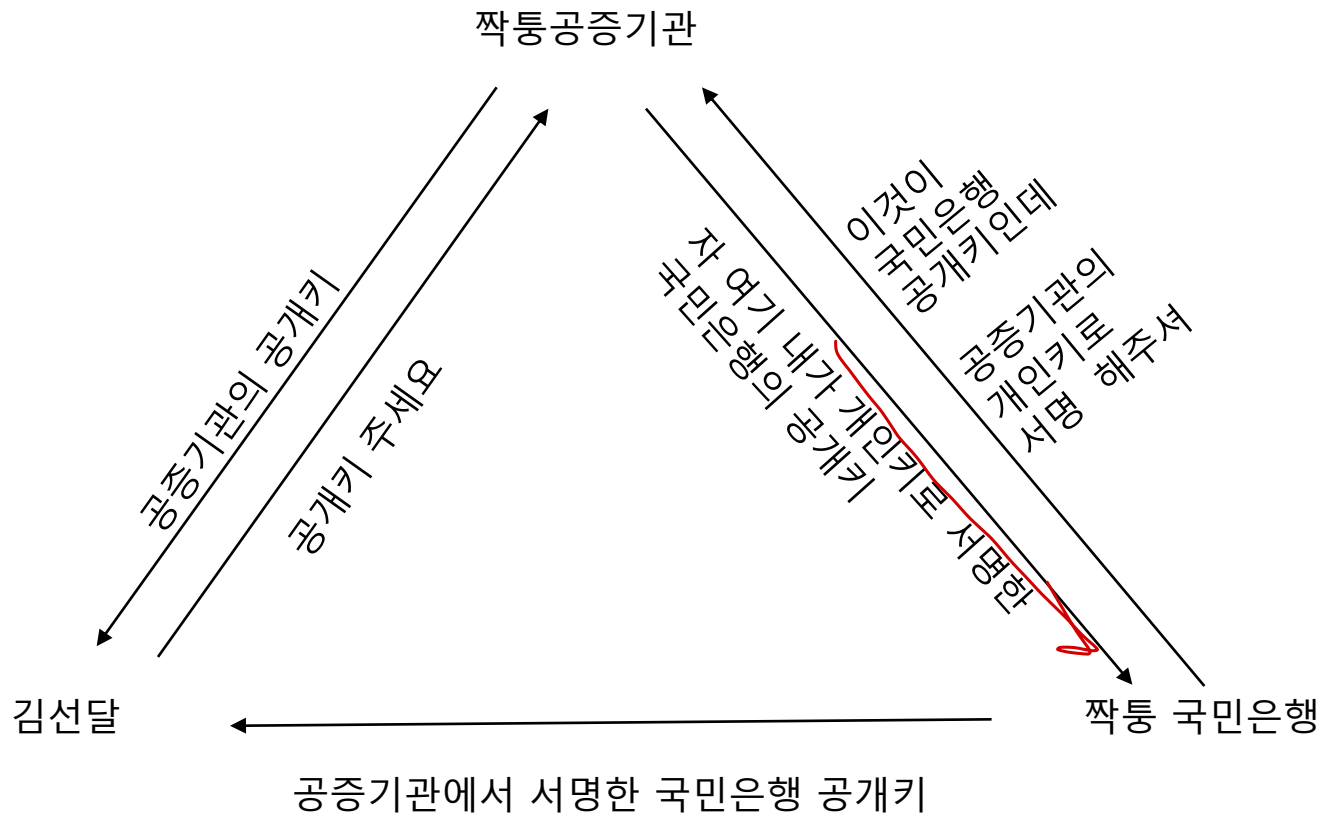
짜통의 공개키는 공증기관의 서명을 받을 수 없음



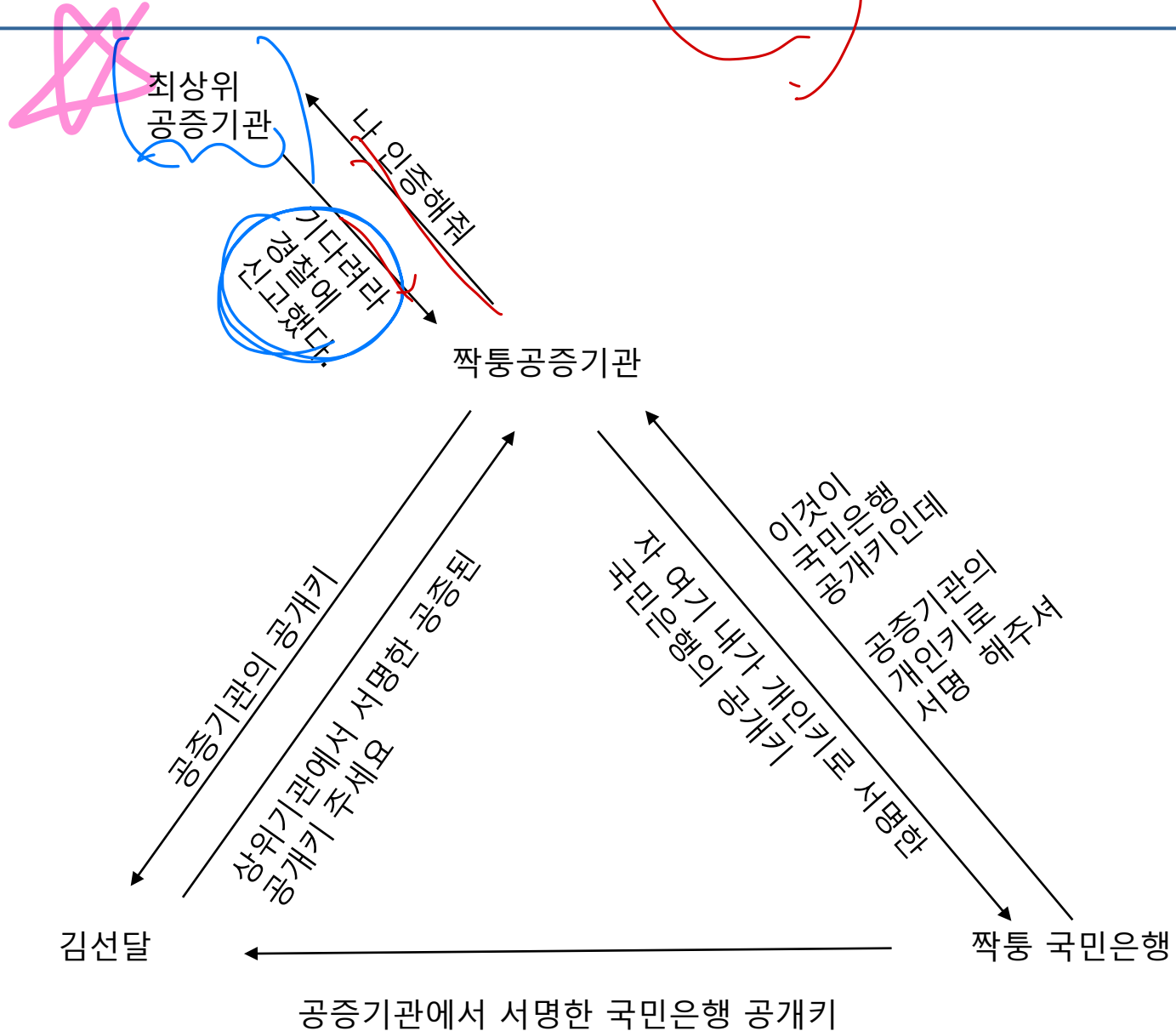
공증

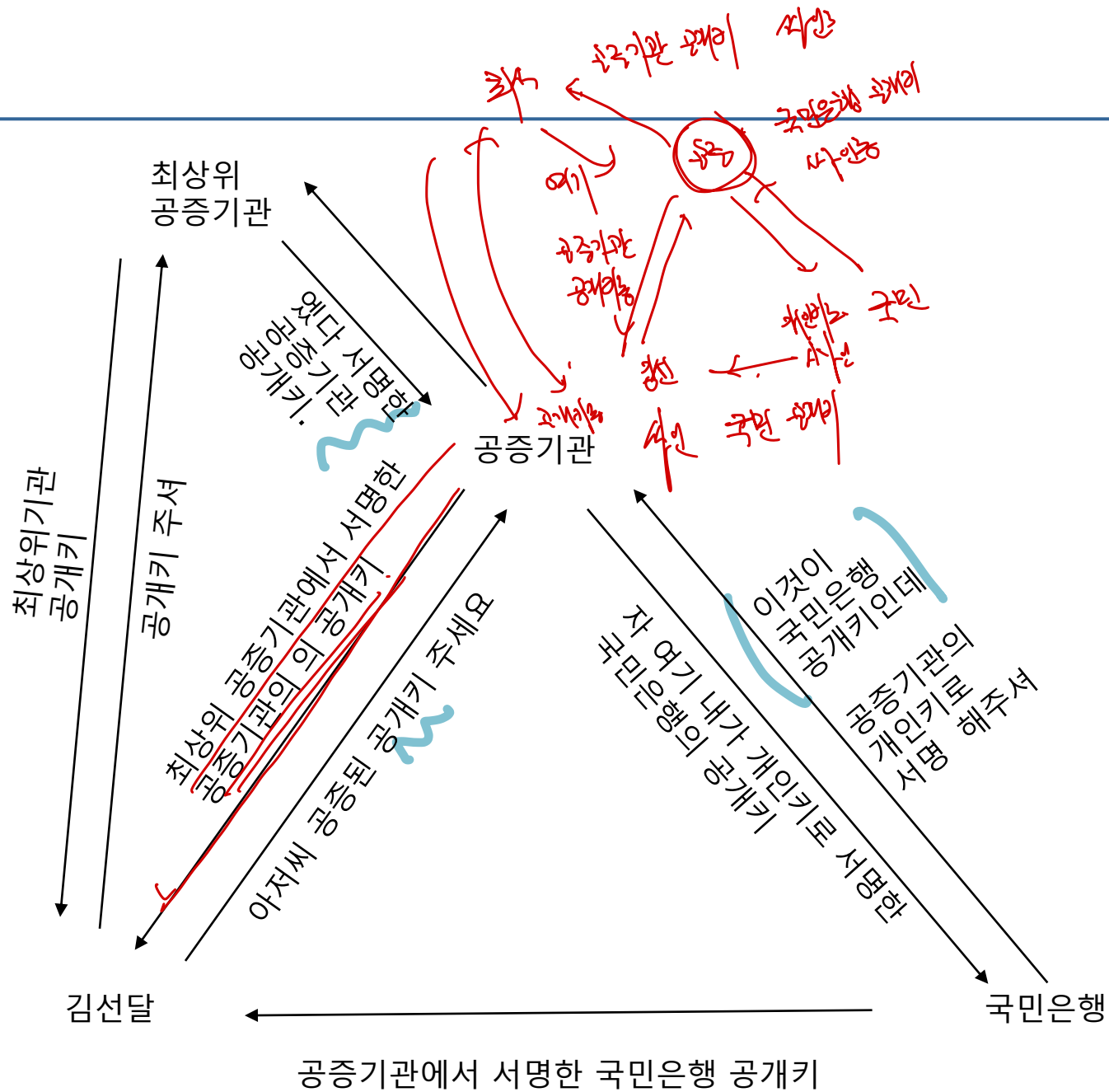


짜통 들끼리 짜고 치는 go-stop

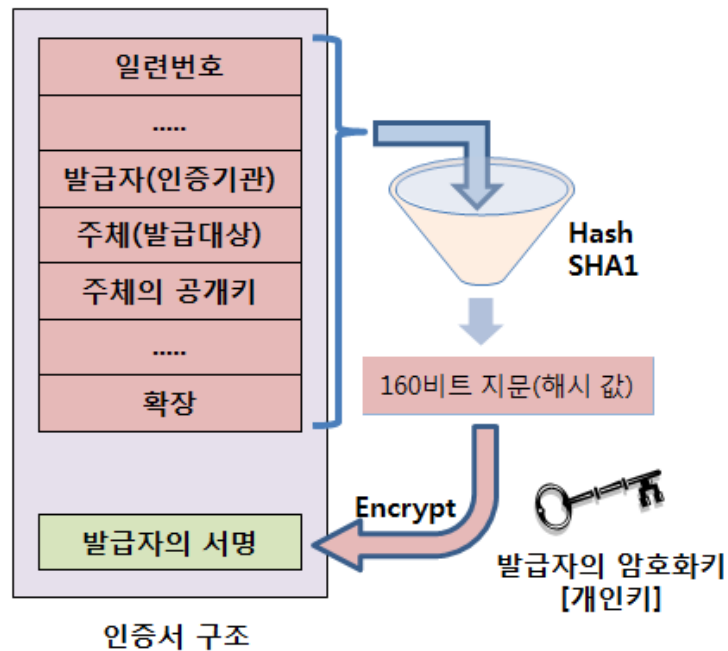


짜통 들끼리 짜고 치는 go-stop 이기는 법

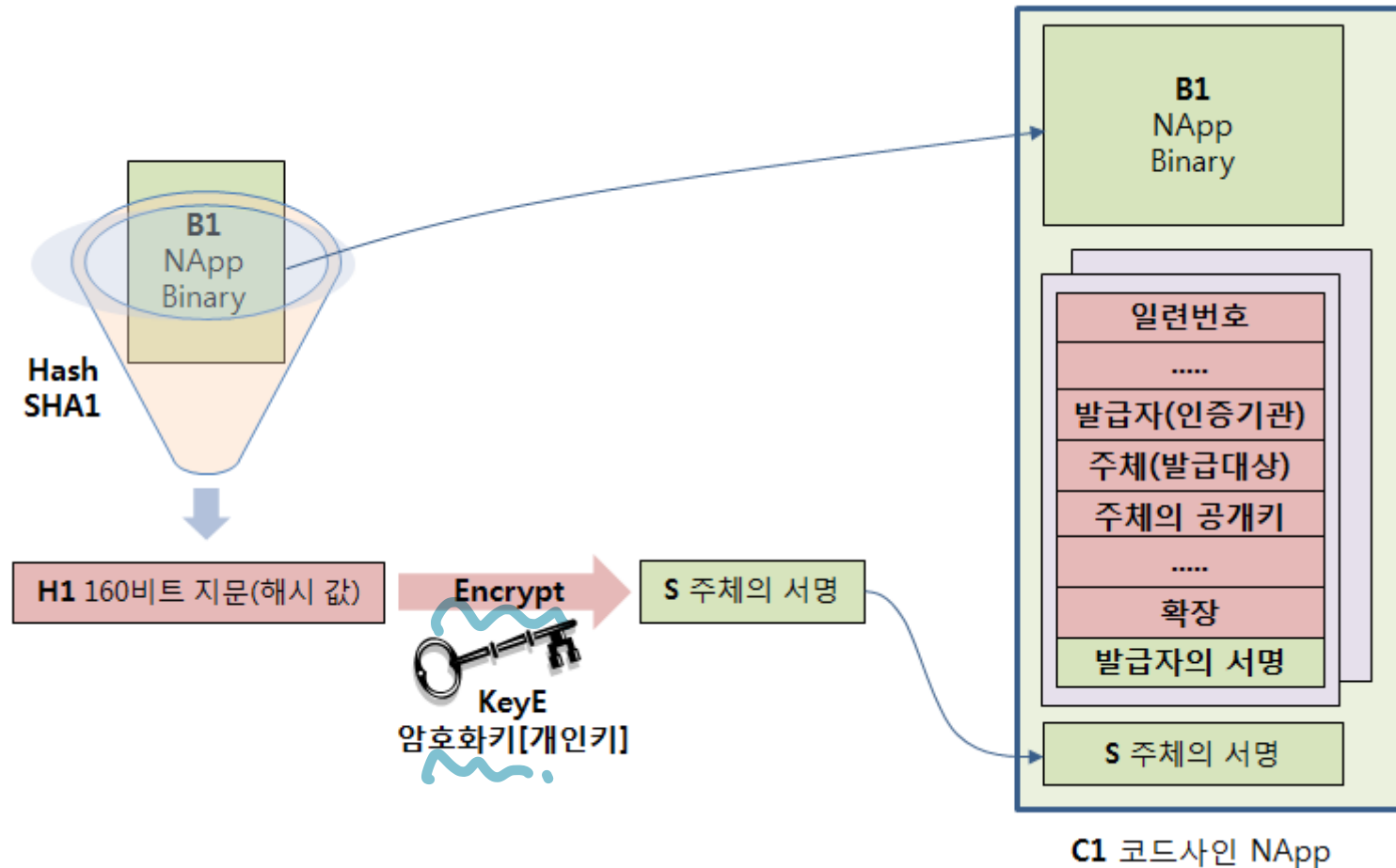




공인인증서 – 공인 인증된 공개키



자료의 무결성 확인 - 네이버



15.3 인터넷 보안

보안 프로토콜: SSL

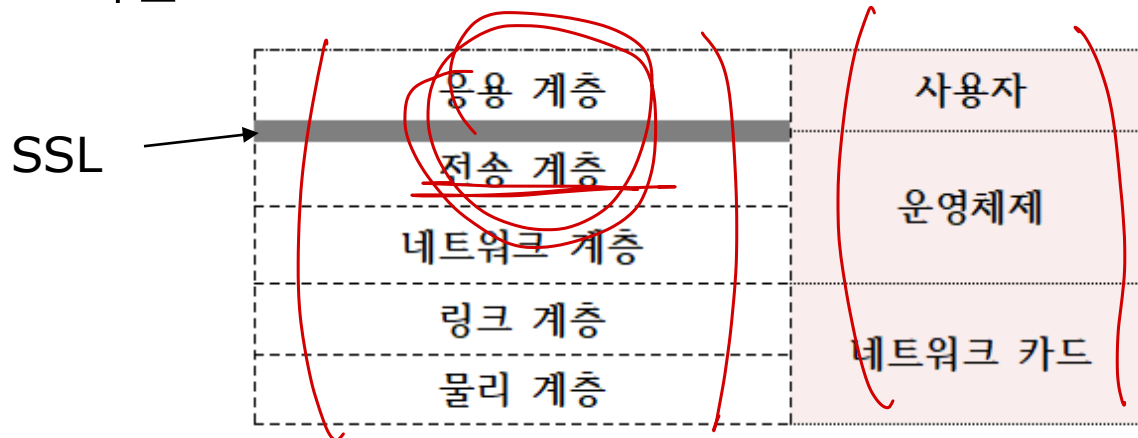
□ 보안 소켓 계층(SSL: Secure Sockets Layer)

□ 웹 브라우저와 웹 서버간의 통신에서 보안 서비스를 제공

- ▶ MS 익스플로러, 구글 크롬, 모질라 파이어폭스, 애플 사파리 등 웹브라우저
- ▶ Apache, Windows IIS 웹서버

□ TCP/IP 통신 모델에서의 SSL

□ 응용(프로그램) 계층과 전송 계층 사이에서 라이브러리 형태로 지원



응용 계층의
웹 브라우저와
서버간의
통신에
보안
서비스를
제공

port to port
end to end
program to program

보안 프로토콜: IPSec

- 인터넷 보안 프로토콜 (IPSec, Internet Protocol Security)
 - 네트워크 계층에서 IP패킷 단위로 보안서비스 제공
 - 인증, 암호화, 키관리
- TCP/IP 통신 모델에서 IPSec의 위치

응용 계층	사용자
전송 계층	운영체제
네트워크 계층	
링크 계층	네트워크 카드
물리 계층	

" IP 계층에 대한
보안. "

- SSL과의 주요 차이점
 - IPSec은 운영체제의 일부로 구현
 - SSL은 웹 응용프로그램에서 구현

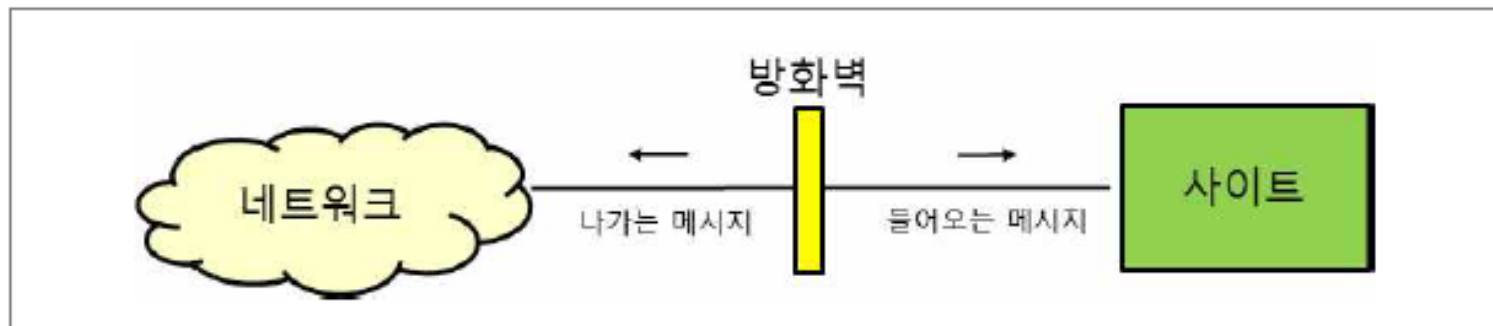
IPSec: 운영체제
SSL: 웹 응용프로그램

방화벽

패킷 필터링
방화벽

□ 개념

- 정보 보안을 위해 외부에서 내부, 내부에서 외부의 네트워크에 불법적으로 접근하는 것을 차단하는 시스템
- 내부망(인트라넷)과 외부망(인터넷) 간의 연결 통로에 설치
- 네트워크 트래픽을 모니터링
- 정해진 보안 규칙을 기반으로 특정 트래픽의 허용 또는 차단을 결정
 - ▶ 예) 설정된 보안규칙에 따라 특정 IP주소 (예: 131.34.0.0) 혹은 특정 포트번호(예: 23, 80)에 대해서는 패킷전달 차단



방화벽의 종류

- 소프트웨어 방화벽
- 하드웨어 방화벽
- 칩 기반의 방화벽
- 멀티코어 프로세서 기반의 방화벽
 - 한 번에 많은 양의 패킷을 처리할 수 있음

15.4 악성 소프트웨어

악성 소프트웨어

- 악의적인 의도를 가지고 보안 침해를 목적으로 구현한 소프트웨어를 통칭
- 멀웨어라고도 불림
크래커
- 특징에 따른 분류
 - 바이러스: ...
 - 웜: ...
 - 트로이목마: ...
 - 트랩도어: ...
 - ...*랜섬웨어*

악성 소프트웨어

- 악성 소프트웨어를 이용한 범죄 수법 유형
 - 프로그램 변경
 - 데이터 변경
 - 부정 접근
 - ▶ 권한이 없는 자가 시스템 사용 권한을 부정으로 획득
 - 에러 조작
 - 컴퓨터 시간 통제

15.5 컴퓨터 범죄

컴퓨터 범죄 개요

- 어떠한 유형의 컴퓨터 범죄가 발생할까?
 - 예측하기 어렵지만...

- 컴퓨터 범죄의 방향 예측
 - 하드웨어와 소프트웨어의 발전과 같은 축으로 증가
 - 하드웨어를 구성하는 모듈 중 특정 모듈의 이용에 의존
 - 소프트웨어를 이용한 범죄 급증
 - 컴퓨터 바이러스를 이용한 범죄
 - 국경을 초월하여 발생
 - 인공지능 기술을 이용한 지능 범죄

컴퓨터 범죄 수법

□ 컴퓨터 범죄 유형

- 데이터 디들링 (데이터를 망가뜨리는 등)
- 슈퍼잡핑 (교장 노을 때)
- 스케베닝 (주머니에서 가져갈 것..?)
- 피키백킹/임펄스네이션
- 와이어 태핑

데이터 디들링 : 데이터를 망가뜨리는 등 또는 변조하는 것

슈퍼잡핑 : 교장 노을 때

스케베닝 : 주머니에서 가져갈 것. (리모컨)

피키백킹 : 가방을 훔치는 것.
(예를 들어, 주머니에서 가져갈 것)

와이어 태핑 : 배선으로 정보를 훔치는 것

컴퓨터 범죄 수법

□ 데이터 디들링(Data Diddling)

- 금융기관의 컴퓨터 범죄에서 많이 볼 수 있음
- 데이터를 입력하는 동안이나 변환하는 순간에 데이터를 절취, 삭제, 변경, 추가하는 행위

□ 슈퍼 잭핑(Super Zapping)

- 컴퓨터가 다운되어 복구나 재부팅에 의해서 다시 정상적인 작동을 할 수 없을때 발생
- 어떠한 제한이나 장애를 다 통과할 수 있는 강력한 기능을 가진 유틸리티 프로그램을 실행하여, 접근이 금지된 영역에 침입하거나 부정 행위를 함

컴퓨터 범죄 수법

□ 스캐베닝(Scavenging)

- 컴퓨터 작업 수행이 끝난 뒤나 그 주위에서 정보를 획득하는 방법:
- 버려진 종이의 비밀 번호 또는 출력된 폐지 등에서 정보를 불법으로 획득
- 작업을 마친 컴퓨터의 메모리에 남아있는 내용을 덤프하여 분석

□ 피키백킹/임펄스네이션(Piggybacking/Impersonation)

- 단말기의 회선을 다른 단말기에 부정 연결하여 정보를 획득
- 사용 허가를 받지 않은 자가 컴퓨터를 부정 사용

□ 와이어 태핑(Wiretapping)

- 네트워크에 불법적으로 접속하여 정보를 절취하거나 컴퓨터를 부정 사용
- 유무선 도청