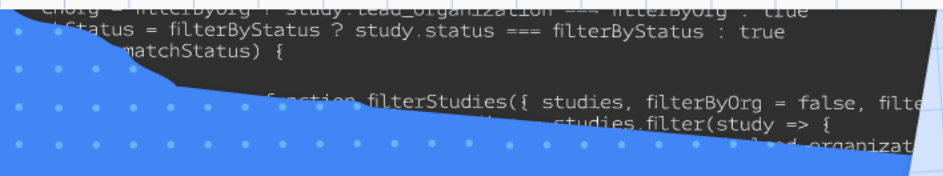
Google Developer Student Clubs
Soongsil University

HTTPS는 어떻게 보안성을 높이는가

HTTPS와 SSL 그리고 CA

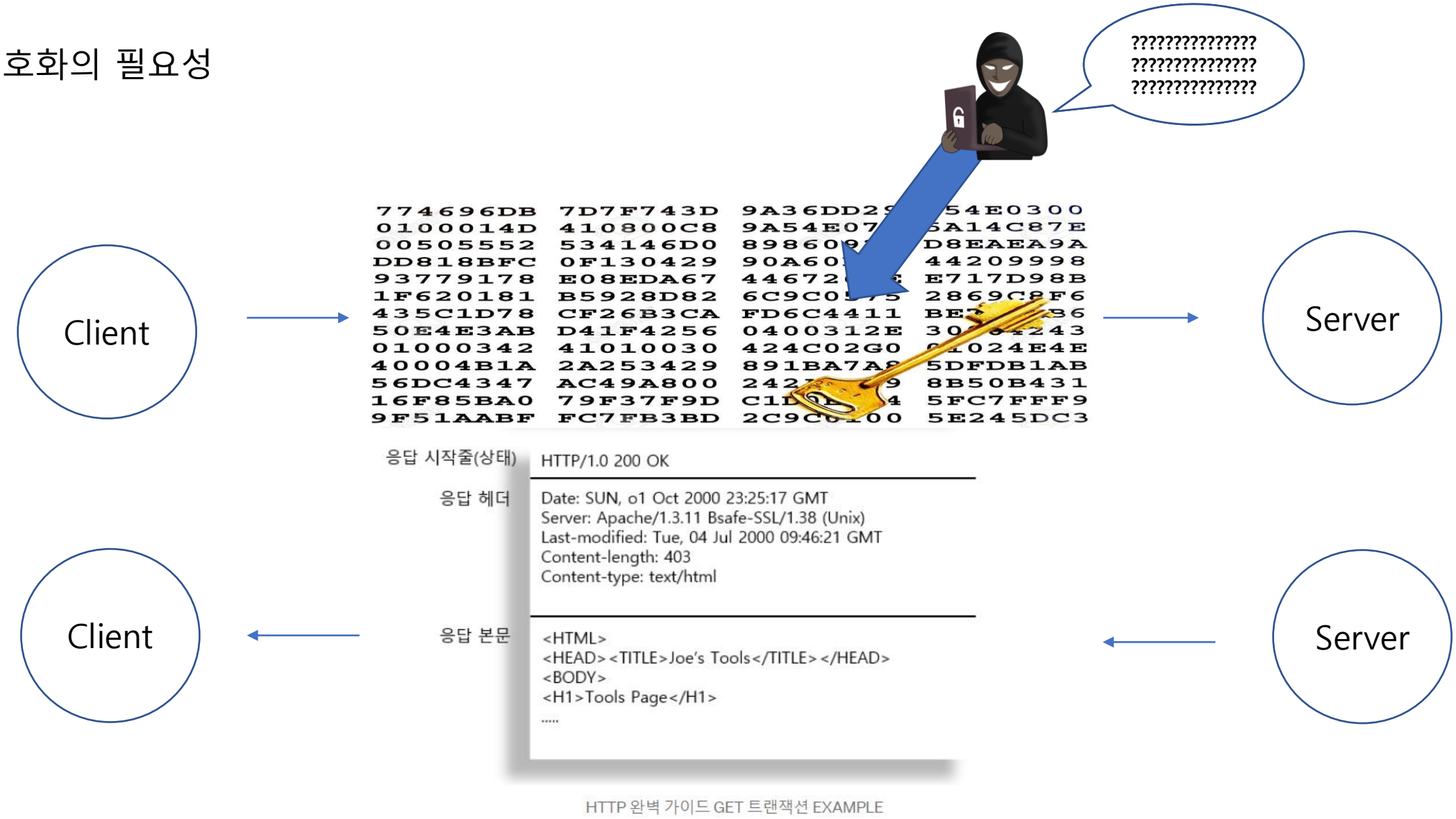


1. SSL의 암호화 방식

   - 대칭키
   - 공개키

2. CA는 왜 필요할까

암호화의 필요성



HTTP 완벽 가이드 GET 트랜잭션 EXAMPLE

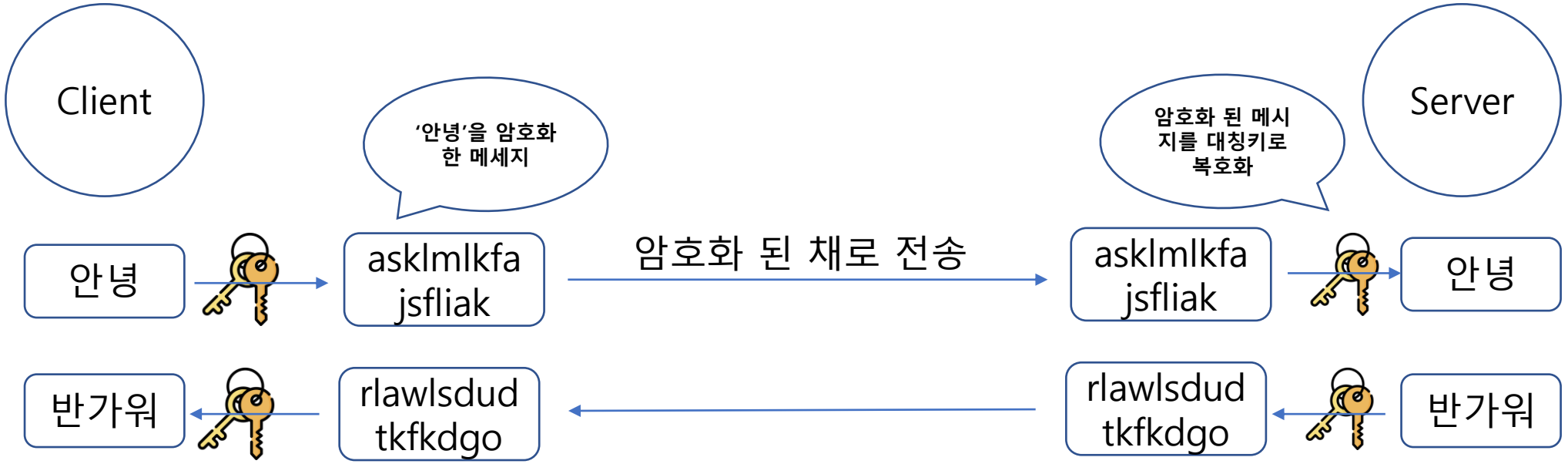
HTTPS란 HTTP 메시지를 SSL을 이용하여 암호화 한 것

SSL을 이해하기 위하여 알야아 하는 암호화 방법 2가지

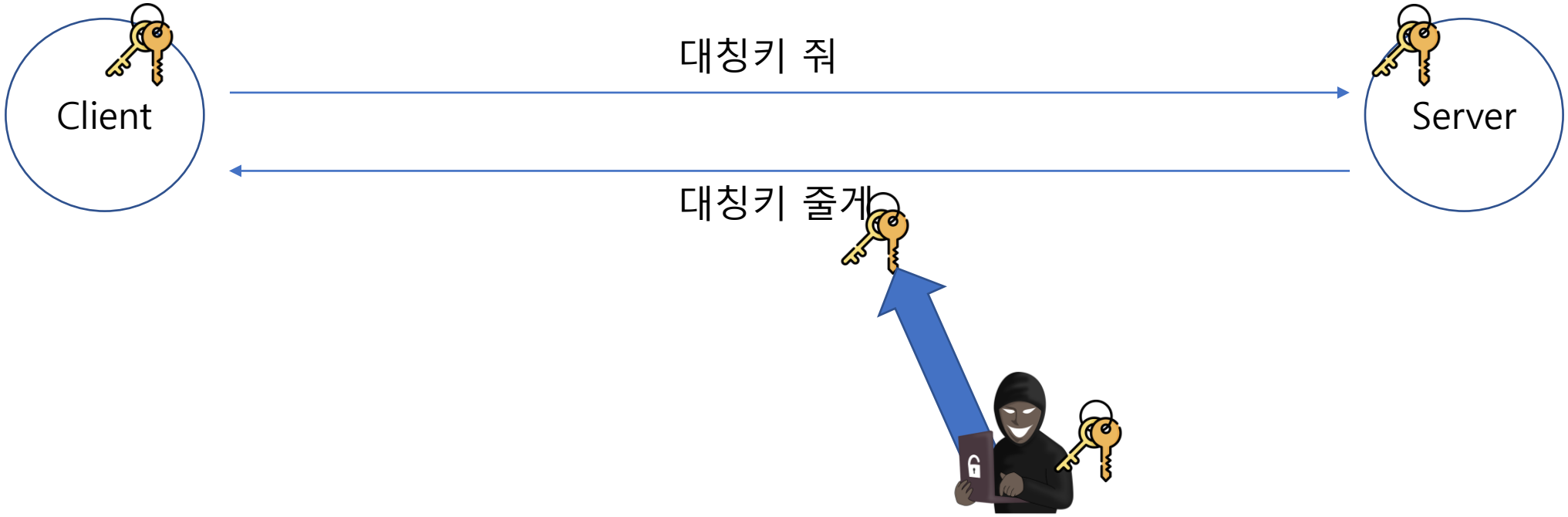
1. 대칭키

2. 공개키

대칭키


Client
'안녕'을 암호화 한 메세지
암호화 된 메시지를 대칭키로 복호화
Server
안녕
asklmlkfa jsfliak
암호화 된 채로 전송
asklmlkfa jsfliak
안녕
반가워
rlawlsdud tkfkdgo
rlawlsdud tkfkdgo
반가워

대칭키의 한계



공개키

공개키의 특징

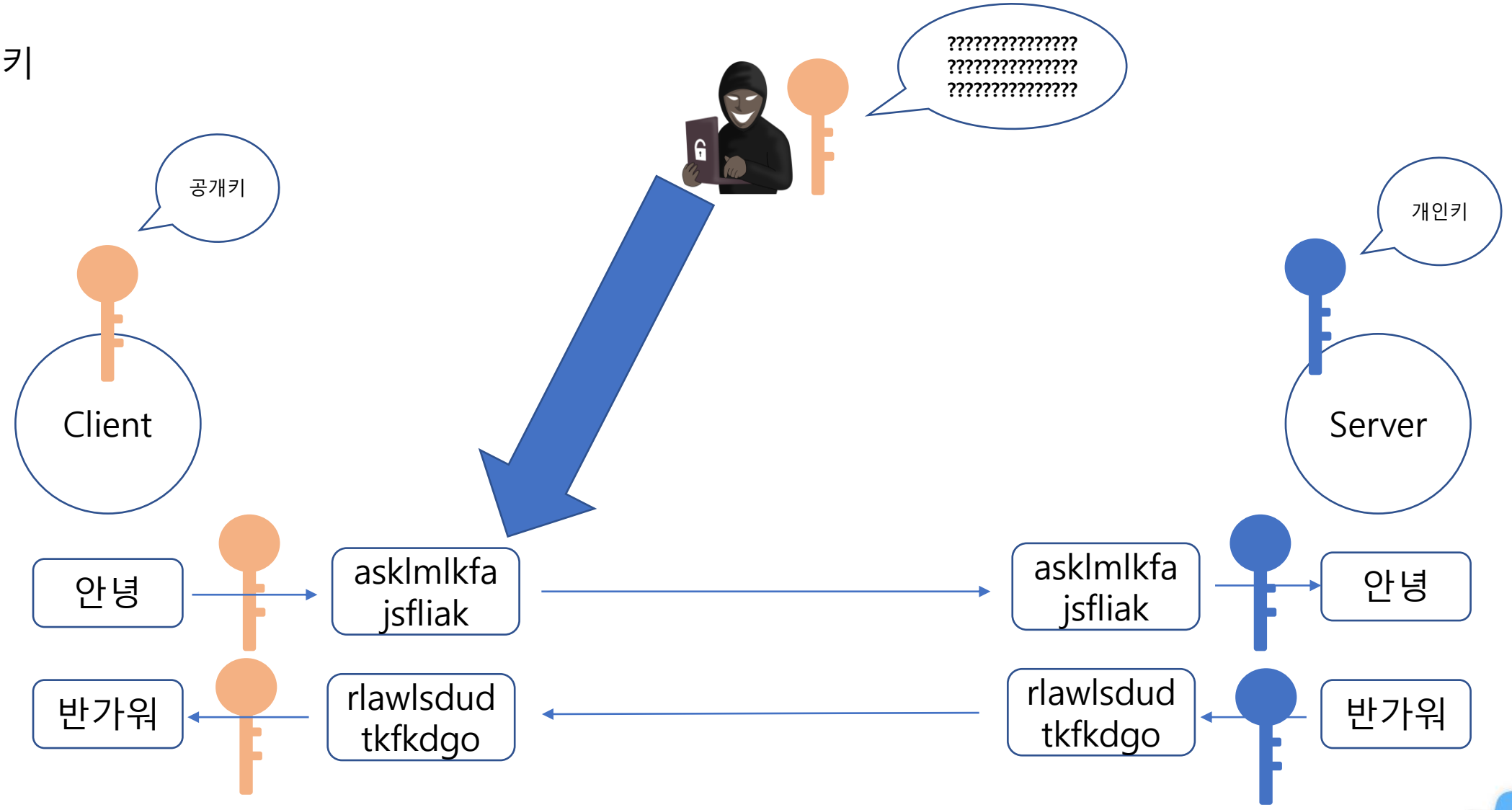
개인키로 암호화 된 메시지는 공개키로 복호화 할 수 있고,

공개키로 암호화 된 메시지는 개인키로 복호화 할 수 있다.

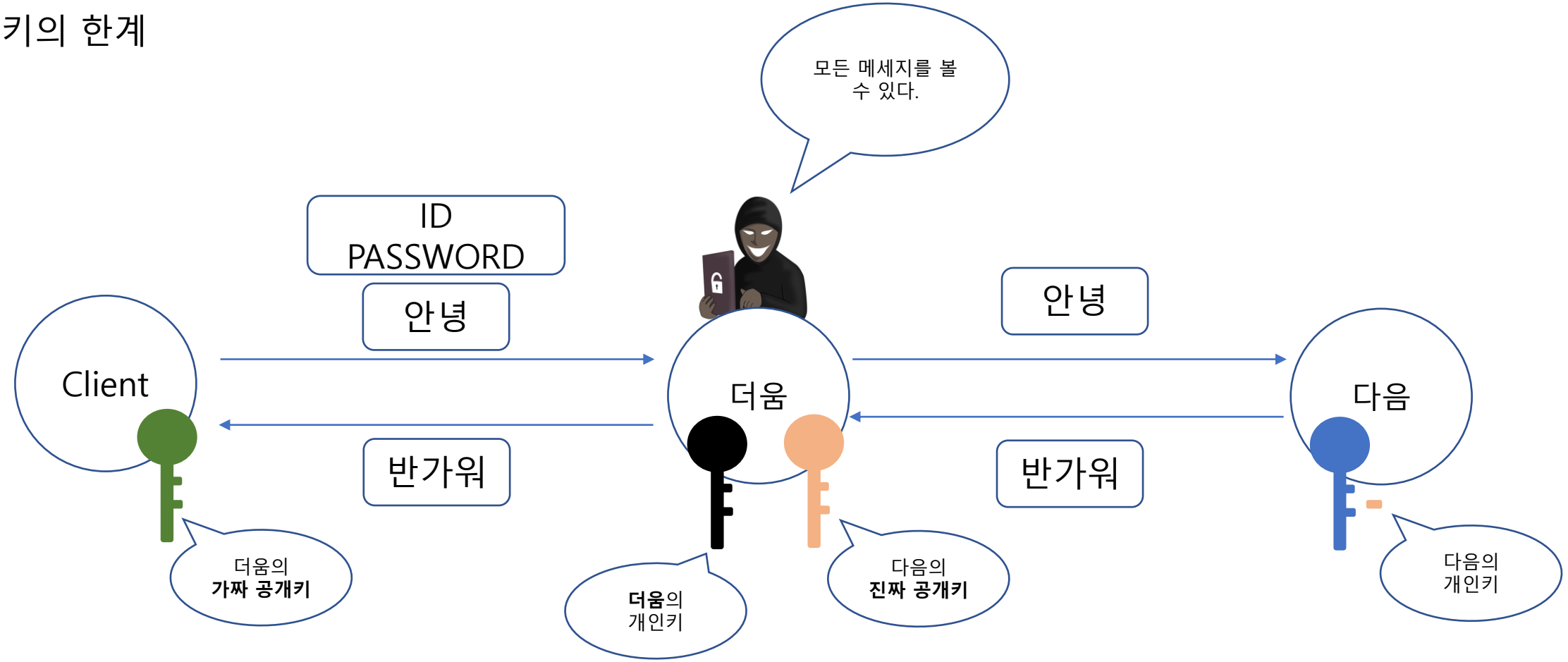
즉 개인키로 개인키로 암호화 한 메시지를 복호화 할 수 없고,

공개키로 암호화 한 메시지를 공개키로 복호화 할 수 없다.

공개키

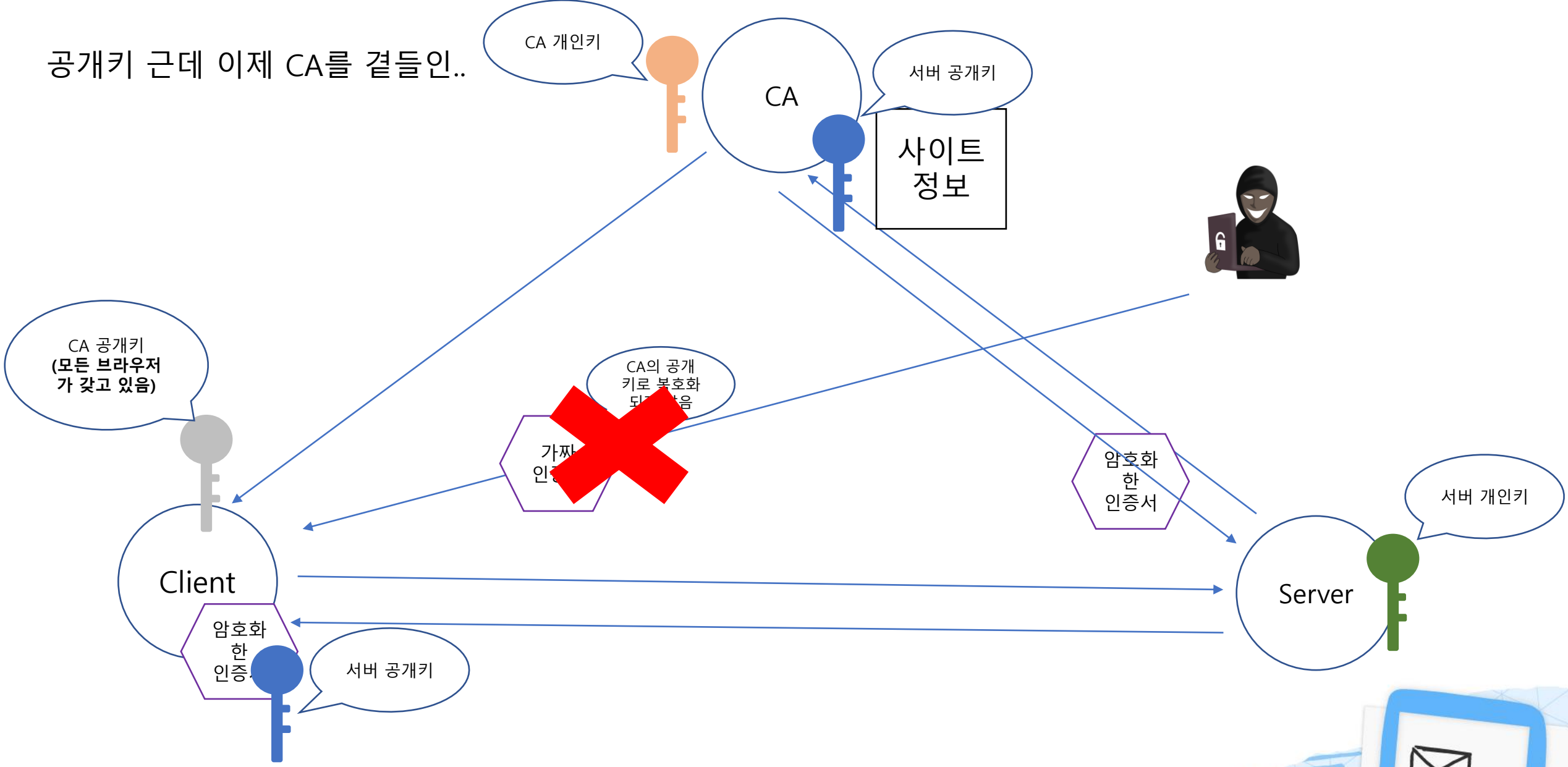

??????????????
??????????????
??????????????
공개키
Client
개인키
Server
안녕
asklmlkfa
jsfliak
asklmlkfa
jsfliak
안녕
반가워
rlawlsdud
tkfkdgo
rlawlsdud
tkfkdgo
반가워

공개키의 한계


모든 메세지를 볼 수 있다.
ID
PASSWORD
안녕
Client
더움
안녕
다음
반가워
반가워
더움의
가짜 공개키
더움의
개인키
다음의
진짜 공개키
다음의
개인키

그래서 드디어 CA !!!

공개키 근데 이제 CA를 곁들인..



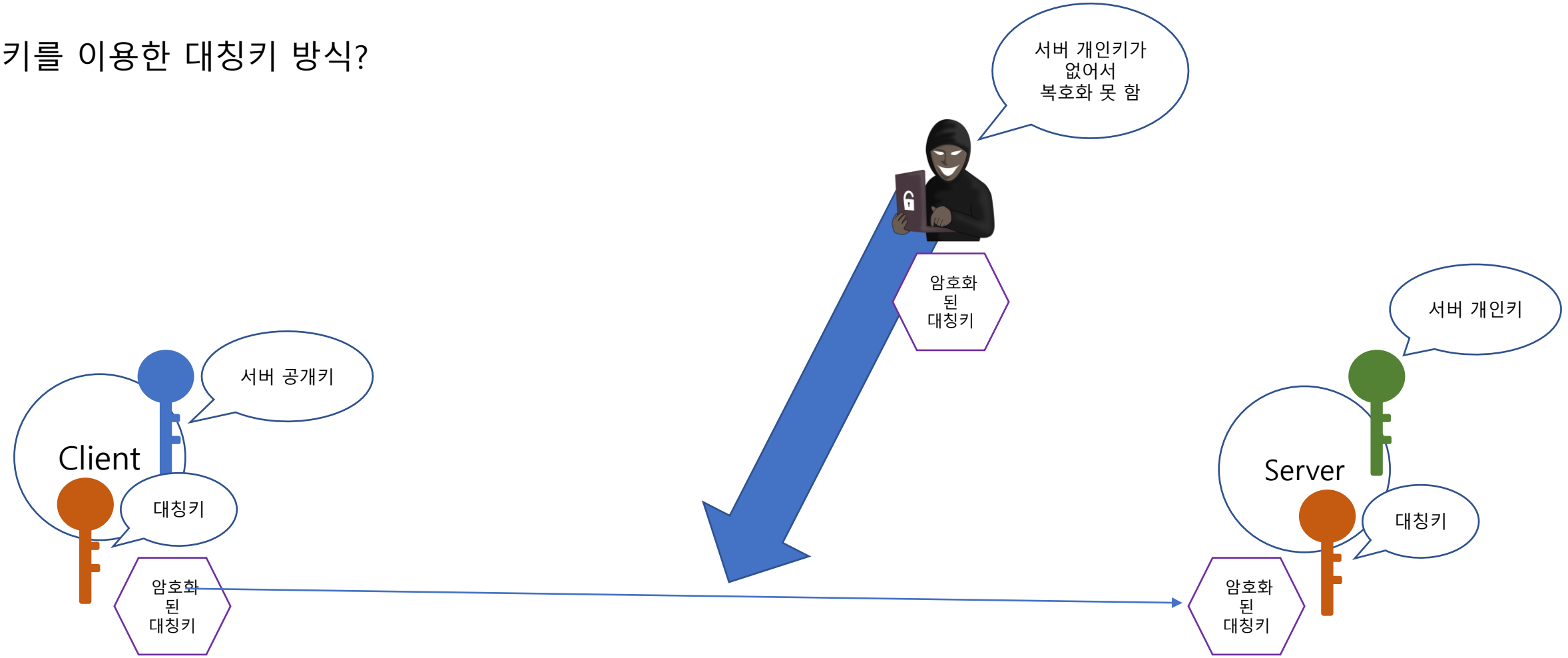
Google Developer Student Clubs
Soongsil University

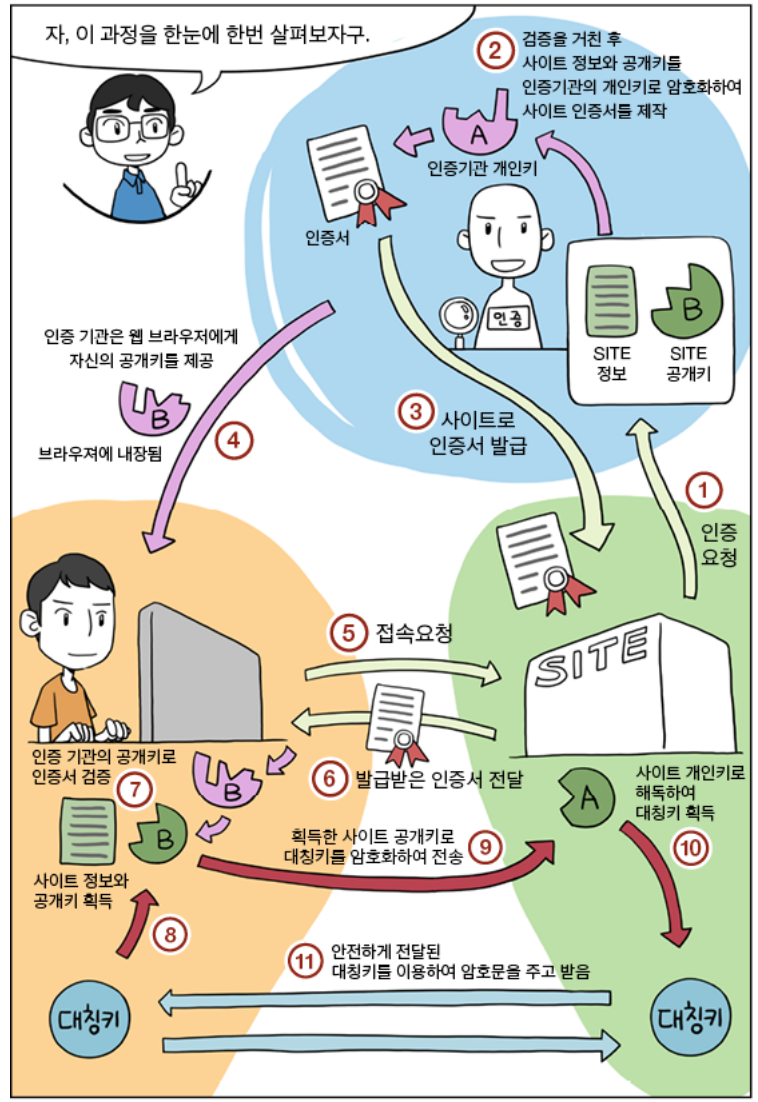
해치웠나...?

모든 메시지를 공개키 방식으로 암호화, 복호화 하는 것은

너무 큰 부담이 됨

공개키를 이용한 대칭키 방식?




자, 이 과정을 한눈에 한번 살펴보자구.
② 검증을 거친 후
사이트 정보와 공개키를
인증기관의 개인키로 암호화하여
사이트 인증서를 제작
A
인증기관 개인키
인증서
인증
SITE
정보
B
SITE
공개키
③ 사이트로
인증서 발급
인증 기관은 웹 브라우저에게
자신의 공개키를 제공
B
브라우져에 내장됨
④
① 인증
요청
⑤ 접속요청
SITE
⑥ 발급받은 인증서 전달
인증 기관의 공개키로
인증서 검증
⑦
B
사이트 정보와
공개키 획득
⑧
획득한 사이트 공개키로
대칭키를 암호화하여 전송 ⑨
A
사이트 개인키로
해독하여
대칭키 획득
⑩
⑪ 안전하게 전달된
대칭키를 이용하여 암호문을 주고 받음
대칭키
대칭키

감사합니다