HTTP와 HTTPS

김예지

HTTP
Hypertext Transfer Protocol

HTTP의 단점

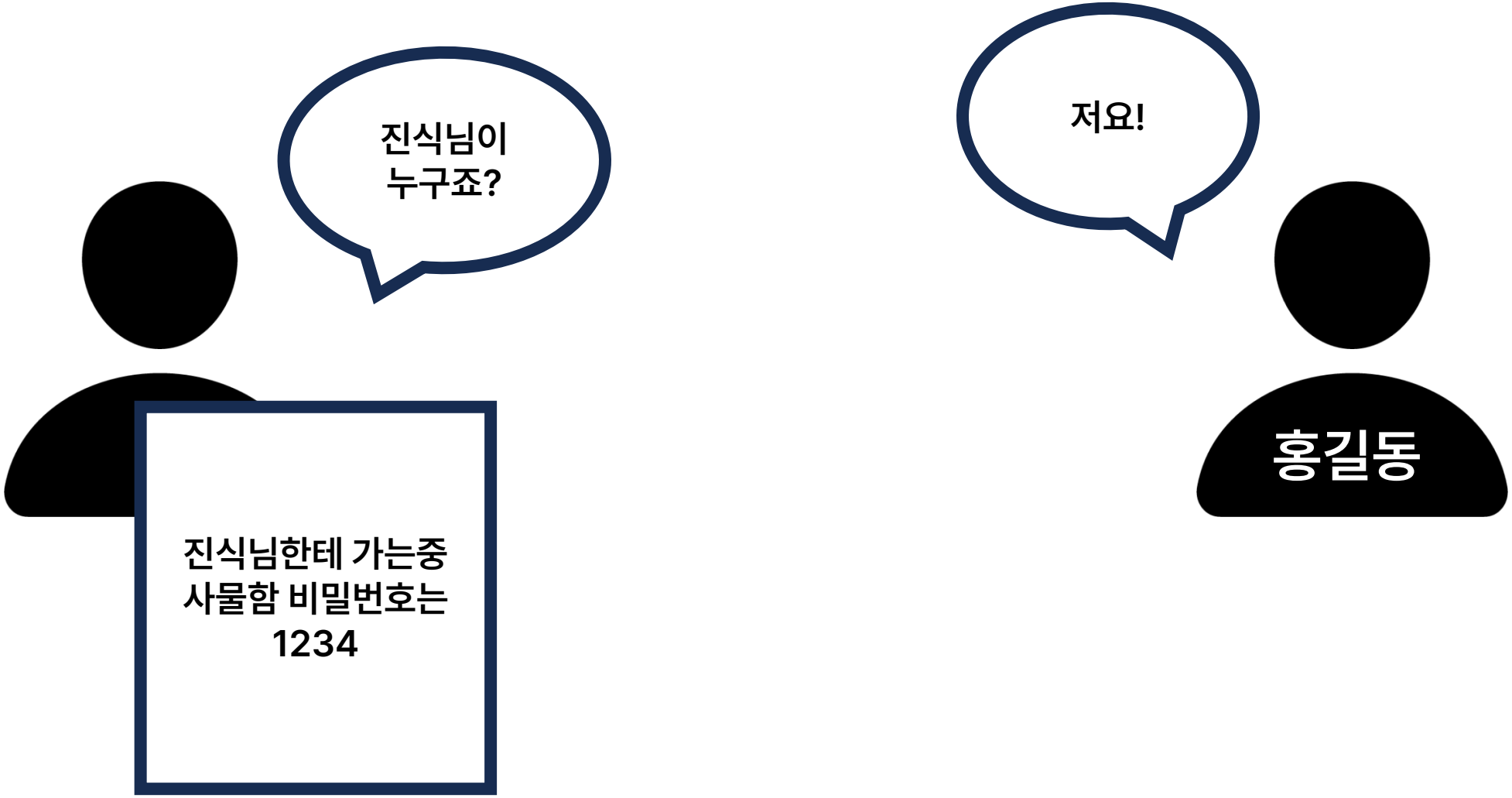
- 평문이다(암호화 되어있지 않다.)
- 통신 상대를 확인하지 않아서 위장이 가능하다
- 완전성을 증명할 수 없기 때문에 변조가 가능하다.

HTTP의 단점

평문이다(암호화 되어있지 않다.)

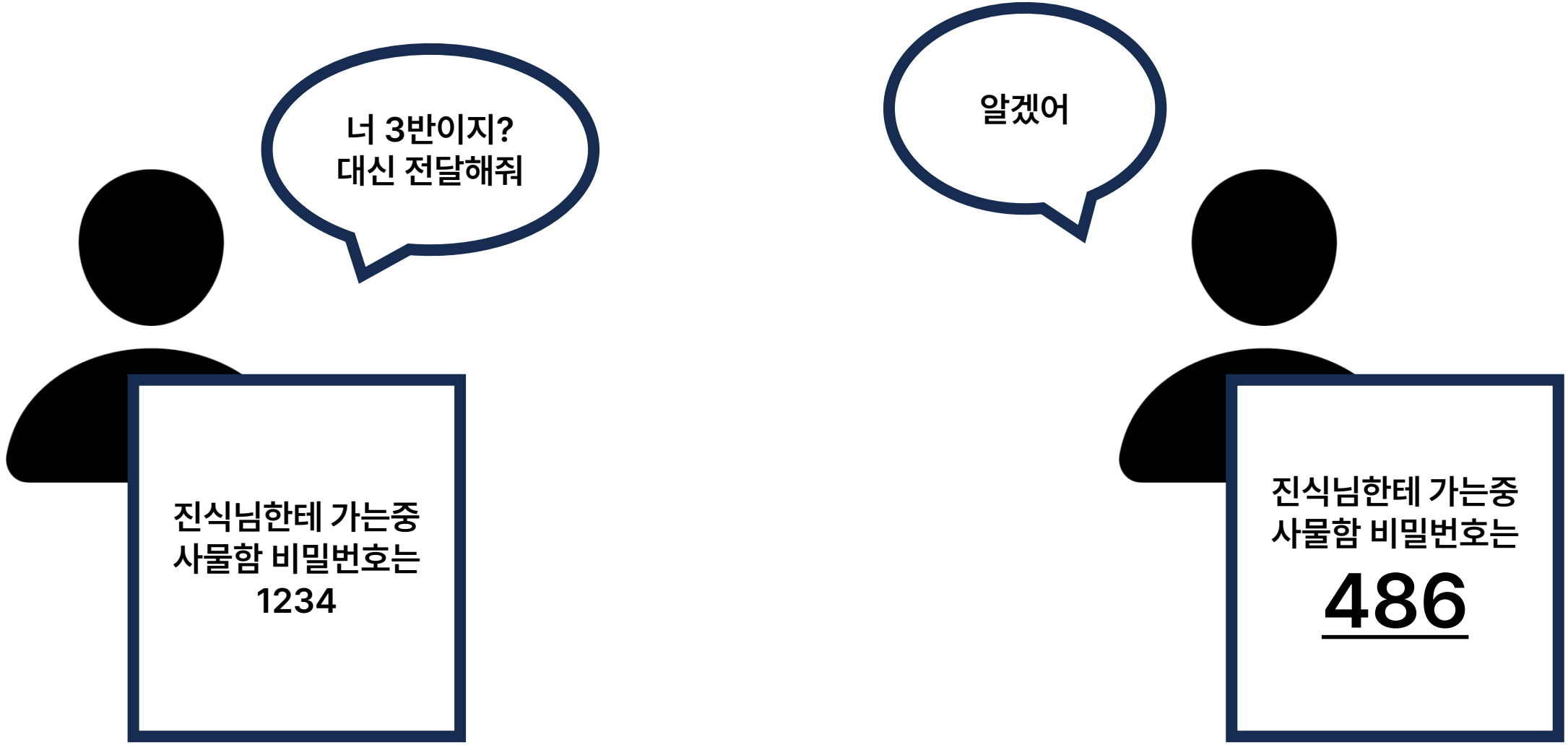
HTTP의 단점

통신 상대를 확인하지 않아서 위장이 가능하다

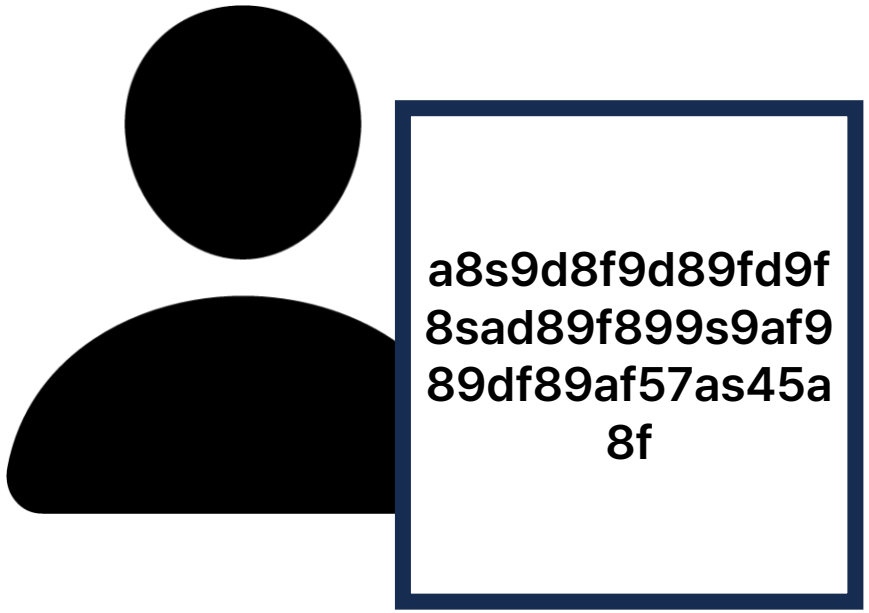


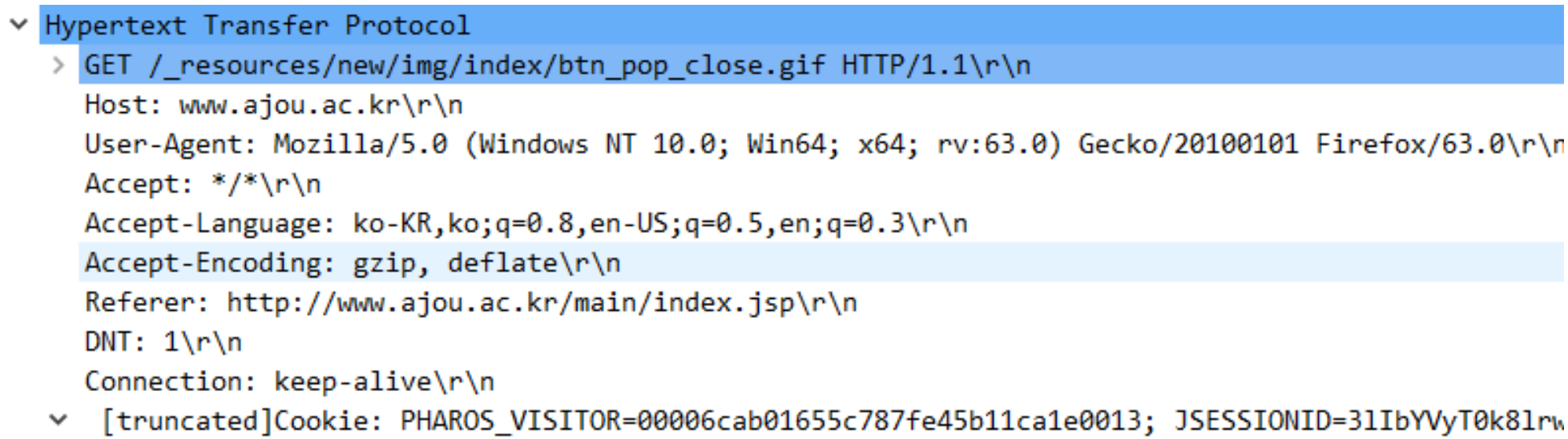
HTTP의 단점

완전성을 증명할 수 없기 때문에 변조가 가능하다.



HTTPS
Hypertext Transfer Protocol
Secure


a8s9d8f9d89fd9f
8sad89f899s9af9
89df89af57as45a
8f


Hypertext Transfer Protocol
GET /_resources/new/img/index/btn_pop_close.gif HTTP/1.1\r\n
Host: www.ajou.ac.kr\r\n
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:63.0) Gecko/20100101 Firefox/63.0\r\n
Accept: */*\r\n
Accept-Language: ko-KR,ko;q=0.8,en-US;q=0.5,en;q=0.3\r\n
Accept-Encoding: gzip, deflate\r\n
Referer: http://www.ajou.ac.kr/main/index.jsp\r\n
DNT: 1\r\n
Connection: keep-alive\r\n
[truncated]Cookie: PHAROS_VISITOR=00006cab01655c787fe45b11ca1e0013; JSESSIONID=3lIbYVyT0k8lrw

주의 : HTTPS는 HTTP 헤더까지 암호화한다.

```
Secure Sockets Layer
  TLSv1 Record Layer: Application Data Protocol: http-over-tls
       Content Type: Application Data (23)
       Version: TLS 1.0 (0x0301)
       Length: 656
       Encrypted Application Data: a906b20191e1148849ed19c89e6fad1798dbbd8cd4f34a81...
```

HTTPS를 사용하면 구글에서 가산점을 준다.
상위에 노출될 수 있다.

SSL/TLS

- Secure Sockets Layer
- Transport Layer Security
- TLS가 SSL의 보완된 버전
  - 이름이 바뀐것은 SSL을 개발한 Netscape가 업데이트에 참여하지 않게 되어 소유권 변경을 위해서였다고 한다.

Layer	Layer Name	Data Unit	Protocol	Device
7	응용 계층		HTTP, FTP, SMTP, DNS	
6	표현 계층		JPG, MPEG, AFP, PAP	
5	세션 계층		NetBIOS, SSH	
4	전송 계층	TCP – segment UDP - datagram	TCP, UDP	게이트 웨이
3	네트워크 계층	Packet	IP, RIP, ARP, ICMP	라우터
2	데이터 링크 계층	Frame	Ethernet, PPP, HDLC	브릿지, 스위치
1	물리 계층	Bit	RS-232, RS-449	허브, 리피터

도깨비말을 아시나요?


놀라운 토요일
도레미 마켓
여자친구 유주 X 엄지
오늘은 나만 잘하고 싶어요
tvN
예시-'ㅂ'버전
혜리 선배님
tvN


놀라운 토요일
도레미 마켓
여자친구 유주 X 엄지
오늘은 나만 잘하고 싶어요
tvN
예시-'ㅂ'버전
혜벼리비서번배배니빔
tvN

대칭키(공통키) 암호화

- 도깨비말
- 도깨비말의 비밀을 알게 되면 누구나 해독할 수 있다. **(위험 포인트)**

싸피 최고!

싸바피비 최뵈고보!

평문	암호문
싸	싸바
피	피비
최	최뵈
고	고보

대칭키(공통키) 암호의 딜레마

- 상대방에게 키를 넘겨 줘야한다
- 키를 넘겨주는 동안에 도청되면 키를 뺏긴다

어떻게 하는 것이 좋을까요?

¯_(ツ)_/¯

비대칭키(공개키/비밀키) 암호화

- RSA방식이 가장 대표적

- 서버가 공개키를 클라이언트에게 준다
- 클라이언트는 공개키로 보낼 내용을 암호화한다
- 공개키로 암호화한 내용은 공개키로 복호화할 수 없다.
- 서버는 클라이언트에서 받은 암호화된 내용을 비밀키로 복호화한다.

- 복잡한 수학적 연산이 필요해서 공개키보다 처리가 느리다.

대칭키(공통키)는
빠르고 쉽다


놀라운 토요일
도레미 마켓
여자친구 유주 X 엄피
오늘은 나만 잘하고 싶어요
메이네 식료품
tvN
한번
해보요!!
외계어로 서로 소통까지 가능
tvN


놀라운 토요일
도레미 마켓
여파친구 유주 X 엄지
오늘은 나만 잘하고 싶어요
tvN
우수리시 오소느슬
기신자상하사지시마살고소
자살하사자사
tvN

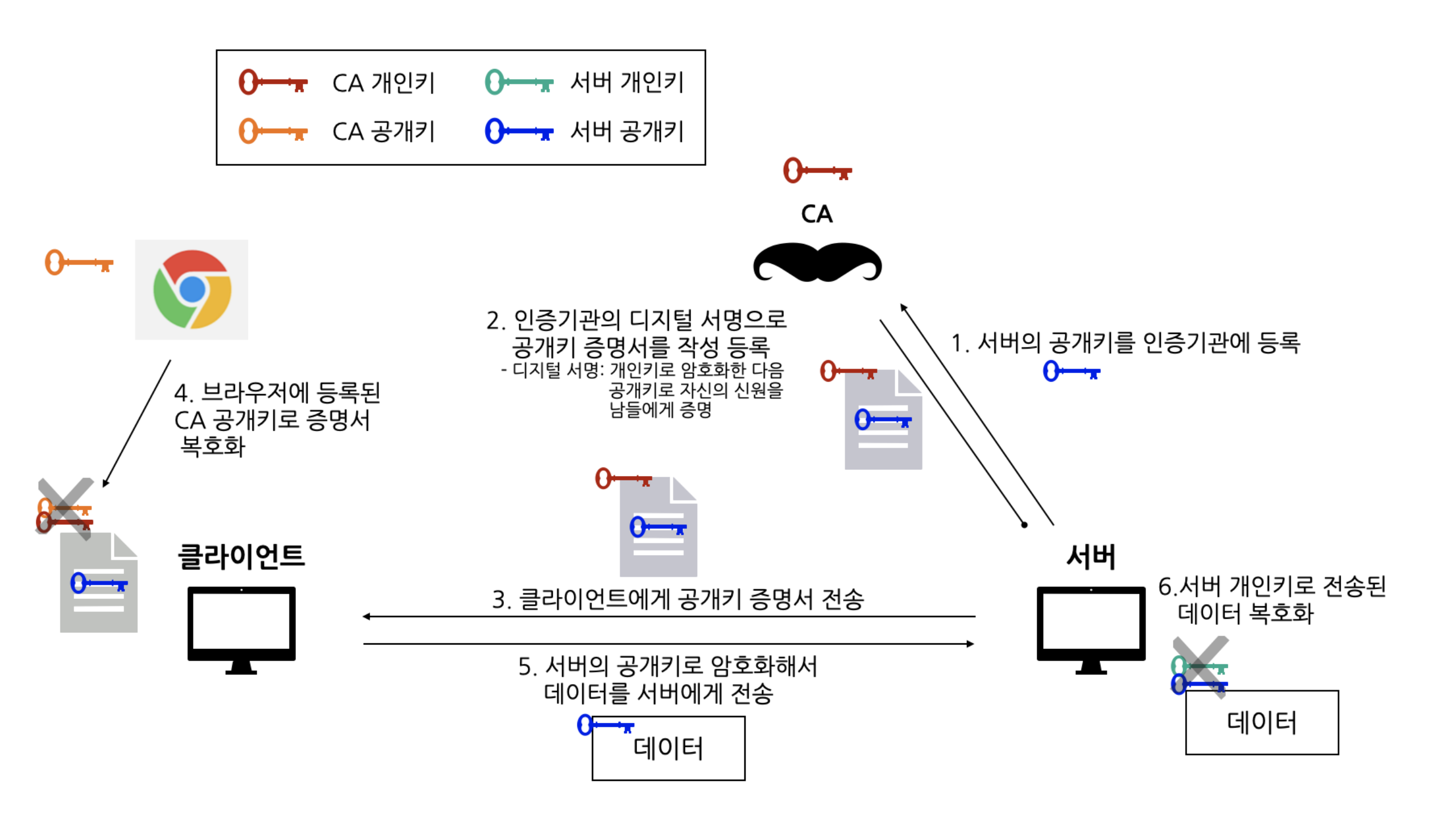

놀라운 토요일
도레미 마켓
여파친구 유주 X 엄지
오늘은 나만 잘하고 싶어요
tvN
조보그븜 기빈자방해뱄느븐데베
자발하발수부이빘으블거벗가밭아바
(화솨이시티싱!) 화봐이비티빙!
tvN

대칭키 전달시에만 비대칭키를 사용한다.

- 대칭키가 안전하게 전달된 후에는 대칭키로만 암호화해서 통신한다.
- 여전한 문제 : 공개키가 진짜인지 알 수 없다.
- 진짜 진식님의 공개키일까? 홍길동의 공개키를 받은건 아닐까?

CA(Certificate Authority)

- 제 3자이며 공신력 있는 CA가 인증해준다.
- 비용이 드는 경우가 많다. (졸업증명서 발급시에도 돈을 내는 것과 비슷)
- Ex)


CA 개인키
서버 개인키
CA 공개키
서버 공개키
CA
2. 인증기관의 디지털 서명으로
공개키 증명서를 작성 등록
- 디지털 서명: 개인키로 암호화한 다음
공개키로 자신의 신원을
남들에게 증명
1. 서버의 공개키를 인증기관에 등록
4. 브라우저에 등록된
CA 공개키로 증명서
복호화
클라이언트
서버
3. 클라이언트에게 공개키 증명서 전송
5. 서버의 공개키로 암호화해서
데이터를 서버에게 전송
데이터
6.서버 개인키로 전송된
데이터 복호화
데이터

추가자료

Http와 https 통신을 직접 뜯어본 후기글
https://parksb.github.io/article/24.html

공개키 원리를 알고 싶다면?
https://www.youtube.com/watch?v=aG0024G9-0k

복습을 위한 쉬운 영상
https://www.youtube.com/watch?v=H6lpFRpyl14