

BioStar 2 ..... 1

  HTTP ..... 1

  HTTPS ..... 1

  SSL ..... 2

    SSL ..... 2

      (     ) ..... 2

      ..... 3

      ..... 3

      ..... 3

      (             ) ..... 4

      ..... 5

      ..... 5

      ..... 5

      ..... 5

      ..... 5

      ..... 7

BioStar 2, HTTP, HTTPS

# BioStar 2

70% 가 가

HTTPS) BioStar2 가 (HTTP

HTTPS

## HTTP

HTTP Hypertext Transfer Protocol , HTML(HyperText Markup Language)

( ) ( )

TCP/UDP , 80

HTTP 가 가 'Request' 'Response'

가

HTTP , 가 가 'Request' 'Response' 가 HTTPS 가

## HTTPS

HTTPS Hypertext Transfer Protocol over Secure Socket Layer , HTTP

. HTTPS 'Request' 'Response' 가

SSL(Secure Socket Layer) TLS(Transport Layer Security)

HTTPS HTTP 가 ,

# HTTP + SSL = HTTPS

HyperText Transfer Protocol

Secure Socket Layer

HyperText Transfer Protocol  
Secure Socket Layer

*Data transmission*

*Encryption*

*Transmission of secure data*

**+ SSL TLS**

SSL (Netscape Engineering Task Force) SSL

가 TLS

IETF (Internet Engineering Task Force) TLS

## SSL

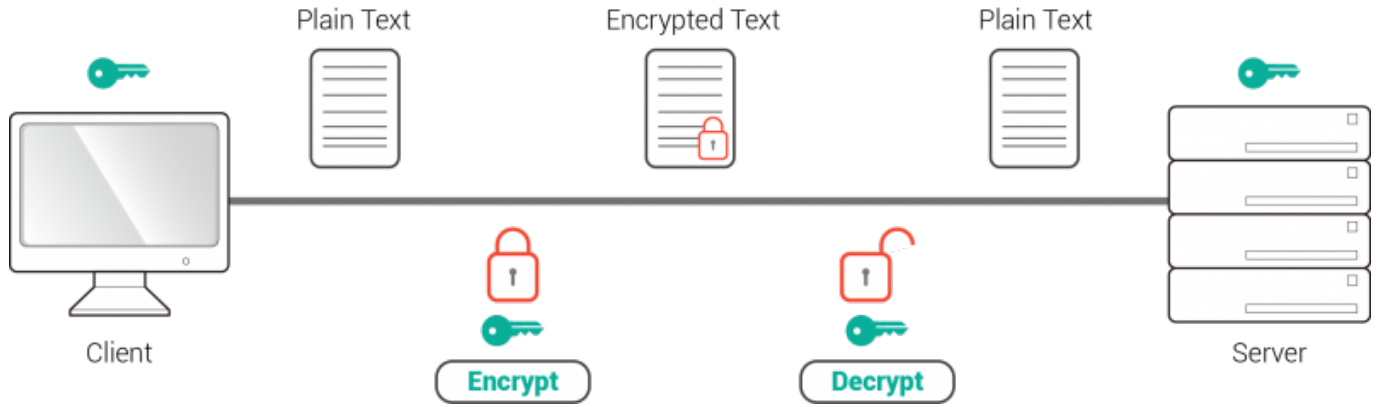
HTTPS는 SSL을 사용하여 데이터를 암호화하고 전송하는 프로토콜입니다. SSL은 3가지 버전 (SSL 1.0, SSL 2.0, SSL 3.0)이 있으며, 현재는 SSL 3.0과 TLS가 널리 사용됩니다. SSL은 데이터의 기밀성을 보장하고, ID를 사용하여 인증을 수행하며, (sniffing)을 방지합니다.

## SSL

SSL은 공개 키 암호화 (Key)를 사용하여 데이터를 암호화하고 전송하는 프로토콜입니다. SSL은 인증서를 사용하여 인증을 수행하며, ID를 사용하여 인증을 수행합니다.

( )

1245 가 , 1245



128 256 , 가  
 , 128 가 가  $2^{128} =$   
 340,282,366,920,938,463,463,374,607,431,768,211,456 , (brute-force  
 attack) 128 .

- AES (Advanced Encryption Standard)
- DES (Data Encryption Standard)
- 3DES
- IDEA (International Data Encryption Algorithm)
- Blowfish
- Twofish
- Serpent
- CAST5
- RC4

•  
 • 100 ~ 1000  
 •

• 가 가  
 가 가  
 가 가  
 • 가

+

## (Brute-force Attack)

가

( )

가

A B ( C ) , B A

, A B 가

가

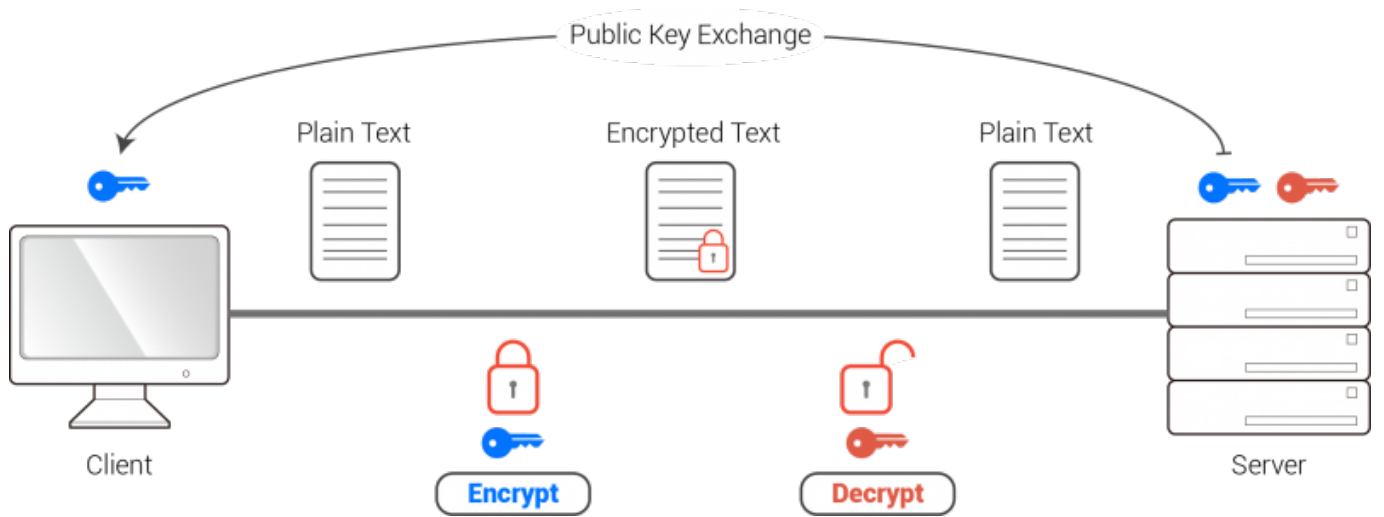
가

가

가

가

가



가

가

가

가

가

가

가

가

가

가

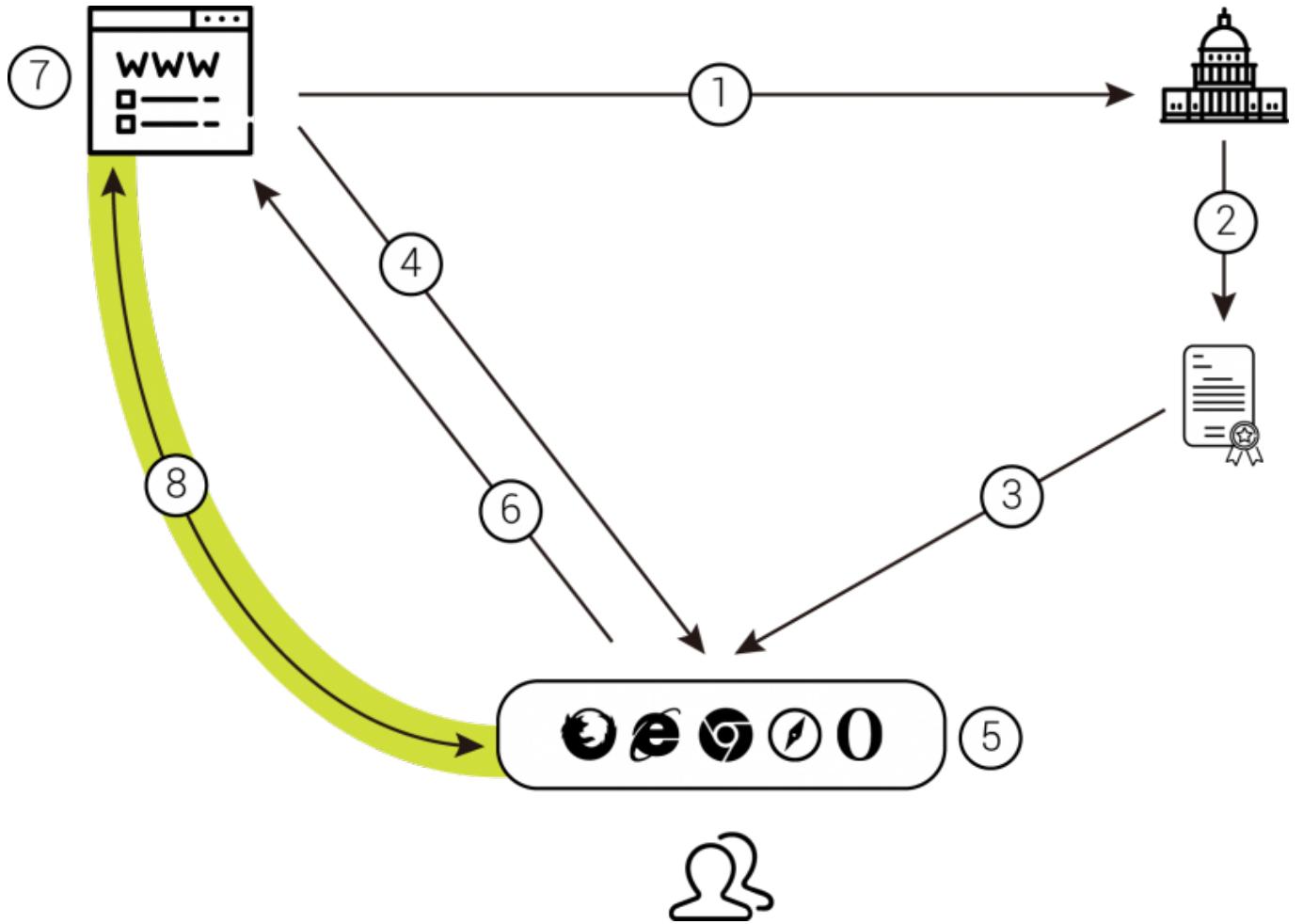
- RSA (Rivest-Shamir-Adleman cryptosystem)
- DSA (Digital Signature Algorithm)

- 가

- 100 ~ 1000 가
- 

가 , ,

SSL



- 1.
- 2.
3. SSL
4. 가 SSL
5. SSL
6. SSL
7. 가 가
- 8.
- \*

