HTTP - Hyper Text Transfer Protocol

- Plain text
- Layer 7 (application)
- Insecure
- Light weight
- Port 80

HTTPS - Hyper Text Transfer Protocol Secure

- Encrypted data
- Layer 4 (transport)
- Public and private key exchanging for encryption
- Heavier than http
- CA (Certificate Authority) - an entity that issues digital certificates
- Port 443

SSL - Secure Socket Layer
TLS - Transport Layer Security
SSL stripping is a technique by which a website is downgraded from https to http.

SSL encryption

- *Symmetric*
  One key.
- *Asymmetric*
  Public and private keys.

Algorithm

1. Server sends asymmetric public key to the browser.
2. Browser generates a symmetric session key.
3. Server receives encrypted session key and decrypts it with its private key.