3.5.1 Security

SSL | TLS

Decryption Prvt. Key.

→ Plain text

( ZAFAR )
A B G B S
Encryption Pub. Key
↘ Cypher text.

192.168.0.1 : 8080
IP Add. Port
Socket.

CNN.com

1. action request
2. Pub. Key
3. Encrypted Session Key
4. Welcome msg
5. Secured Communication Session Key

my Computer

Certificate Authority.

SSL

Pub.
Prvt.

Pub.
Prvt.

Bob      xchange Pub.      ALICE

- Pub. Prvt. Key Algorithm
- Asymmetric Encryption

- Symmetric Key -

**AUTHORISATION:** When using computers and networks such as Internet, we have to tell the server that who we are; this is called authorisation. Usually username, thumb impression or other means of biometric are used to authorise a person. <span style="color:red">E.g: username.</span>

**AUTHENTICATION:** After telling who you are (authorisation), it is necessary to prove that as well. This is a required process so that no one without proper proof could access our accounts. <span style="color:red">E.g: password.</span>