

#flo #inclass #atomic

1 | Internet Security

go to website -> website gives certificate -> which is signed using the bank's private key and verified by our browser with the public key

basic outline: - Authentication - the person you are communicating with is in fact the bank

- TLS (transport layer security)
 - privacy
 - generate symmetric key
 - * with asymmetric protocol?
- Untampered
 - hashes a message, gives the hash, checks the hashes against each other to make sure they haven't been tampered with

and now, we can send in the authentication credentials (password)

1.0.1 | Factors

also, 2FA! or rather, 3FA? multi-factor auth. types of factors: something i know, something i am, and something i have -> password, fingerprints, phone number 2FA usually uses the first and the last, whereas iPhone uses the first and the second.