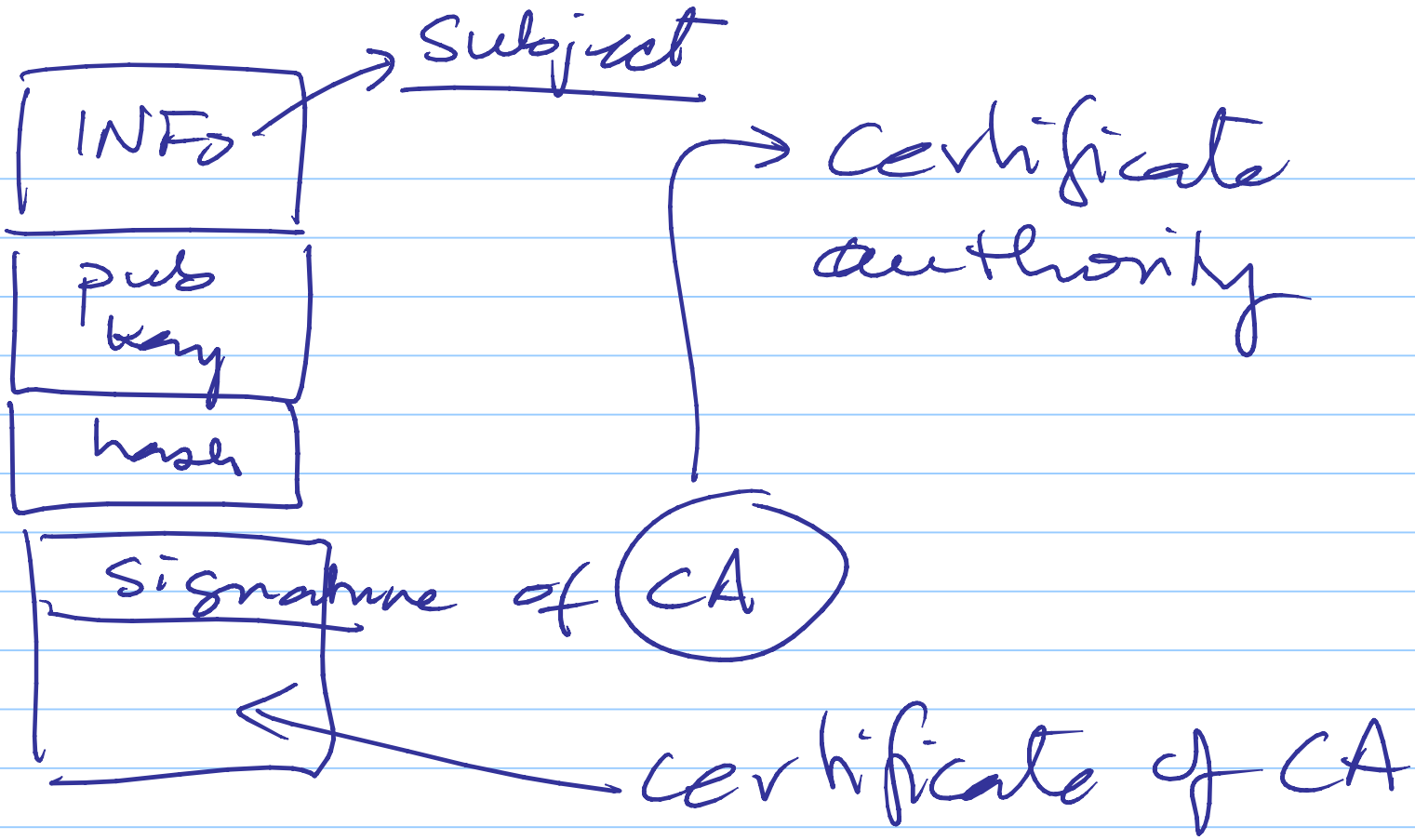
Note Title

Web encryption / security

- certificates → public information
  → not encrypted
  → ties a name to a public key


Subject
INFO
pub key
hash
Signature of CA
certificate
authority
certificate of CA

Verify a certificate

→ get all the info in the cert (subject, subject pub key)

→ generate a hash (using correct function)

↳ x

→ decrypt the signature with the CA's public key ← how to get this?

CA
CA cert
CA pub key
CA name etc
info
issuer
sig

CA cert

↳ obtain from certificate store

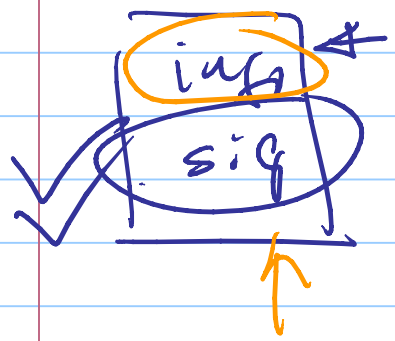
- windows cert store
- Chrome " "
- firefox cert store

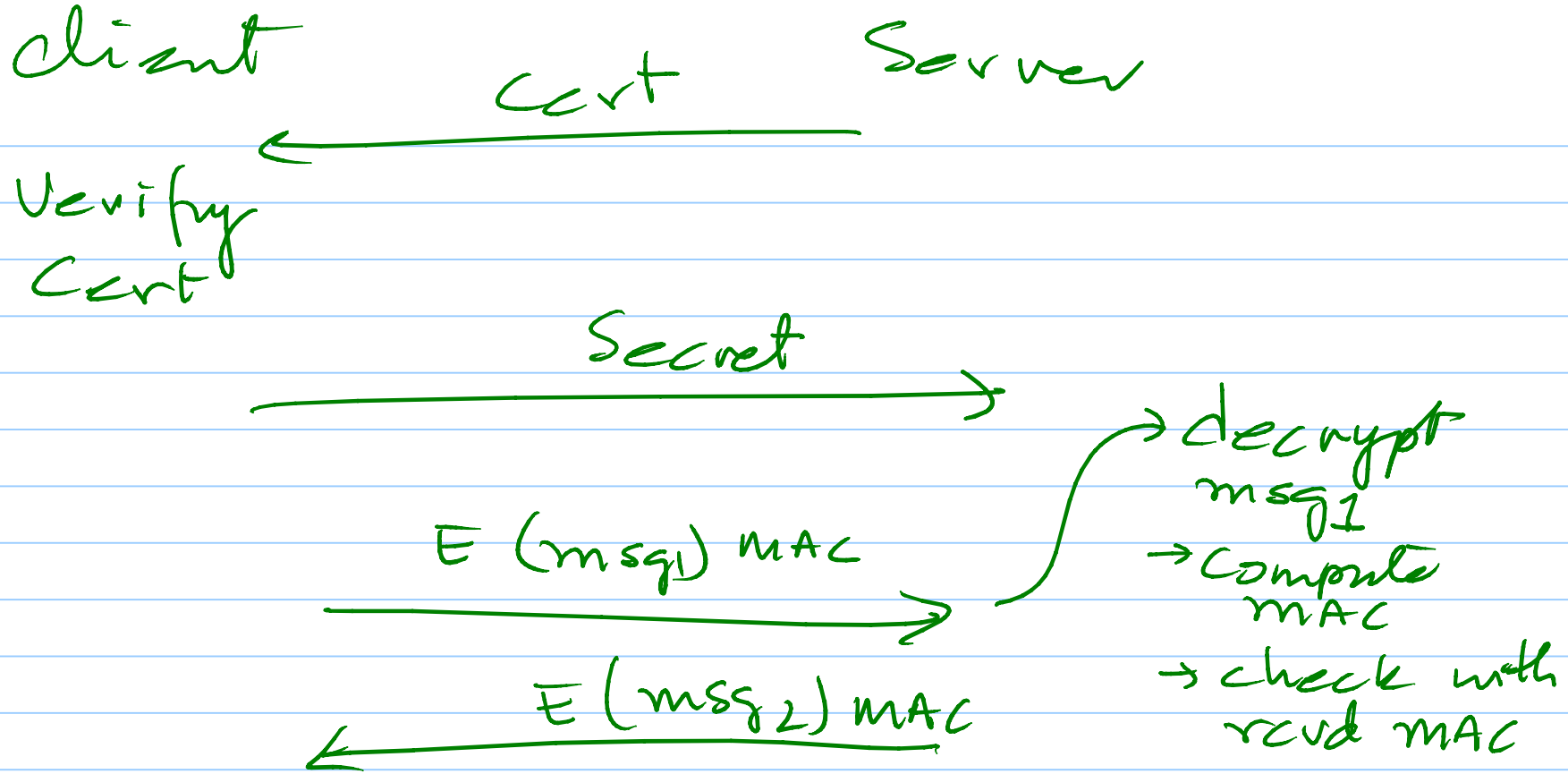
Certificate authority responsibilities

- Verify subject name & public key
- Keep CA private key secure
- sign the certificate

- Verify CA signed certificate

- Verify subject important




client
Server
cert
Verify cert
Secret
E (msg1) MAC
decrypt msg1
→ compute MAC
→ check with rcvd MAC
E (msg2) MAC