Authentication

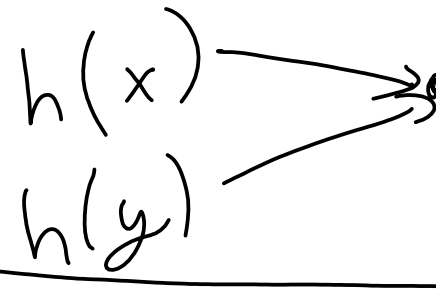
factors: something you...

- know (password, code, ...)
- have (phone, key ...)
- are (fingerprints, face, eyes...)

---

passwords

hash: non-invertable function



---

h(password)

store w/ user info

---

log in: username, password

check for match w/ h(password)

---

same pass hash to same value

salt value - random string

$h(passwd \oplus salt)$

$h("123456", 7421) \neq h("123456", 3754)$

store hashed pwd, salt

Securing Data - encryption

- at rest (file, db)
- in motion (communication) https tls
- in process (CPU, memory)

erase pwd after use in mem.

Encryption: (use well known algorithms)

Symmetric Key - same key for encrypt/decrypt

AES - advanced encryption standard

Public Key - K^+, K^-

public private

encrypt w/ K^+

decrypt w/ K^-

---

1. communicate w/ public/private key
2. "exchange" a symmetric key
3. comm. w/ symmetric

---

private key: digital signatures

sign a hash of a document: d

$h(d)$

sign: $K^-(h(d))$

↑ encode

verify: $K^+(K^-(h(d))) = h(d)$ is this $h(d)$?

↑ decode

matches when K^+, K^- are a key pair and d is the doc. that was signed