Fingerprint — unique, available, immutable, are everywhere
small hard to forge

Hash — 1-way det func
diff input → diff output (usually)
fast
hard to forge
small output

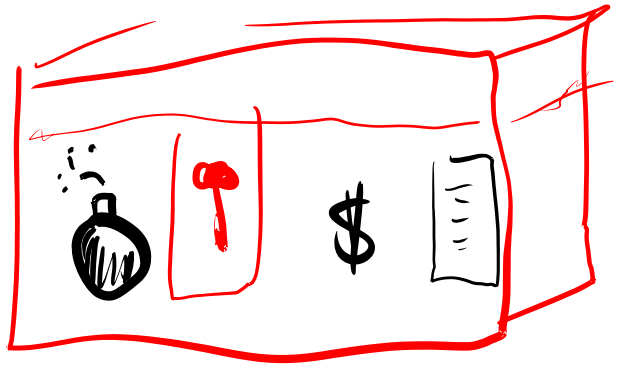
Sha-1
Sha-2
sha-256

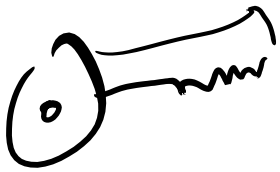
return 1

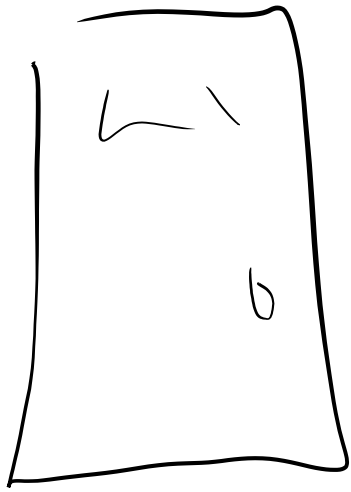
$(k+1) \bmod 32$

$(k^{811}) \bmod 32$

$(C[i] \cdot seed[i]) \% old$
prime







Symmetric cipher

same key (lock — encrypt
unlock — decrypt

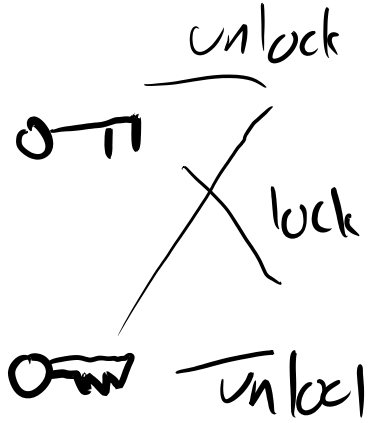
AES

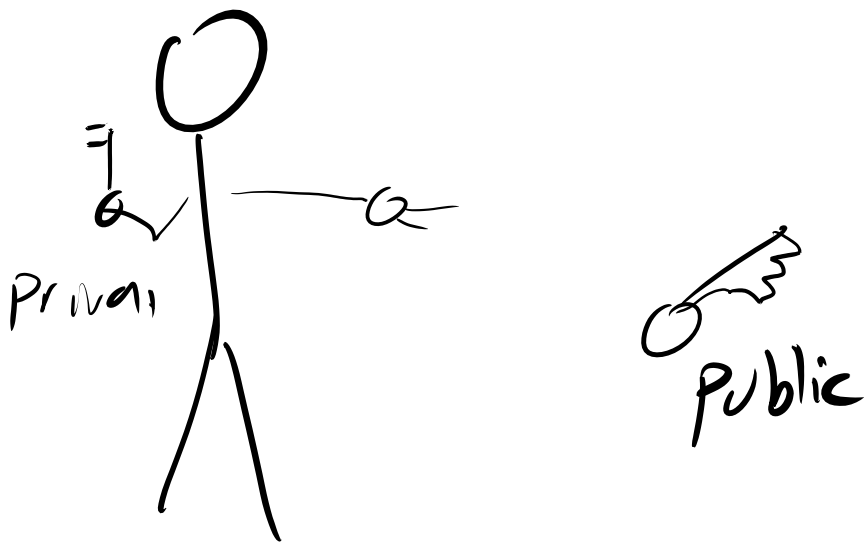
handwriting 1 person create, many read

telephone number any ↔ 1

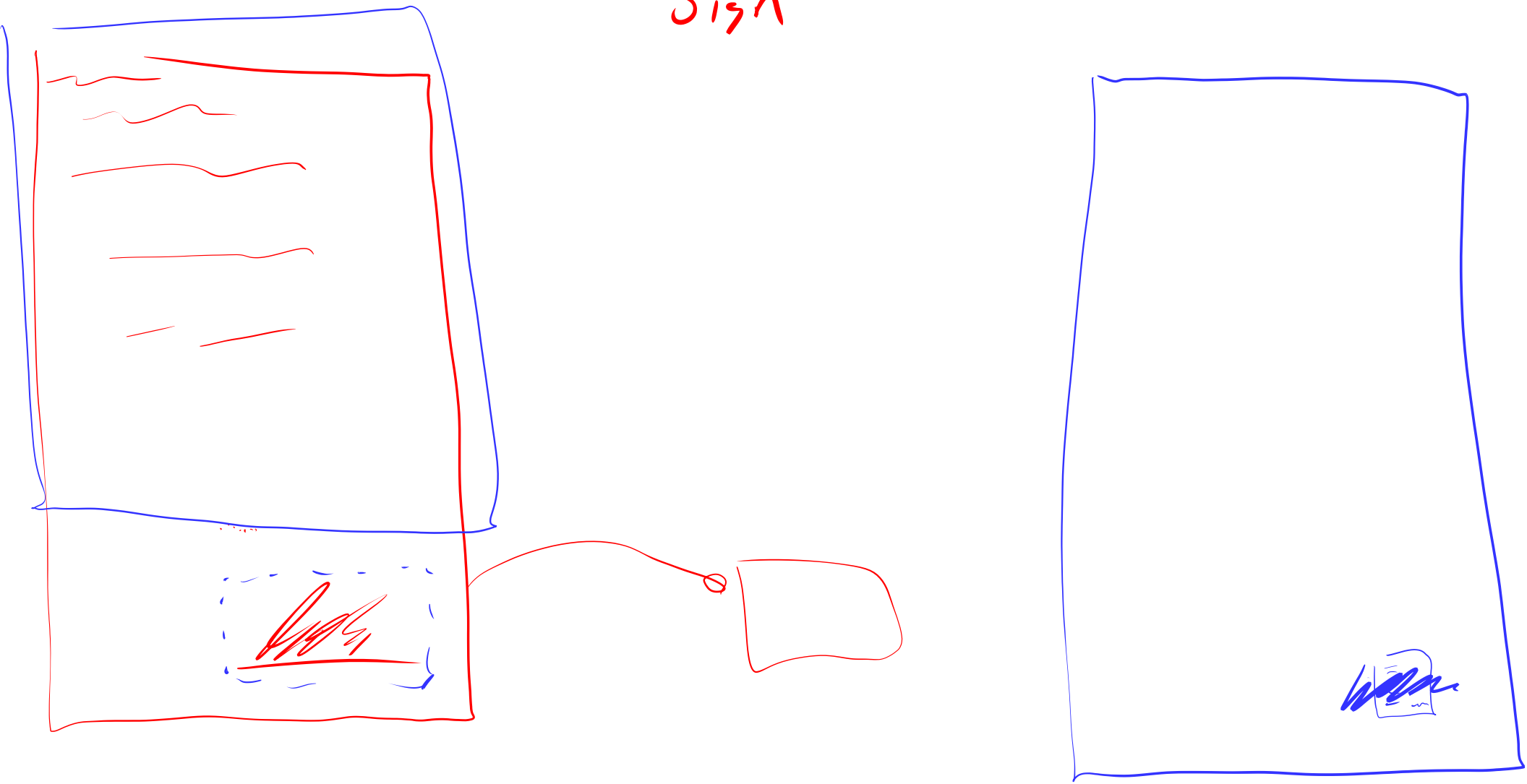
public-key cipher

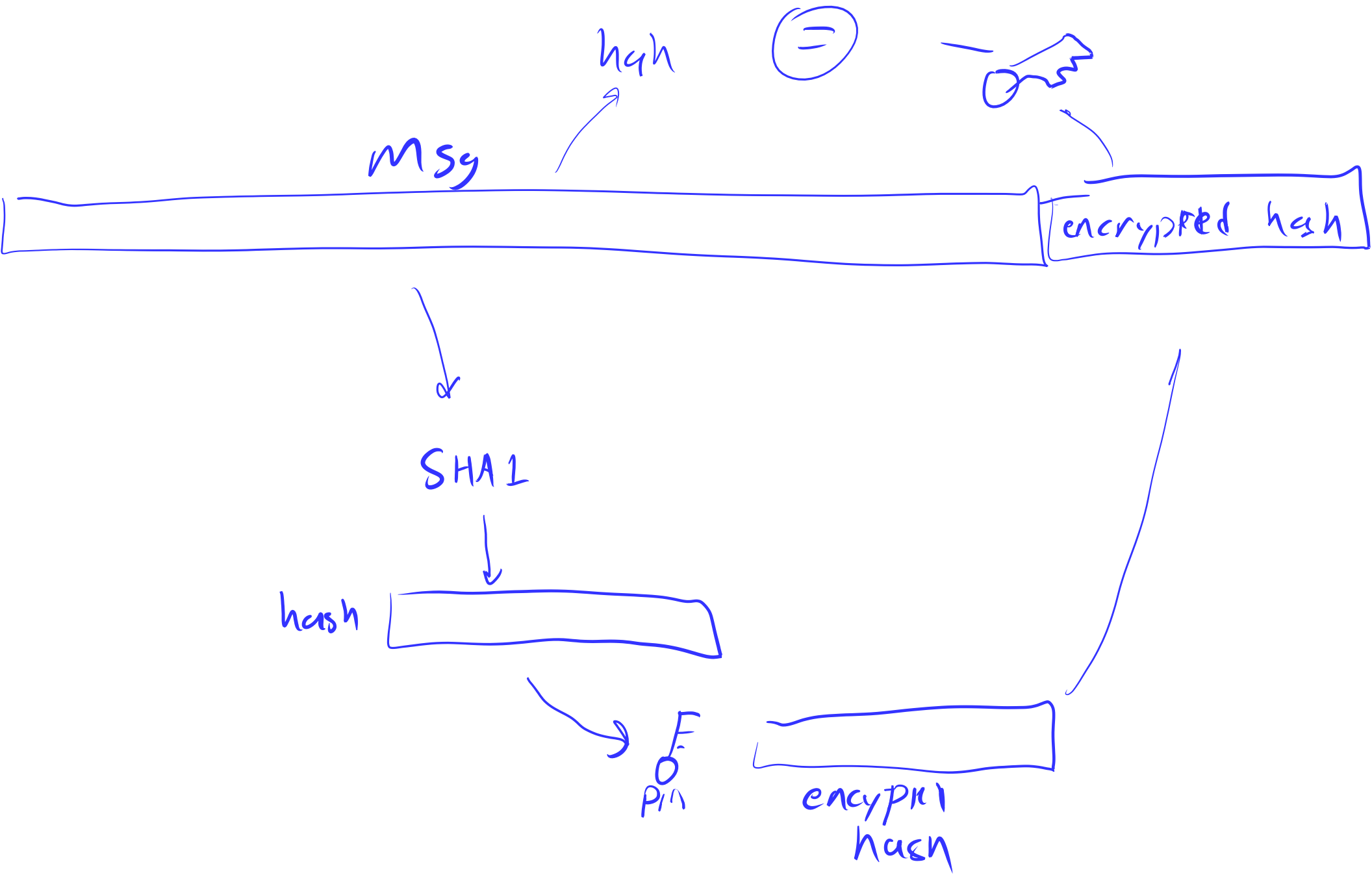
RSA

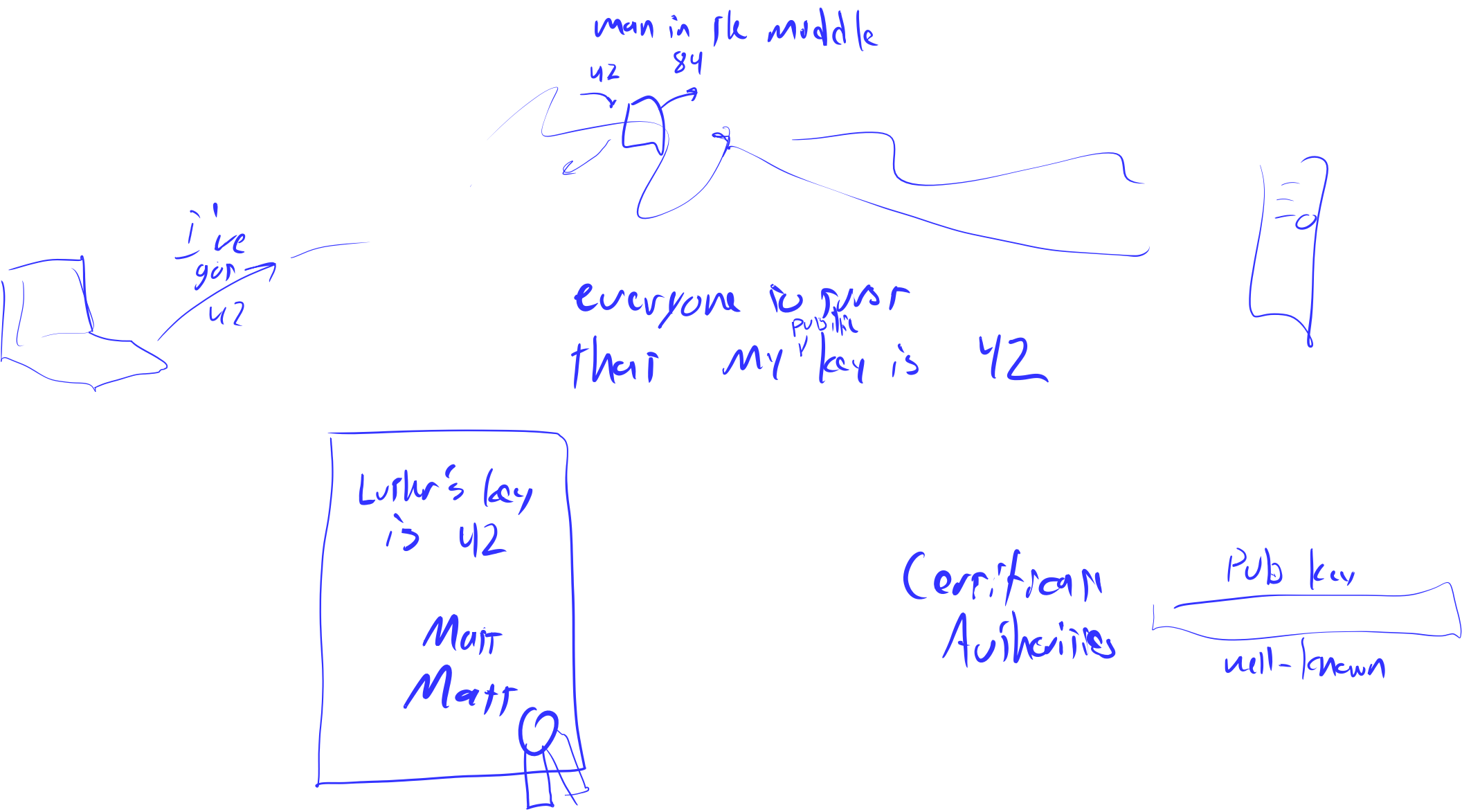


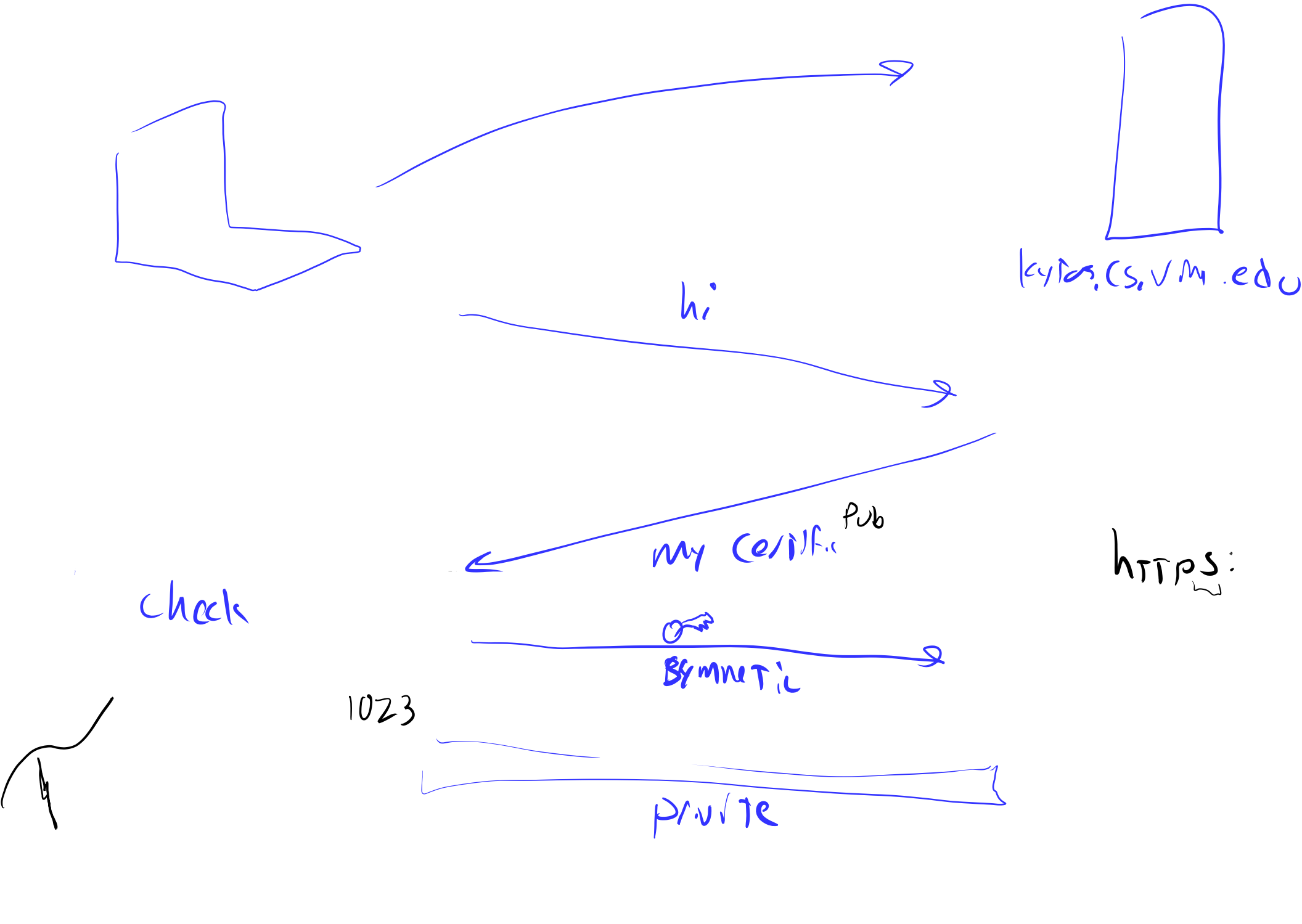


Sign




hash
=
Msg
encrypted hash
SHA1
hash
F
PK
encrypt
hash


man in the middle
42
84
i've got 42
everyone in town that my public key is 42
Luthor's key is 42
Matt
Matt
Certificate Authorities
Pub key
well-known


hi
check
1023