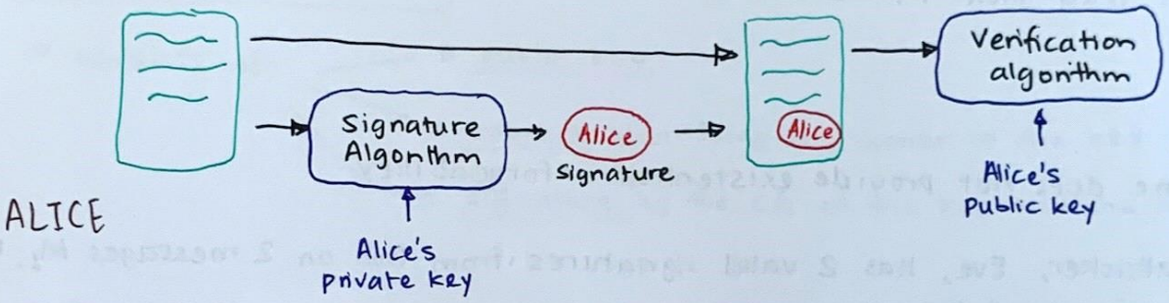
CRYPTOGRAPHY:

DIGITAL SIGNATURE & CERTIFICATES

→ is a way for an entity to demonstrate the authenticity of a message by binding its identity w/ tht. message



ADVANTAGES OVER MACs

1) MACs are not publicly verifiable (and so not transferable)
   - No one else, except Bob, can verify tag t

2) MACs do not provide non-repudiation → If Alice signs a doc. w/ her secret key, she cannot deny it later!
   - Tag t is not bound to Alice's identity only.
   - Alice could claim thr. she didn't compute t herself. It could be Bob since he also knows the key k

→ A good digital signature shld. satisfy existential unforgeability

RSA SIGNATURE

→ Bob encrypts a message M using his secret key d as ff:

$$S = M^d \bmod n$$

→ Any third party can verify this signature w/ the public key (e, n):

Is it true that $M = S^e \bmod n$?

PROBLEMS

→ This scheme does not provide existential unforgeability

e.g. An attacker, Eve, has 2 valid signatures from Bob on 2 messages M_1, M_2

$$S_1 = M_1^d \bmod n \quad \text{and} \quad S_2 = M_2^d \bmod n$$

Eve could produce a new signature which would validate as a verifiable signature from Bob on the message $M_1 \cdot M_2$:

$$S_1 \cdot S_2 \bmod n = (M_1 \cdot M_2)^d \bmod n$$

→ This can be solved by using CHF; apply a hash fn H before computing RSA fn

SIGNING $\quad S = (M, H(M)^d \pmod n)$

VERIFYING $\quad V = \begin{cases} T & \text{if } H(M) = S^e \bmod n \\ \perp & \text{otherwise} \end{cases}$

PUBLIC KEY INFRASTRUCTURE (PKI)

→ is used to establish & manage public-key encryption

→ How does Alice trust that pk_{Amazon} is Amazon's public key?

PUBLIC-KEY CERTIFICATE

→ consists of:
- a public key
- a subject identifying the owner of the key
- a signature by the CA on the key and the subject binding them tgther

→ The X.509 standard defines the most commonly used format for pk certificates

CHAIN OF TRUST

→ Having a single CA sign all certificates is not practical

→ Instead, a root CA signs certificates for level 1 CAs, and so on...

Transitive trust

root of trust is embedded in our OS and browser

REVOCATION

→ A certificate needs to be revoked if the corresponding private key has been compromised

→ Certificate Revocation Lists (CRL) are the soln adopted in X.509

→ Online certificate status Protocol (OCSP) is the modern soln

→ Our web browser will also get an update on all revoked certificates