Digital Signatures:

First zero knowledge proof:
I know the secret key, but won't reveal

RSA Signatures:

Gen (1^n): same as PKC

$\text{sign}_{sk}(m) = \sigma$

$\text{Vrfy}_{pk}(m, \sigma) = \text{Yes}/\text{No}$

Signing : $\sigma = m^d \mod N$

Vrfy : $\langle m, \sigma \rangle$

Yes if $m = \sigma^e \mod N$

where $pk = \langle N, e \rangle$ $N = pq$ $(e, \phi(N)) = 1$,

$s_k = \langle p, q, d \rangle$ $ed \equiv 1 \pmod{\phi(N)}$

Insecurity of textbook RSA signatures

Forging RSA signatures:

Choose message as : Choose random σ

$m = \sigma^e \mod N$

$\langle m, \sigma \rangle$

Create signature then get corresponding message. Verification will pass even though the message was never sent, but adversary does not have control over the message.

RSA, like El Gamal is multiplicatively homomorphic

$m'', \sigma'' = ?$

$$\left.\begin{matrix} mm', \sigma' \\ m, \sigma \end{matrix}\right\} \frac{mm'}{m} = m''$$

$$m'', \sigma'' = \frac{\sigma'}{\sigma}$$

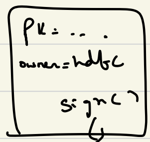
Hash & Sign Paradigm:

RSA Signatures

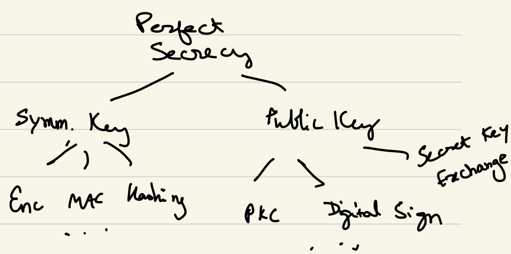
Sign : $\sigma = (H(m))^d \mod N$

Vrfy : m, σ Check: $H(m) \stackrel{?}{=} \sigma^e \mod N$

Digital Certificates:



By certification authority (CA) whose pk is known



a) Oblivious Transfer
b) Master Theorem (private protocol for any task)
c) Zero Knowledge Proof
d) Bit Commitment
e) Secret Sharing
f) Quantum Crypto g) Noisy Channels
h) Impossibility interference