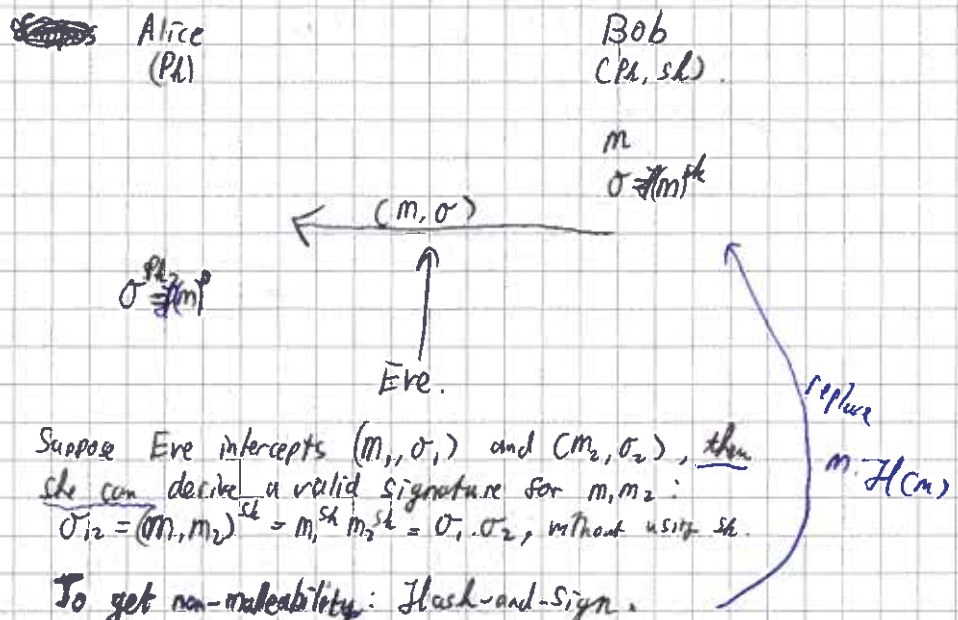
Hash functions and Message Authentication Codes

Motivation: → Non-Malleability of e.g. RSA-signature schemes:

Application



Suppose Eve intercepts (m_1, σ_1) and (m_2, σ_2), then she can decide a valid signature for $m_1 m_2$:
$\sigma_{12} = (m_1 m_2)^{sk} = m_1^{sk} m_2^{sk} = \sigma_1 \cdot \sigma_2$, without using sk.

To get non-malleability: Hash-and-Sign.

replace $\sigma = m^{sk}$, by $\sigma = H(m)^{sk}$

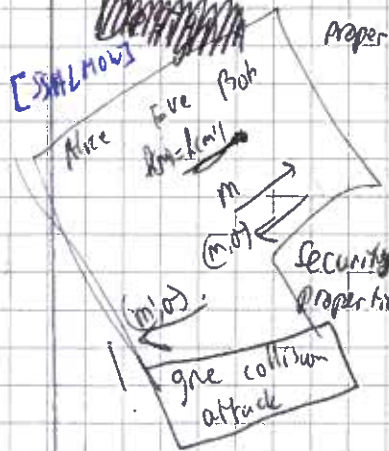
→ Signing long messages.

Note: - RSA-Signature scheme can compute signatures for messages of at most the size of the keys.
- Splitting each message in blocks and sign each block is time-consuming and insecure! (can swap signatures to get a valid signature).

→ Message Authentication codes (upcoming).

→ To implement a random Oracle in Cryptographic protocols.

Properties



properties: → $h: \{0,1\}^* \to \{0,1\}^k$; has input of arbitrary length and a fixed length output.

→ low running time and easy to compute

H_1: Pre-image Resistance: given $h_1 = h(m)$ it should be hard to find m such that $h_1 = h(m)$. (meaning it should take $O(2^k)$ time; the time of exhaustive search).

H_2: Second-preimage Resistance (Weak collision Resistance): given $m, h_1 = h(m)$ it should be hard to find m' such that $m \neq m'$ and $h(m) = h(m')$. (it should also take $O(2^k)$ time).

H_3: (Strong) Collision Resistance: It should be hard to find m, m', where $m \neq m'$ and $h(m) = h(m')$.
(It should take $O(2^{k/2})$ time: the time of exhaustive search due to Birthday paradox)

Birthday paradox: generalized version of the following observation: one needs just $20 \approx \sqrt{365}$ people to have w.h.p. two people with the same birthday.