Message Authentication Codes (MACs) 

→ Can be used as an equivalent replacement for Signatures.

* Alice and Bob share the same shared secret (e.g., DM-key exchange).
* Alice and Bob don't care about non-repudiation.

Bob cannot convince a third party that a message is from Alice, since it would also make the same signature.

Even if Eve not knowing the key, any output should be equally likely.

Weak constructions:

→ $\mathcal{H}_k(m) = \mathcal{H}(\mathcal{H}(m))$ (Suffix MACs)

If $\mathcal{H}$ has MD construction, design $\mathcal{H}_k$ as:

$$\mathcal{H}_k(m) = \mathcal{H}(m') = \mathcal{H}(m)$$

Once fake signatures can be generated, without knowing the key, and security reduces to plain hashing.

If length $m$ and length $m'$ are equal, the strengthened MD construction fails.

→ $H_k(m) = H(\mathcal{H}(m))$ (Prefix MACs)

again if $\mathcal{H}$ has MD construction, so design $H_k$ as:

$$H_k(m) = \mathcal{H}(m) = \mathcal{H}(m', m) = \mathcal{H}(C(m', m)) = \mathcal{H}(H_k(m) \oplus m)$$

Since without knowledge of $k$, a valid signature can be computed for on a different message.

Does not work in the strengthened version.

Typical constructions - HMAC: $H_k(m) = \mathcal{H}(\mathcal{H}(m) \oplus \mathcal{H}(E_k(m)))$

Extra security: $E_k(m) \oplus \mathcal{H}(E_k(m))$

Alice

(\(k\))

Bob

(\(k\))

Agent $m$ as message from Bob.

$\mathcal{H}(m) = \mathcal{H}(k)$

In practice, it is not required to insert $m$.