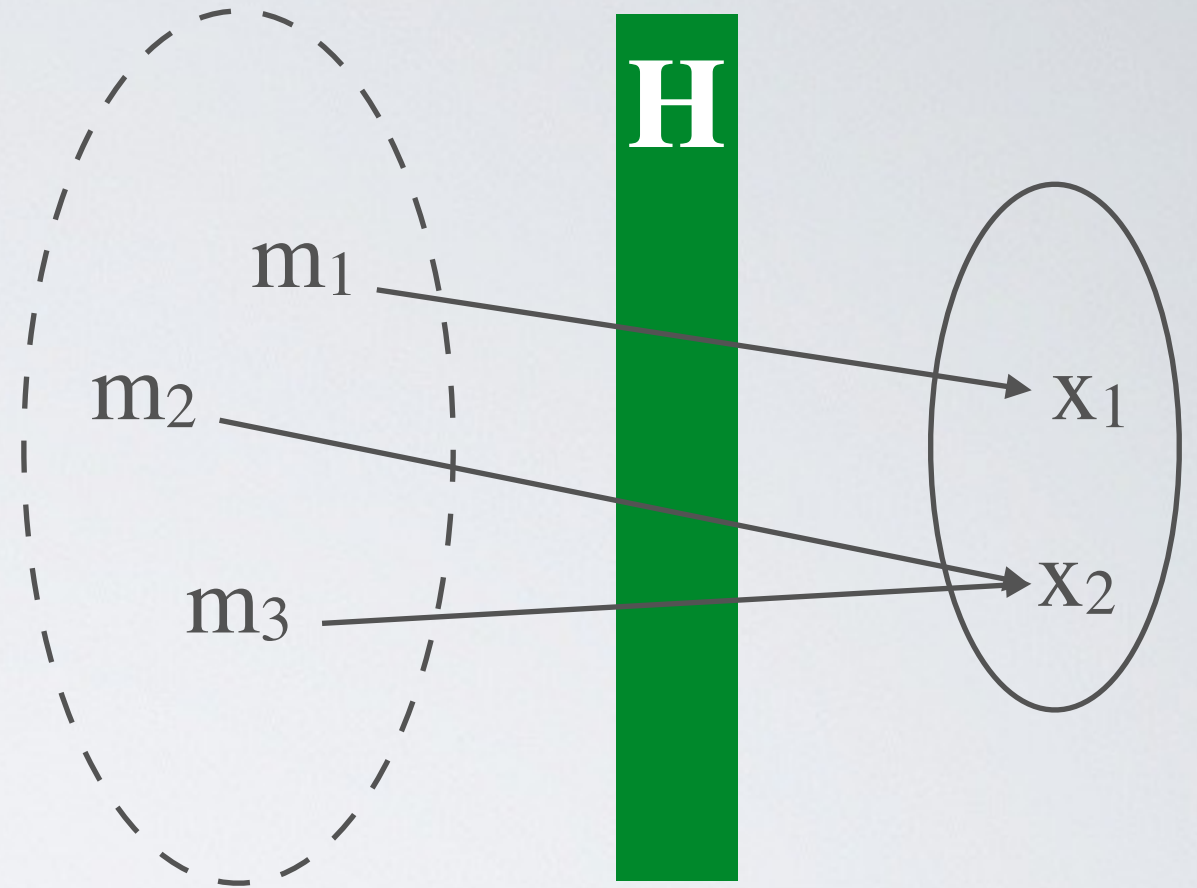# Message digests

Message digests are meant for creating fingerprints of messages

- Un-keyed message digest : hashes, checksum

- Keyed message digests : MACs

Cryptographic hashing

$H(m) = x$ is a hash function if

- H is one-way function

- m is a message of any length

- x is a message digest of a fixed length

➡ H is a lossy compression function
  necessarily there exists x, m_1 and m_2 | $H(m_1) = H(m_2) = x$