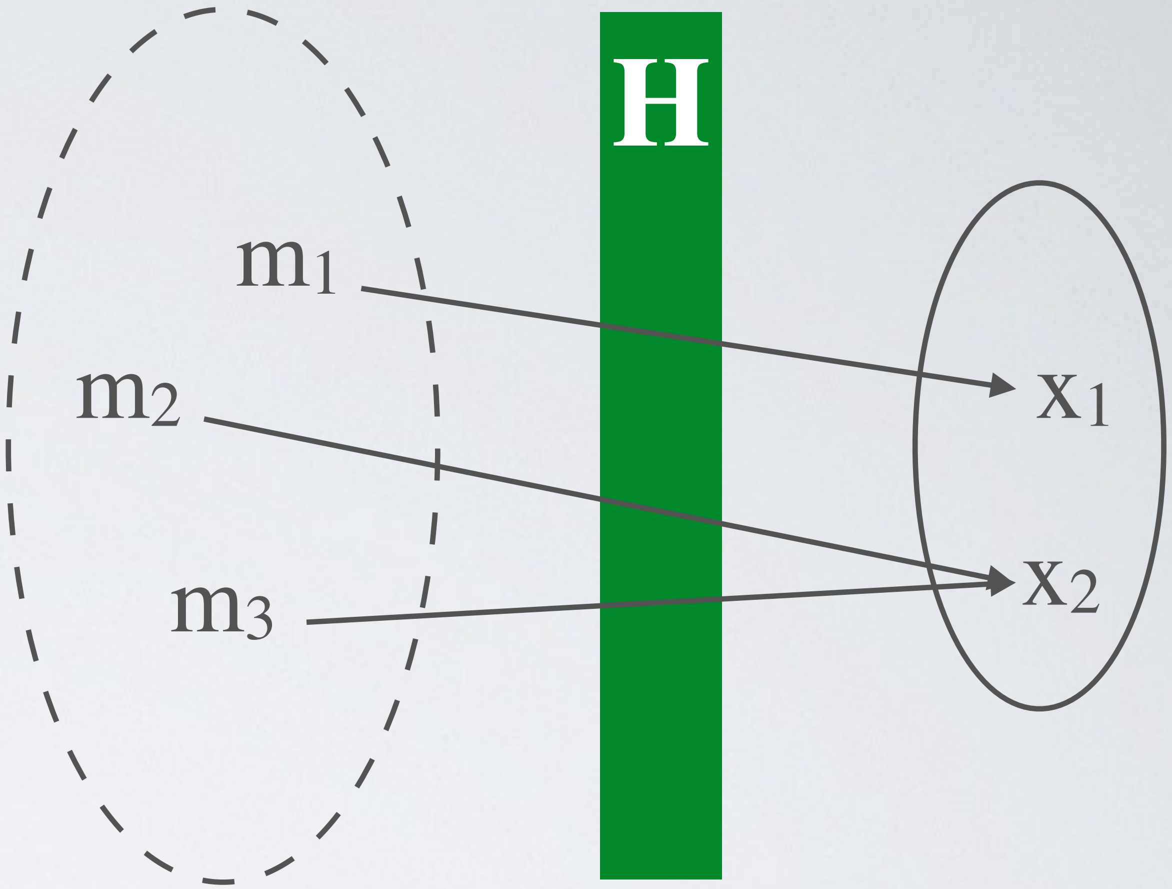
Cryptographic hashing

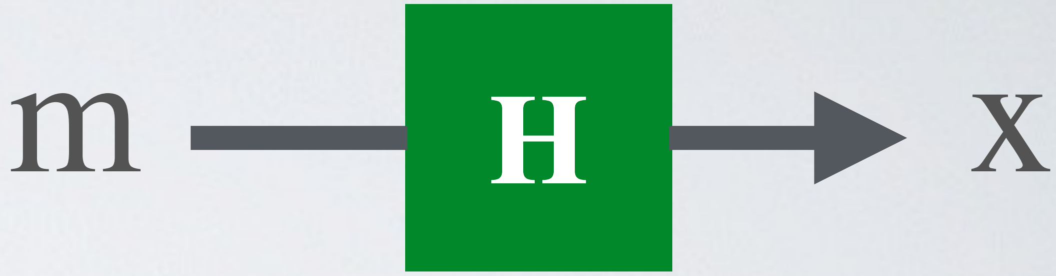


$H(m) = x$ is a hash function if

- 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 | $H(m_1) = H(m_2) = x$

Computational complexity



- Given H and m, computing x is **easy** (polynomial or linear)
- Given H and x, computing m is **hard** (exponential)

➡ H is **not invertible**