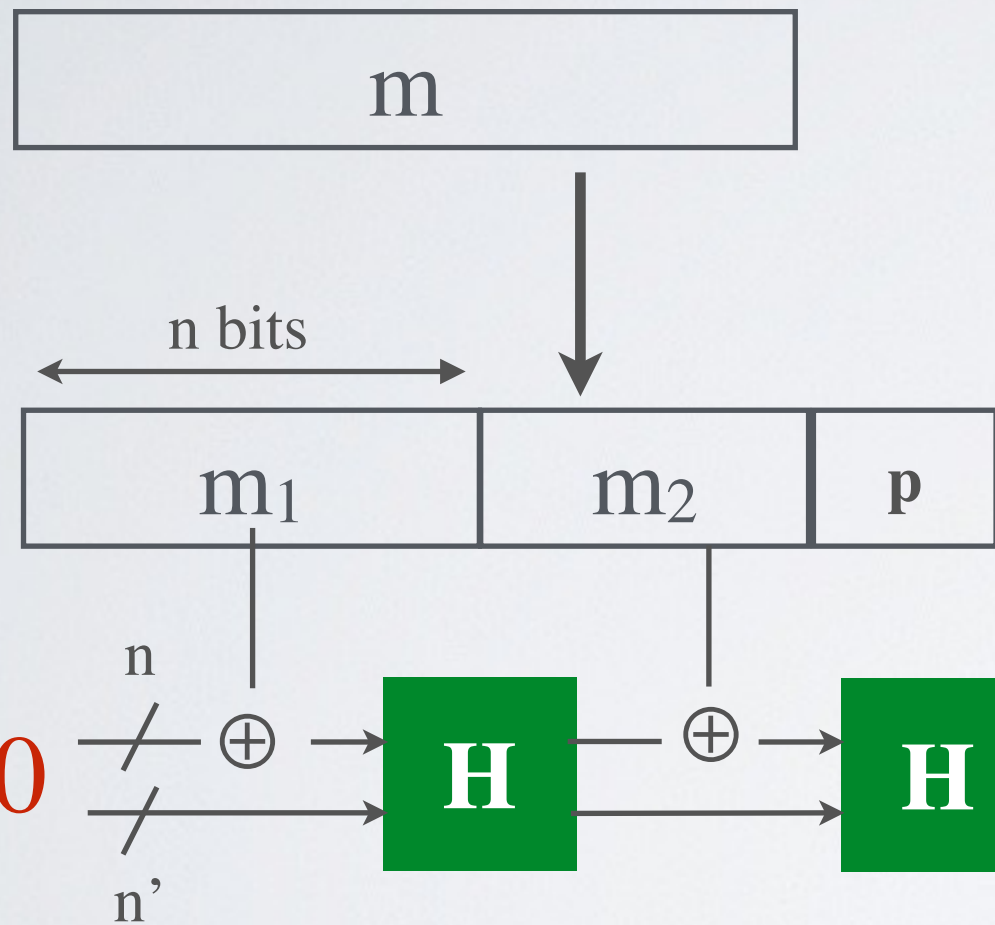


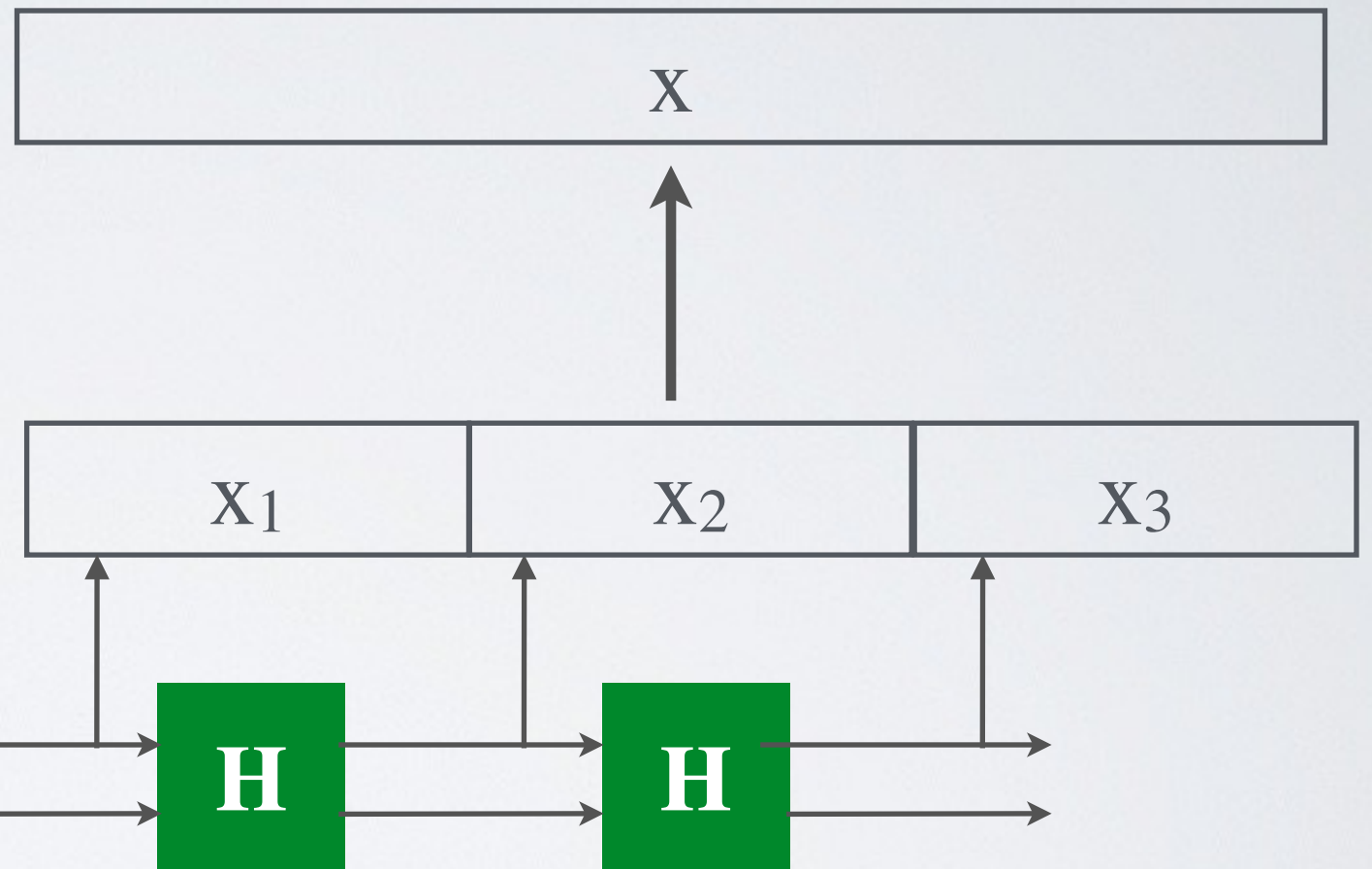
How to hash long messages ?

Sponge construction (SHA-3)

split m in blocks of n bits
and add padding p



assemble the hash



absorbing : *squeezing*

Property : if H is CR then Sponge is CR

Brute-forcing a hash function



CR - Collision Resistance

➡ given H , hard to find m and m' such that $H(m) = H(m') = x$

Given a hash function H of n bits output

- There are 2^n hashes
- Given a specific hash, an attacker will find the corresponding input in ~~2^{n-1} tries~~