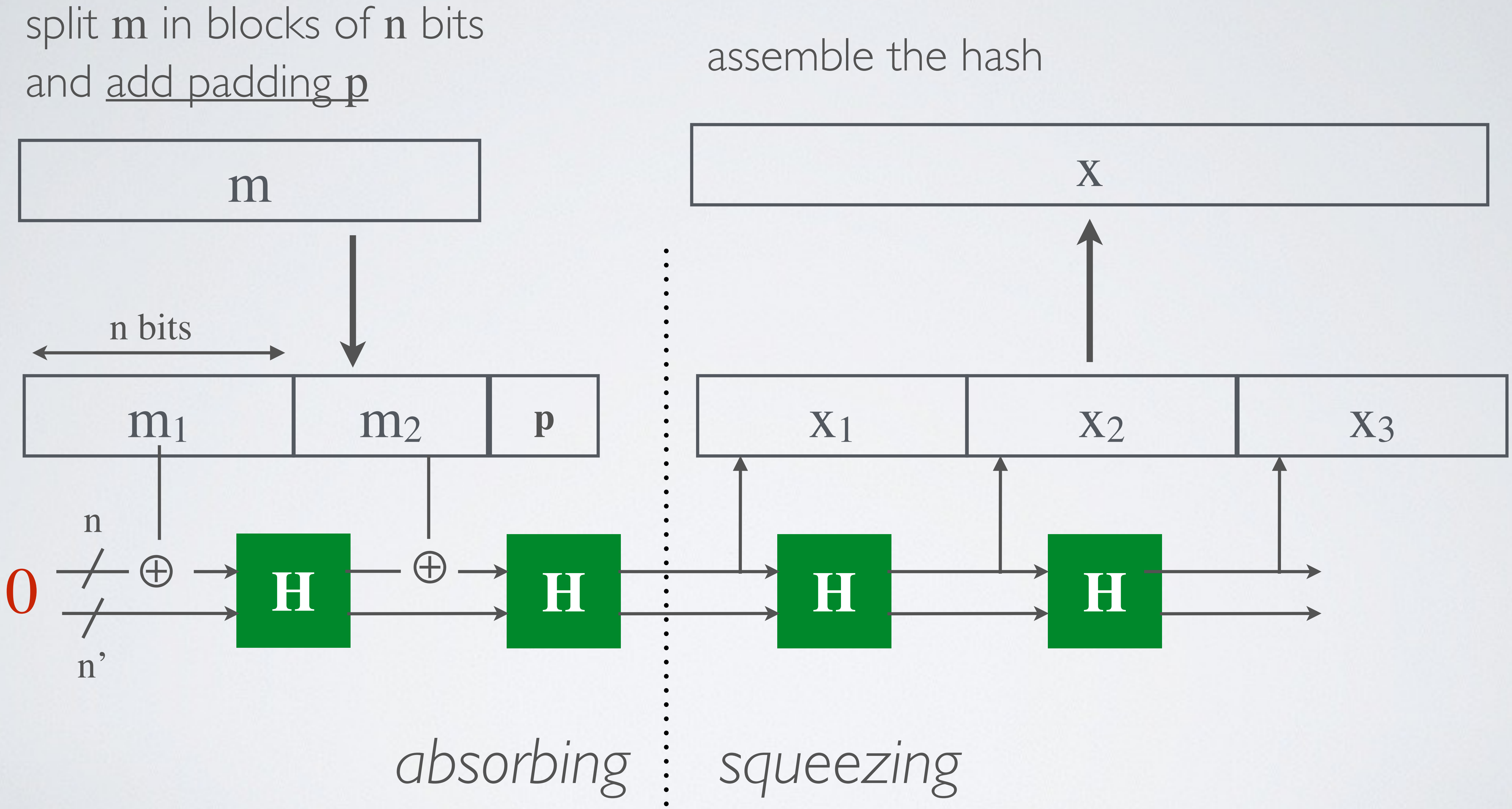
How to hash long messages ?

Sponge construction (SHA-3)



Property : if **H** is CR then Sponge is CR

Brute-forcing a hash function

CR - Collision Resistance

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

Given a hash function $\mathbf{H}$ of $\mathbf{n}$ bits output

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