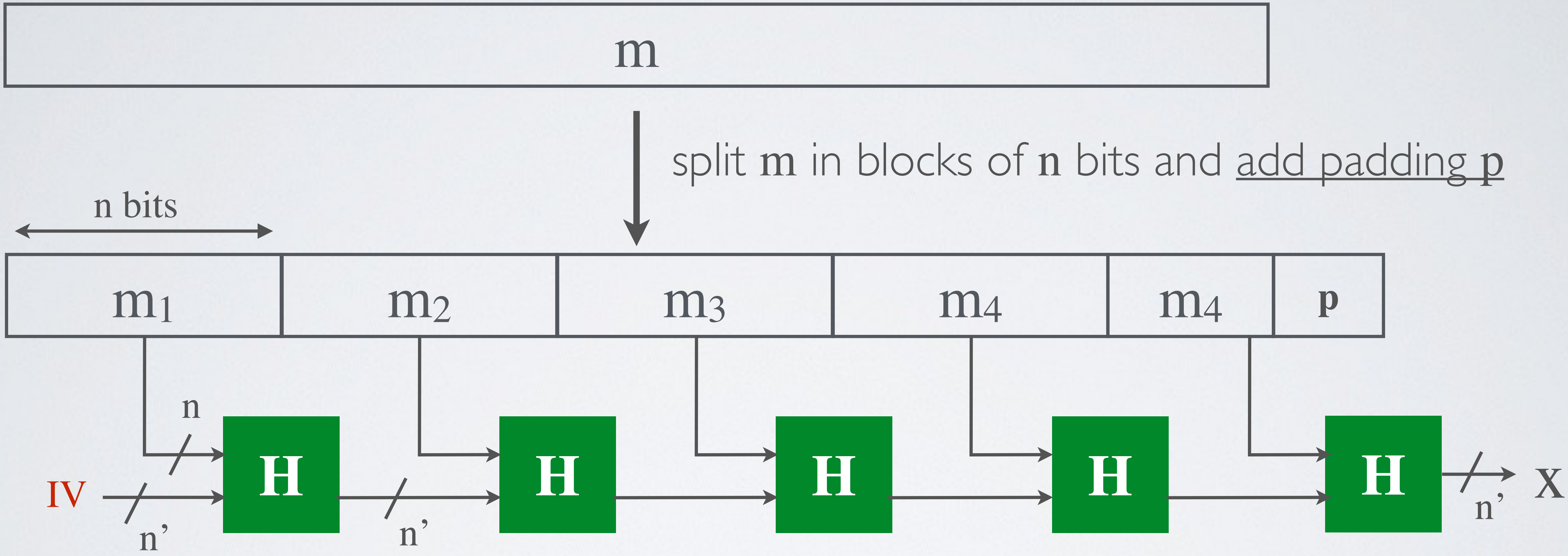
How to hash long messages ?

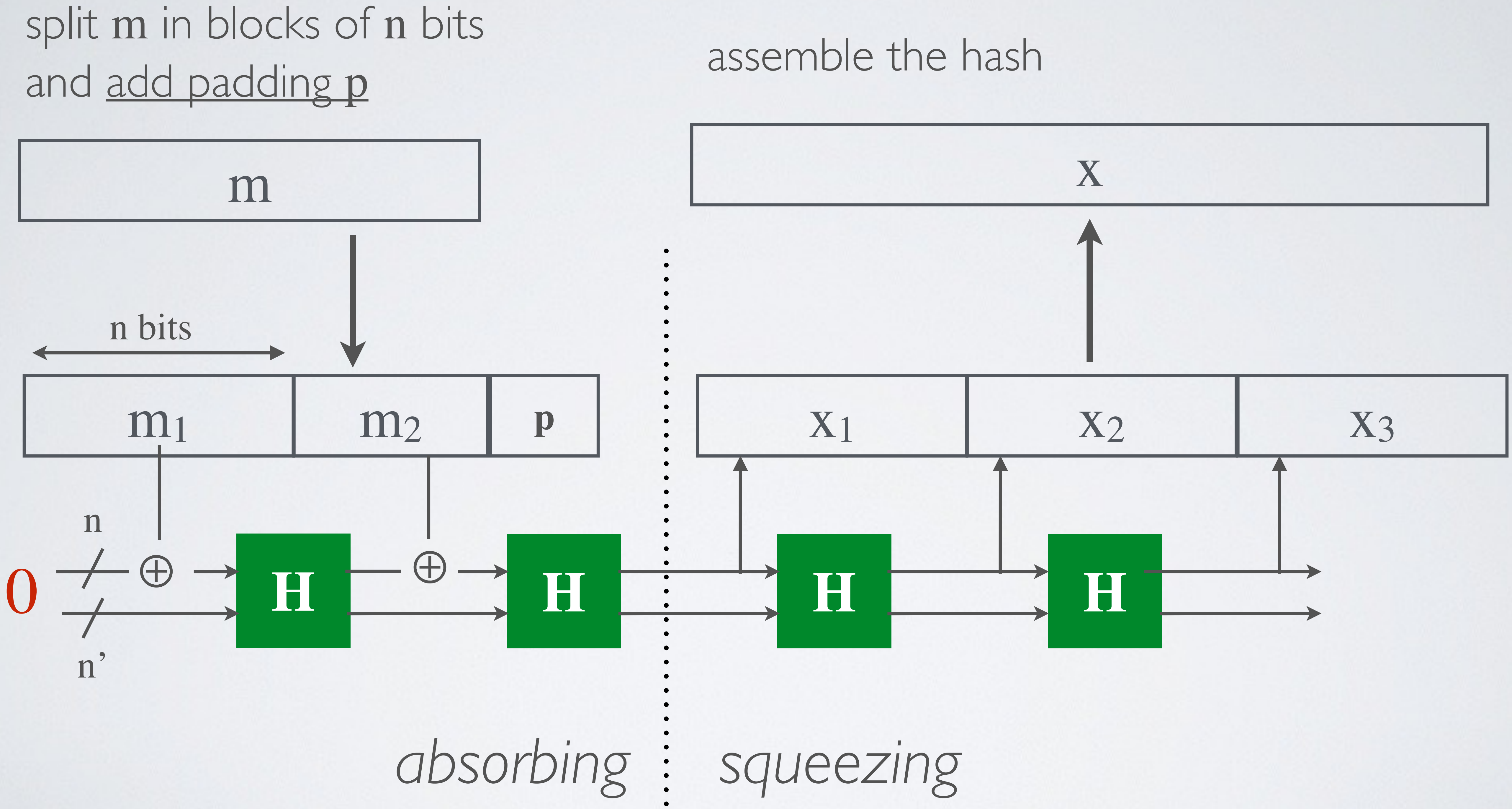
Merkle–Damgård construction (MD5, SHA-1 and SHA-2)



Property : if H is CR then Merkel-Damgard is CR

How to hash long messages ?

Sponge construction (SHA-3)



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