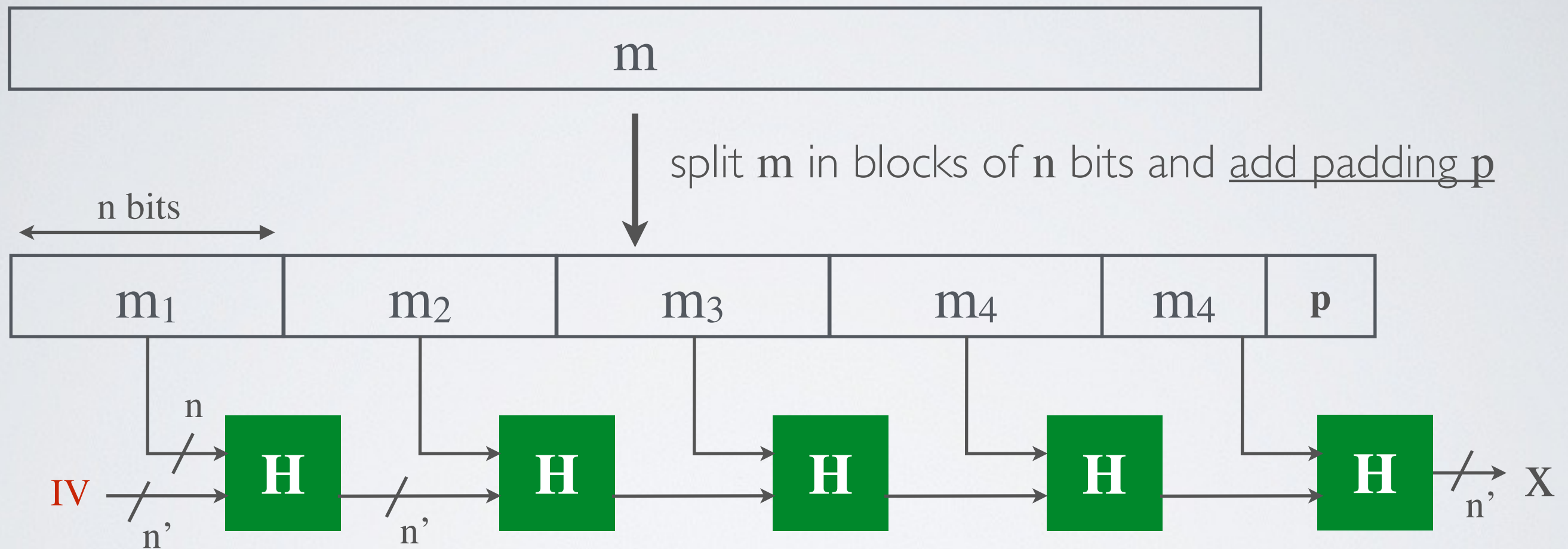


How to hash long messages ?

Merkle–Damgård construction



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

Using hash functions for Integrity