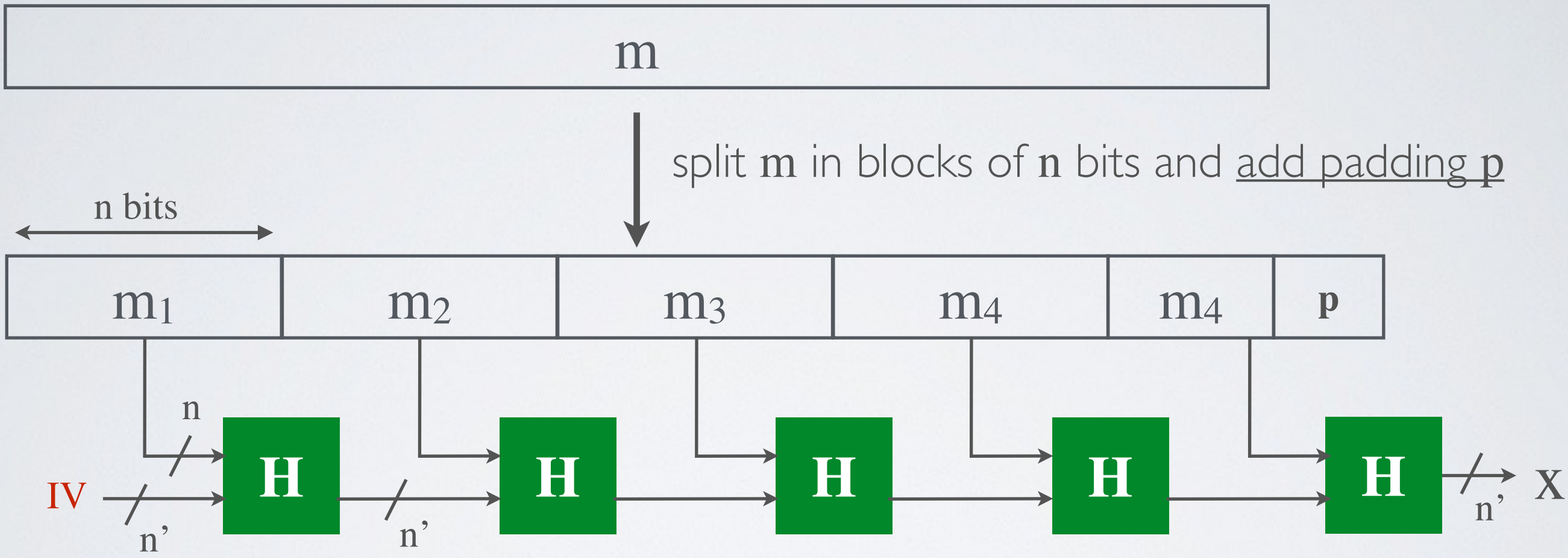
How to hash long messages ?
Merkle–Damgård construction



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

Security of hash functions