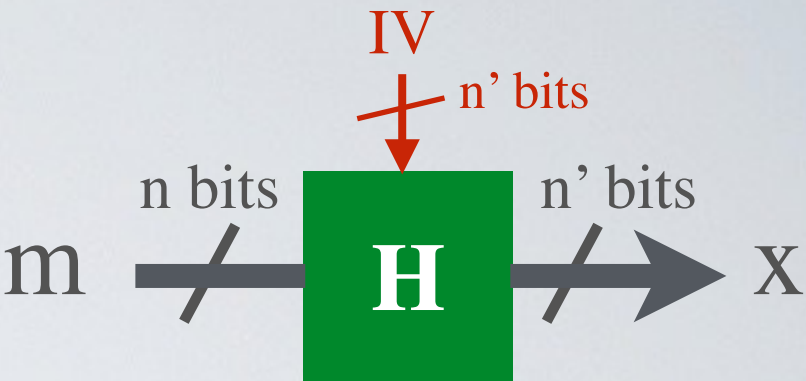


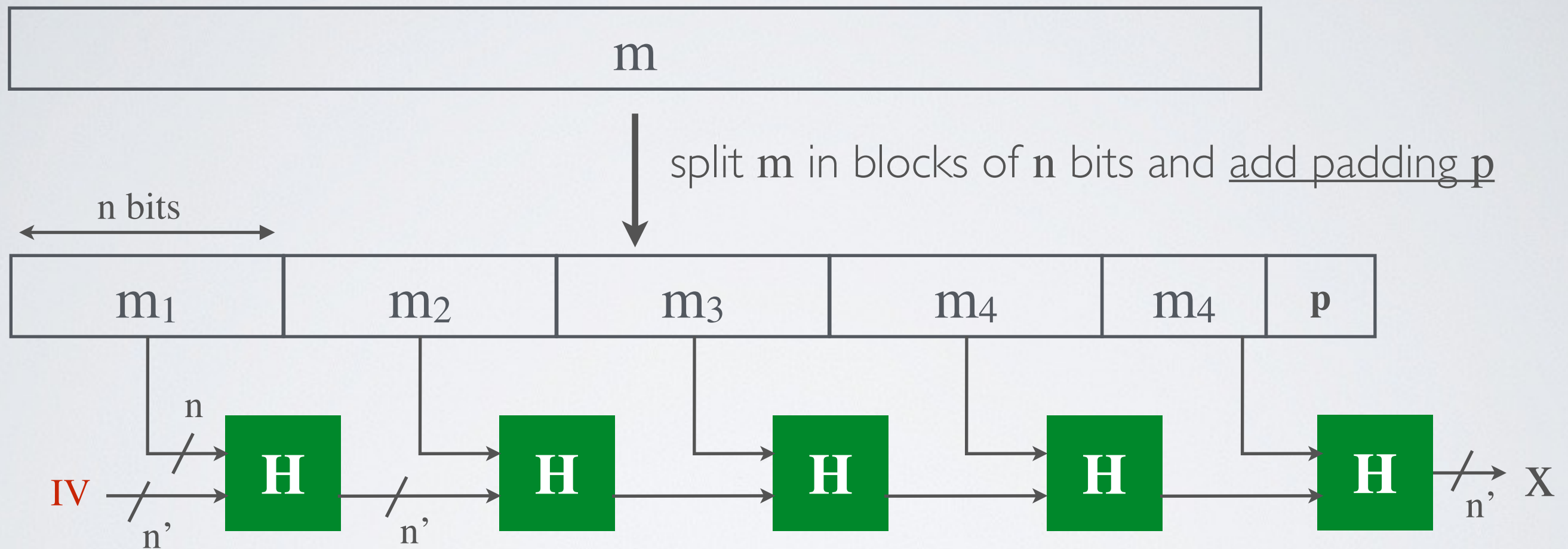
Common hash functions



Name	MD5	SHA-1	SHA-2				SHA-3			
Variant			SHA-224	SHA-256	SHA-384	SHA-512	SHA3-224	SHA3-256	SHA3-384	SHA3-512
Year	1992	1993	2001				2012			
Designer	Rivest	NSA	NSA				Guido Bertoni, Joan Daemen, Michaël Peeters, and Gilles Van Assche			
Input n bits	512	512	512	512	1024	1024	1152	1088	832	576
Output n' bits	128	160	224	256	384	512	224	256	384	512
Speed cycle/byte	6.8	11.4	15.8		17.7		12.5			
Considered Broken	yes	yes	no				no			

How to hash long messages ?

Merkle–Damgård construction



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