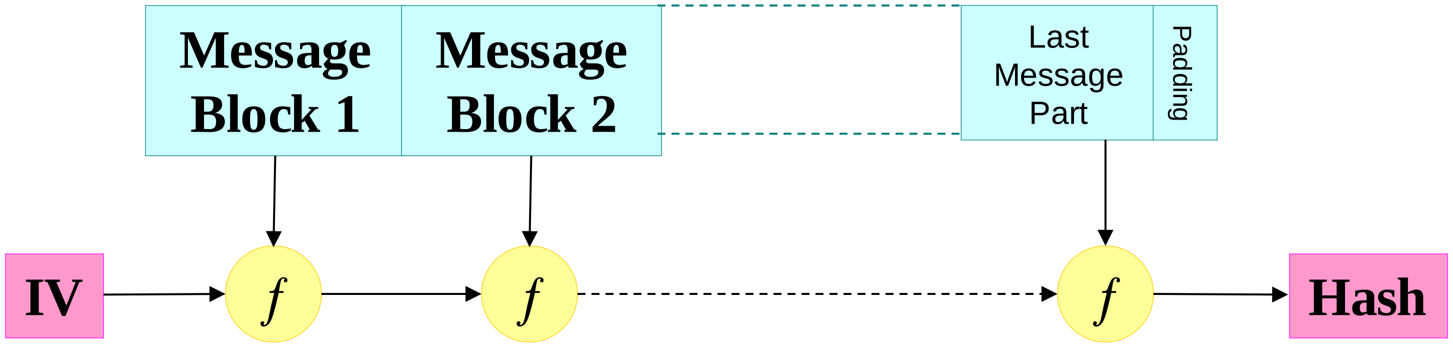
CSCI471/971
Modern Cryptography

Workshop

Question-1

Question 1. Assume that we use a good hash function H s.t. H(K || M) can be modelled as a secure pseudorandom function $F_K(M)$. Please show that MAC(K,M)=H(K||M) is a secure message authentication code.

Question-2



Suppose the function f is collision-resistant (and thus the hash function H is also collision resistant). Let IV be fixed for all messages.

Show that MAC(K,M)=H(K||M) is forgeable under chosen-message attack. Here K is as large as one message block.

END