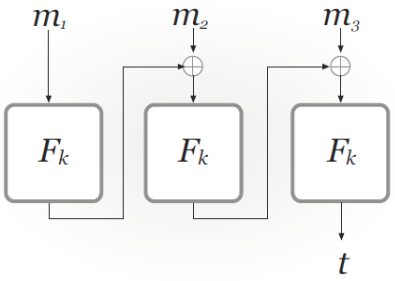
ENEE 459E/CMSC 498R: Introduction to Cryptology
CBC-MAC Class Exercise 3/8/16

Recall the CBC-MAC construction for fixed-length messages:



1. Show that CBC-MAC is no longer secure for fixed-length messages when the intermediate values (i.e. $t_1 = F_k(m_1)$ and $t_2 = F_k(t_1 \oplus m_2)$) are outputted as part of the tag.

2. Show an attack on CBC-MAC when variable-length messages are allowed. I.e. when the Sender and Receiver do not agree in advance on the length of the messages.