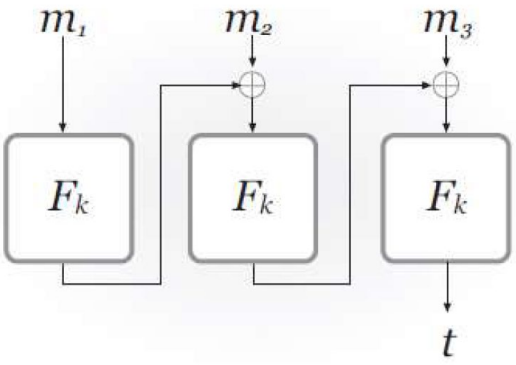
ENEE 457
CBC-MAC Class Exercise



The above version of CBC-MAC is secure for messages of length 3 blocks. Note that CBC-MAC differs from CBC-Enc in the following ways: (1) no random IV is chosen, (2) the intermediate values are not outputted.

1. Consider the following change to the above scheme: The MAC algorithm chooses a random IV and outputs:

$$t \coloneqq (IV, F_k(F_k(F_k(IV \oplus m_1) \oplus m_2) \oplus m_3)$$

Show that this scheme is not secure for 3 block messages.

2. Consider the following change to the above scheme: We now consider again macs for 3 block messages m_1, m_2, m_3. The MAC algorithm outputs:

$$t \coloneqq (F_k(m_1), F_k(F_k(m_1) \oplus m_2), F_k(F_k(F_k(m_1) \oplus m_2) \oplus m_3)$$

Show that this scheme is not secure for 3 block messages.

3. Finally, consider the original scheme but now allow the adversary to request signatures on 1, 2, or 3 block messages and output a forgery on a 1,2, or 3 block message. Show that the scheme is insecure in this setting.