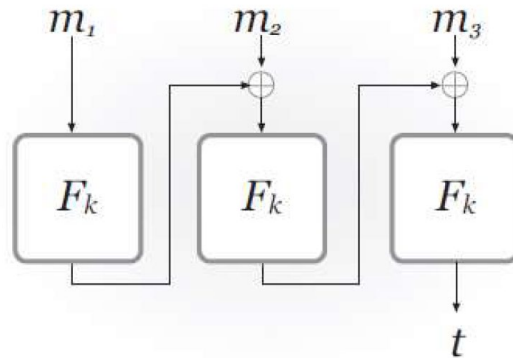


# ENEE 457

## 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:

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

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

**Solution:** A: query  $m = m_1, m_2, m_3$ , receive back  $t = (IV, \tau)$   
 Forge:  $m' = m'_1, m_2, m_3$  and  $t' = (IV', \tau)$ , where  $IV' = IV \oplus m_1 \oplus m'_1$

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:

$$t := (F_k(m_1), F_k(F_k(m_1) \oplus m_2), F_k(F_k(F_k(m_1) \oplus m_2) \oplus m_3))$$

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

**Solution:** A: fix target message  $m^* = m_1^*, m_2^*, m_3^*$   
 (1) query  $m = m_1^*, m_2, m_3$ , receive back  $t = (t_1^*, t_2, t_3)$ ; (2) query  $m' = t_1^* \oplus m_2^*, m_2', m_3'$ , receive back  $t' = (t_2^*, t_2', t_3')$ ; (3) query  $m'' = t_2^* \oplus m_3^*, m_2'', m_3''$ , receive back  $t'' = (t_3^*, t_2'', t_3'')$ ;  
 Forge:  $m^* = m_1^*, m_2^*, m_3^*$  and  $t^* = t_1^*, t_2^*, t_3^*$

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.

**Solution:** A: fix target message  $m^* = m_1^*, m_2^*, m_3^*$   
 (1) query  $m = m_1^*$ , receive back  $t_1^*$ ; (2) query  $m' = t_1^* \oplus m_2^*$ , receive back  $t_2^*$ ; (3) query  $m'' = t_2^* \oplus m_3^*$ , receive back  $t_3^*$ ;  
 Forge:  $m^* = m_1^*, m_2^*, m_3^*$  and  $t^* = t_1^*, t_2^*, t_3^*$

**Challenge:** Can you create a forgery on a 3-block message using only MAC queries for 2 and 3 block messages?