CSIC 4331/6331

Quiz 5

Name(s):

Domain Extension for MACs:

In this quiz, we will investigate domain extension for MACs. We have thus far seen how to build a fixed-length MAC that can authenticate n-bit messages. But, we would like to be able to authenticate arbitrary length messages.

Let $m = m_1||m_2||\cdots||m_\ell$ be a message where for each i, $|m_i| = n$.
Let $\Pi' = (\mathsf{Gen}', \mathsf{Mac}', \mathsf{Verify}')$ be a secure n-bit fixed-length MAC

1. For each of the following constructions, describe an attack breaking the security of the resulting MAC.

   (a) MAC each block separately: $t = t_1||t_2||\cdot||t_\ell$, where $t_i = \mathsf{Mac}'_k(m_i)$

   (b) Authenticate block index with the block: Same as in part a, but $t_i = \mathsf{Mac}'_k(i||m_i)$ (For this part, assume that the length of each block is short enough so that $\big|i||m_i\big| = n$)

   (c) Authenticate message length in each block: Same as in part a, but $t_i = \mathsf{Mac}'_k(\ell||i||m_i)$ (Again, assume blocks are short enough to allow for this.)

2. Describe a modification to the last construction above to avoid this attack (Hint: How can you add a message id?).