Solutions to the homework exercises

Homework 7

Question 1:

The security defintion is pretty much the same as in the fixed length case: The adversary is granted access to an authentication oracle, this time for arbitrary lenght messages. She is then asked to produce a forgery, i.e. a message-tag-pair that has not been previously output by the oracle. Note that the message length of the forgery is allowed to be different from any of the messages sent to the oracle.

The attack works as follows. First, the adversary sends any message $m = m_1 \| m_2 \| ... \| m_l$ to the oracle, with $|m_1| = n$. This results in a tag t. Now the adversary outputs $(m \| m', t)$, with $|m'| = l$, $m'_1 = m_1 \oplus t$, and $m'_i = m_i$ for all other $i = 2, ..., l$. This attack works because $m_1 = m_1 \oplus t_0 = t \oplus m'_1$.