Solutions to the homework exercises

Homework 7

Question 2:

The security definition is pretty much the same as in the fixed length case: The adversary is granted access to an authentication oracle, this time for arbitrary length 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.

- Query some m_1, $|m_1| = n$, the oracle outputs (m_1, t).
- The forgery is $(m^*, t^*) = (m_1 \| m_1 \oplus t, t)$

The attack works because $m_1 \| m_1 \oplus t \neq m_1$ and $(m_1 \| m_1 \oplus t, t)$ is a valid message-tag pair. To be more precise $\mathrm{MAC}_k(m*) = F_k(F_k(m_1) \oplus (m_1 \oplus t)) = F_k(t \oplus m_1 \oplus t) = F_k(m_1) = t$.

Question 3:

The attack works as follows.

- Query $m_1 \| m_2 \| m_3$, where all m_i are distinct and $|m_i| = n$, the oracle outputs $(m_1 \| m_2 \| m_3, t)$.
- The forgery is $(m^*, t^*) = (m_1 \| m_3 \| m_2, t)$

The attack works because $m_1 \| m_3 \| m_2 \neq m_1 \| m_2 \| m_3$, m_i are distinct, and $\mathrm{MAC}_k(m_1 \| m_3 \| m_2) = F_k(m_1) \oplus F_k(m_3) \oplus F_k(m_2) = F_k(m_1) \oplus F_k(m_2) \oplus F_k(m_3) = t$.

Question 4:

The attack works as follows.

- Query $m_1 \| m_2 \| m_3$ and $m_4 \| m_5 \| m_6$ where all m_i are distinct and $|m_i| = n$, the oracle outputs $(m_1 \| m_2 \| m_3, t_1)$ and $(m_4 \| m_5 \| m_6, t_2)$.
- Query $m_1 \| m_2 \| m_6$, the oracle outputs $(m_1 \| m_2 \| m_6, t_3)$.
- The forgery is $(m^*, t^*) = (m_4 \| m_5 \| m_3, t_1 \oplus t_2 \oplus t_3)$

The attack works because $m_4 \| m_5 \| m_3 \notin \{m_1 \| m_2 \| m_3, m_4 \| m_5 \| m_6, m_1 \| m_2 \| m_6\}$, and

$$\begin{aligned}\mathrm{MAC}_k(m^*) =& F_k(\langle 1 \rangle \| m_4) \oplus F_k(\langle 2 \rangle \| m_5) \oplus F_k(\langle 3 \rangle \| m_3) \\ =& \underbrace{F_k(\langle 1 \rangle \| m_4) \oplus F_k(\langle 2 \rangle \| m_5) \oplus F_k(\langle 3 \rangle \| m_6)}_{t_2} \oplus \underbrace{F_k(\langle 3 \rangle \| m_6) \oplus F_k(\langle 3 \rangle \| m_3)}_{t_1 \oplus t_3}.\end{aligned}$$

Question 5:

The attack works as follows.

- Query $m_1 \| m_2$ and $m_3 \| m_4$ where all m_i are distinct and $|m_i| = n$, the oracle outputs $(m_1 \| m_2, t_1 \| t_2)$ and $(m_3 \| m_4, t_3 \| t_4)$.
- The forgery is $(m^*, t^*) = (m_1 \| m_4, t_1 \| t_4)$

The attack works because $m_1 \| m_4 \notin \{m_1 \| m_2, m_3 \| m_4\}$, and $t_1 = F_k(m_1)$, $t_4 = F_k(F_k(m_4))$, so finally we have that $\mathrm{MAC}_k(m^*) = F_k(m_1) \| F_k(F_k(m_4)) = t_1 \| t_4$.