Introduction to Cryptography: Assignment 5

Group number 57

Elwin Tamminga s1013846

Lucas van der Laan s1047485

1

(a) Query m with $m_1 = m_2$, then $T = B_K(m_1)||B_K(B_K(m_1))||B_K(B_K(m_3))$.
We can now make a forgery $m' = T_1||m_1||m_3$ with the corresponding tag $T' = T_2||T_2||T_3$.
This verifies correctly because querying m' results in:

$$B_K(T_1)||B_K(B_K(m_1))||B_K(B_K(m_3)) = B_K(B_K(m_1))||B_K(B_K(m_1))||B_K(B_K(m_3)) = T'$$

(b) Query m with $m_1 = \overline{m_2}$, then $T = (B_K(m_2) \oplus B_K(m_2))||B_K(\overline{m_2} \oplus \overline{m_2} \oplus m_3) = 0^n||B_K(m_3)$.
We can now make a forgery $m' = \overline{x}||x||m_3$ with $x = \{0,1\}^n$ and $T' = T$.
This verifies correctly because querying m' results in

$$(B_K(x) \oplus B_K(x))||B_K(\overline{x} \oplus \overline{x} \oplus m_3) = 0^n||B_K(m_3) = T = T'$$

(c) It is not PRF-secure, because when we query m with $m_2 = m_3$, then we can say that we are interacting with the MAC1 function when the output is $a||b||c$ and $b = c$ with $|a| = |b| = |c| = n$. And we are interacting with a random oracle if $b \neq c$.

2

(a) Query m_1 which results in h_1. We can now compute a valid forgery tag h' by using a message m_2 of 128 bits and h_1 in the compression function F, which results in the valid tag h' for $m' = m_1||m_2$. This verifies correctly because $\text{MAC}_K(m') = h(K||m_1||m_2) = h'$.

(b) The inputs of the MAC function should all have a length of 128 bits, as the compression function inside of the MAC function requires two inputs of 128 bits to get a 128 bits answer.

(c) We can create a forgery T_2 for $m_1'||m_2'$ with the following steps:

- first query the compression function with $m_{2,0}$ and T', which results in h_0

- then for each $m_{2,i}$ from $i \geq 1$ query the compression function with $m_{2,i}$ and h_{i-1} which results in h_i.

- the last compression function output will be the forgery T_2, so $T_2 = h_{n'-1}$

(d) It is not secure, because the Tag and the derived key are the same in keyed hashing and we proved that you can generate a new Tag after you obtained an existing Tag, which could be used as a key.