Introduction to Modern Cryptography
Theresa, Celine, Prisca, Saibaba
December 4, 2022

Solution of Exercisesheet 7

Exercise 7-1

Exercise 7-2

a not secure:
The adversary $\mathcal{A}$ makes two queries to the oracle:
$m^1 = m_1||m_2 \Rightarrow t^1 = t^1_1||t^1_2 = F(K,m_1)||F(K,F(K,m_2))$
$m^2 = F(K,m_1)||m_2 \Rightarrow t^2 = t^2_1||t^2_2 = F(K,F(K,m_1))||F(K,F(K,m_2))$
Then he knows the tag for the message $m^* = m_1||m_1$ which is $t^* = F(K,m1)||F(K,F(K,m1)) = t^1_1||t^2_1$. Because $m^* \neq m^1$ and $m^* \neq m^2$, (m^*,t^*) is a valid attack.

b not secure:
The adversary $\mathcal{A}$ makes one query to the oracle:
$m^1 = m_1||m_2 \Rightarrow t^1 = F(K,m_1) \oplus F(K,m_2)$
Then he knows the tag for the message $m^* = m_2||m_1$ which is $t^* = F(K,m_2) \oplus F(K,m_1) = F(K,m_1) \oplus F(K,m_2) = t^1$. Because $m^* \neq m^1$, (m^*,t^*) is a valid attack.

c not secure:
The adversary $\mathcal{A}$ makes one query to the oracle:
$m^1 = m_1||m_2 \Rightarrow t^1 = (r \oplus (F(K,m_1) \oplus F(K,m_2)), r)$
Then he knows the tag for the message $m^* = m_2||m_1$ which is $t^* = (r \oplus (F(K,m_2) \oplus F(K,m_1)), r) = (r \oplus (F(K,m_1) \oplus F(K,m_2)), r) = t^1$. Because $m^* \neq m^1$, (m^*,t^*) is a valid attack.

Exercise 7-3

Exercise 7-4