Solution of Exercisesheet 7

Exercise 7-1

This modified encryption does not achieve CPA security. Here $H(m)$ will not be random for every encryption because Hash is calculated only based on message. As an Adversary against CPA has access to encryption oracle, Adversary can atleast distuinguish correspoding cipher to a message just by comparing the appended $H(m)$ part in the cipher. Hence this new modified encryption doesnt have indistingushable enryptions and so not CPA secure.

Exercise 7-2

a not secure:
The adversary $\mathcal{A}$ makes two queries to the oracle:
$m^1 = m_1||m_2 \Rightarrow t^1 = t_1^1||t_2^1 = F(K, m_1)||F(K, F(K, m_2))$
$m^2 = F(K, m_1)||m_2 \Rightarrow t^2 = t_1^2||t_2^2 = F(K, F(K, m_1))||F(K, F(K, m_2))$
Then he knows the tag for the message $m^* = m_1||m_1$ which is $t^* = F(K, m1)||F(K, F(K, m1)) = t_1^1||t_1^2$. Because $m^* \neq m^1$ and $m^* \neq m^2$, (m^*, t^*) is a valid attack.

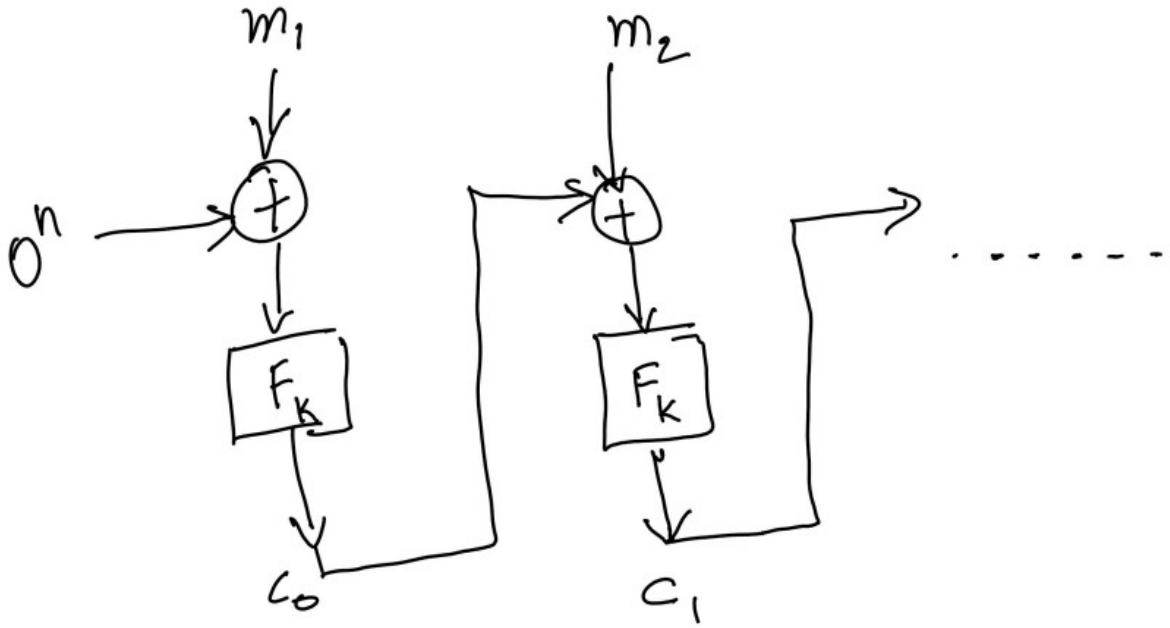
b not secure:
The adversary $\mathcal{A}$ makes one query to the oracle:
$m^1 = m_1||m_2 \Rightarrow t^1 = F(K, m_1) \oplus F(K, m_2)$
Then he knows the tag for the message $m^* = m_2||m_1$ which is $t^* = F(K, m_2) \oplus F(K, m_1) = F(K, m_1) \oplus F(K, m_2) = t^1$. Because $m^* \neq m^1$, (m^*, t^*)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

Solution of Exercisesheet 7

Exercise 7-3

a)



Let us consider two pair of messages and their MACs, (m', t') and (m'', t'')
And let

$$m' = m_1, m_2$$
$$m'' = m_1$$

so

$$c_0 = F_k(m1)$$
$$c_1 = F_k(m_2 \oplus F_k(m1))$$

So as per the message MAC pair we considered

$$t' = c_1$$
$$t'' = c_0$$

Now consider a new message $m''' = m_1, m_2, (m_1 \oplus t')$. MAC for this new message is

$$t''' = F_k(c_1 \oplus (m_1 \oplus t'))$$

replace t' with c_1

$$t''' = F_k(c_1 \oplus (m_1 \oplus c_1))$$
$$t''' = F_k(m_1)$$
$$t''' = c_0$$

So now there exists a possibility to create a third message and MAC pair created (m''', t''') with a valid MAC. As this is a valid forgery, this CBC is not secure.

Solution of Exercisesheet 7

Exercise 7-4