Solution of Exercisesheet 8

Exercise 8-1

Lets assume towards contradiction that the MAC construction is not secure $\Rightarrow$ Probablity of forging this construction Π_{MAC} is a non negligible function:

$$Pr[MacForge_{A,\Pi_{MAC}} = 1] \leq \epsilon(\lambda)$$

where $\epsilon(\lambda)$ is a non negligible function.

That implies there exists an efficient adversary, A, able to generate a new message and tag pair (m^*, t^*) such that $m^* \notin Q$, and $Ver_k(m^*, t^*) == 1$ with a probablity $\epsilon(\lambda)$.

We now consider $\mathcal{B}$ attacking the CCA-securitv. $\mathcal{B}$ runs $\mathcal{A}$ as subroutine. $\mathcal{B}$ only forward all encryption queries that $\mathcal{A}$ asks for to his own encryption oracle. Finally $\mathcal{A}$ outputs a message-tag-pair m^*, t^*. $\mathcal{B}$ then chooses two messages, lets say $\widetilde{m_0}$ as m^* and $\widetilde{m_1}$ as any other random message. If $\mathcal{B}$ gets the tag t^* as $\widetilde{c_b}$, it corresponds to $m_0 = m^*$ otherwise it correponds to random message m_1. This holds, because $Dec_k(t) = m \Leftrightarrow Enc_k(m) = t$.
$\mathcal{B}$ is efficient because it only forwards messages, which are of polynomial length (because $\mathcal{A}$ is efficient), chooses a random number and invokes $\mathcal{A}$. Because $\mathcal{A}$ can break the MAC with non-negligible probability $\epsilon(\lambda)$ and $\mathcal{B}$ uses this in every case, $\mathcal{B}$ can break the CCA security also with non-negligible probability $\epsilon(\lambda)$. Because this a contradiction to the CCA security of Π, our assumption that such an adversary $\mathcal{A}$ against the collision resistance of Π_{MAC} exists, is false. So Π_{MAC} is a collision resistant MAC.

Exercise 8-2

Exercise 8-3

Exercise 8-4

To show: $H(m) : \{0,1\}^{2k} \rightarrow \{0,1\}^{k+n}, H(m) := m_0||H'(m_1)$ is still a collision-resistant hash function when $m = m_0||m_1, |m_0| = |m_1| = k$ and $k > n$. $H'(m) : \{0,1\}^* \rightarrow \{0,1\}^n$ is a collision-resistant hash function.
Proof by contradiction. We assume there is an adversary $\mathcal{A}$, who can break the collision-resistance of $H(m)$ with non-negligible probability. We now build an adversary $\mathcal{B}$ against the collision-resistance of $H'(m)$ who invokes $\mathcal{A}$. $\mathcal{A}$ then outputs two messages m^1, m^2. $\mathcal{B}$ computes his output by truncating the first half of m^1 and m^2 $(m^i = m_0^i||m_1^i, i \in \{1,2\})$.
$\mathcal{B}$ is an efficient adversary because $\mathcal{A}$ is efficient, so the message length is poly and the call to $\mathcal{A}$ needs only poly time and sampling and prepend m_0 and truncating bit from m^1 and m^2 can also be done in polynomial time.
To analyse the success, we know, that with non-negligible probability $\mathcal{A}$ outputs two messages m^1, m^2 with $m^1 \neq m^2$ and $H(m^1) = H(m^2)$. $\mathcal{B}$ outputs only the second half of m^1 and m^2 which results in m_1^1, m_1^2. The probability that these are equal is $\left(\frac{1}{2}\right)^n$, because for each position

Solution of Exercisesheet 8

the probability that the bits are equal is $\frac{1}{2}$. In all other cases $\mathcal{B}$ outputs two messages m_1^1, m_1^2 with $m_1^1 \neq m_1^2$ and $H'(m_1^1) = H'(m_1^2)$. This holds because $H(m^1) = H(m^2) \Rightarrow H(m_0^1||m_1^1) = H(m_0^2||m_1^2) \Rightarrow m_0^1||H'(m_1^1) = m_0^2||H'(m_1^2)$.

$$Pr[HashColl_{\mathcal{B}}(\lambda) = 1] = Pr[HashColl_{\mathcal{A}}(\lambda) = 1] - Pr[x_1' == x_2'] = \texttt{non-negl.} - \left(\frac{1}{2}\right)^k = \texttt{non-negl.}$$

Because this is a contradiction to the collision-resistance of $H'(m)$ such an adversary $\mathcal{A}$ cannot exist.
It follows that $H(m)$ is a collision-resistant hash function.