Tutorial 5: Hash Functions and MACs

Submission Guidelines All problems must be solved in class today. Searching on the internet for solutions is strictly discouraged.

1. Let F be a PRF. Show that the following constructions of MAC are insecure. Let $\mathcal{K} = \{0,1\}^n$ and $m = m_1 \| \cdots \| m_\ell$ with $m_i \in \{0,1\}^n$ for $i \in [1, \ell]$.
   (a) Send $t = F_k(m_1) \oplus \cdots \oplus F_k(m_\ell)$.
   (b) Pick $r \xleftarrow{U} \{0,1\}^n$, compute $t = F_k(r) \oplus F_k(m_1) \oplus \cdots \oplus F_k(m_\ell)$ and send (r, t).
2. If a message m is authenticated by sending $t = F_k(m)$ along with m, the security is implied if F is a PRF. Does security hold when F is a weak PRF?
3. Let $\mathsf{H}_1, \mathsf{H}_2 : \{0,1\}^m \to \{0,1\}^n$ be two hash functions. Define a hash function $\mathsf{H} : \{0,1\}^m \to \{0,1\}^{2n}$ as $\mathsf{H}(x) = \mathsf{H}_1(x) \| \mathsf{H}_2(x)$. Prove that if at least one of $\mathsf{H}_1, \mathsf{H}_2$ is collision resistant, then H is collision resistant.
4. Show that for a hash function, collision resistance implies second pre-image resistance and second pre-image resistance implies pre-image resistance.