# Tutorial 3
# Message Authentication Codes and Hash Functions

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. For a function $g : \{0,1\}^\lambda \to \{0,1\}^\lambda$, let $g^\$$ be an oracle that, whenever queried, chooses $x \xleftarrow{U} \{0,1\}^\lambda$ and returns $(x, g(x))$. We say a keyed function $F : \{0,1\}^\lambda \times \{0,1\}^\lambda \to \{0,1\}^\lambda$ is weakly pseudorandom if there exists a negligile function $\mathsf{negl}$ such that for all probabilistic polynomial time (in $\lambda$) algorithms $\mathscr{D}$,

$$|\Pr[\mathscr{D}^{F_k^\$(\cdot)} = 1] - \Pr[\mathscr{D}^{f^\$(\cdot)} = 1]| \leq \mathsf{negl}(\lambda),$$

   where $k \xleftarrow{U} \{0,1\}^\lambda$ and $f$ is chosen uniformly at random from the set of all functions from $\{0,1\}^\lambda$ to $\{0,1\}^\lambda$.

   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 $\mathcal{H}_1, \mathcal{H}_2 : \{0,1\}^m \to \{0,1\}^n$ be two hash functions. Define a hash function $\mathcal{H} : \{0,1\}^m \to \{0,1\}^{2n}$ as $\mathcal{H}(x) = \mathcal{H}_1(x) || \mathcal{H}_2(x)$. Prove that if at least one of $\mathcal{H}_1, \mathcal{H}_2$ is collision resistant, then $\mathcal{H}$ is collision resistant.

4. Let $\Pi = (\mathsf{Gen}, \mathsf{Mac}, \mathsf{Vrfy})$ be a secure MAC for messages of length $\lambda$ and $H : \{0,1\}^\ell \to \{0,1\}^\lambda$ a collision resistant hash function. Define a MAC $\Pi' = (\mathsf{Gen}', \mathsf{Mac}', \mathsf{Vrfy}')$ for messages of length $\ell$ as follows: $\mathsf{Gen}'(1^\lambda) = \mathsf{Gen}(1^\lambda)$; $\mathsf{Mac}'(k,m) = \mathsf{Mac}(k, H(m))$; $\mathsf{Vrfy}'(k,m,t) = \mathsf{Vrfy}(k, H(m), t)$. If $\Pi'$ a secure MAC? Justify.

5. Let $h : X \to Y$ be a hash function with $|X| = n$, $|Y| = m$. Define

$$h^{-1}(y) = \{x \in X : h(x) = y\}.$$

   Let $p$ denote the probability that $h(x_1) = h(x_2)$ when $x_1$ and $x_2$ are chosen uniformly at random from $X$. Prove that $p \geq \frac{1}{m}$ with equality if and only if $|h^{-1}(y)| = \frac{n}{m}$ for every $y \in Y$.