دانشکده‌ی علوم ریاضی

مقدمه‌ای بر رمزنگاری

آزمون میانترم

مدرّس: دکتر شهرام خزائی — تاریخ: ۱۳۹۹/۹/۲۳

Problem 1

Consider two MAC schemes, $\Pi^1 = (\mathsf{Gen}^1, \mathsf{MAC}^1, \mathsf{Verify}^1)$ and $\Pi^2 = (\mathsf{Gen}^2, \mathsf{MAC}^2, \mathsf{Verify}^2)$. Show whether the following is a secure MAC if either Π^1 or Π^2 is secure. Provide a proof or counterexample for your answer.

- Define $\Pi^a = (\mathsf{Gen}^a, \mathsf{MAC}^a, \mathsf{Verify}^a)$, where

  $$\mathsf{MAC}^a_{(k_1,k_2)}(m) := (t_1, t_2)$$

  where $t_i \leftarrow \mathsf{MAC}^i_{k_i}(m)$ for $i \in \{1, 2\}$, and Verify^a accepts iff both $\mathsf{Verify}^1_{k_1}(m, t_1)$ and $\mathsf{Verify}^2_{k_2}(m, t_2)$ accept.

Problem 2

Let H be a hash function which is constructed by the Merkel-Damgard transform. Show that $\mathsf{H}(k||x)$ is not a secure PRF.

Problem 3

Fix $l > 0$ and a prime p. Let $\mathcal{K} = \mathbb{Z}_p^{l+1}$, $\mathcal{M} = \mathbb{Z}_p^l$, and $\mathcal{T} = \mathbb{Z}_p$. Define $h : \mathcal{K} \times \mathcal{M} \to \mathcal{T}$ as

$$h_{k_0,k_1,..,k_l}(m_1, .., m_l) = \left[k_0 + \sum_{i=1}^{l} k_i m_i\right] \quad mod\, p$$

Prove that h is strongly universal.

Hint: A function $h : \mathcal{K} \times \mathcal{M} \to \mathcal{T}$ is strongly universal if for all distinct $m, m' \in \mathcal{M}$ and all $t, t' \in \mathcal{T}$ it holds that

$$\Pr[h_k(m) = t \wedge h_k(m') = t'] = \frac{1}{|\mathcal{T}|^2}$$

where the probability is taken over uniform choice of $k \in \mathcal{K}$.