Theoretical Foundations of Cryptography | **Instructor: Chris Peikert**
Georgia Tech, Spring 2011 | **Homework 4** | **Student: YOUR NAME HERE**

This homework is due by the **start of class on March 10** via the course page on T-Square. Start early!

Instructions. Solutions must be typeset in LaTeX (a template for this homework is available on the course web page). Your work will be graded on *correctness*, *clarity*, and *conciseness*. You should only submit work that you believe to be correct; if you cannot solve a problem completely, you will get significantly more partial credit if you clearly identify the gap(s) in your solution. It is good practice to start any long solution with an informal (but accurate) "proof summary" that describes the main idea.

You may collaborate with others on this problem set and consult external sources. However, you must ***write your own solutions*** and ***list your collaborators/sources*** for each problem.

1. (25 points) *(Authenticated encryption and chosen-ciphertext security.)*
   (a) (15 points) Let $\mathrm{SKC} = (\mathsf{Gen}, \mathsf{Enc}, \mathsf{Dec})$ be an IND-CPA-secure shared-key encryption scheme, and let $\mathrm{MAC} = (\mathsf{Gen}, \mathsf{Tag}, \mathsf{Ver})$ be a SUF-CMA-secure MAC. For each of the following schemes $\mathrm{SKC}' = (\mathsf{Gen}', \mathsf{Enc}', \mathsf{Dec}')$, consider whether it is a secure *authenticated encryption* scheme, as defined in class (see the lecture notes for a precise definition). If it is, then prove it; otherwise, give the simplest counterexample you can find.
   In all of the schemes below, Gen' works as follows: let $k_a \leftarrow \mathrm{MAC.Gen}$ and $k_e \leftarrow \mathrm{SKC.Gen}$, and output $k = (k_a, k_e)$.
      i. $\mathsf{Enc}'_k(m)$: let $c \leftarrow \mathsf{Enc}_{k_e}(m)$ and $t \leftarrow \mathsf{Tag}_{k_a}(m)$. Output $c' = (c, t)$.
      $\mathsf{Dec}'_k(c' = (c, t))$: let $m \leftarrow \mathsf{Dec}_{k_e}(c)$. If $\mathsf{Ver}_{k_a}(m, t)$ rejects, output $\perp$; else, output m.
      ii. $\mathsf{Enc}'_k(m)$: let $t \leftarrow \mathsf{Tag}_{k_a}(m)$ and output $c' \leftarrow \mathsf{Enc}_{k_e}((m, t))$.
      $\mathsf{Dec}'_k(c')$: let $(m, t) \leftarrow \mathsf{Dec}_{k_e}(c')$. If $\mathsf{Ver}_{k_a}(m, t)$ rejects, output $\perp$; else, output m.
      iii. $\mathsf{Enc}'_k(m)$: let $c \leftarrow \mathsf{Enc}_{k_e}(m)$ and $t \leftarrow \mathsf{Tag}_{k_a}(c)$. Output $c' = (c, t)$.
      $\mathsf{Dec}'_k(c' = (c, t))$: if $\mathsf{Ver}_{k_a}(c, t)$ rejects, output $\perp$. Otherwise, output $\mathsf{Dec}_{k_e}(c)$.
   (b) (10 points) Prove that any secure authenticated encryption scheme $\mathrm{AE} = (\mathsf{Gen}, \mathsf{Enc}, \mathsf{Dec})$ is itself IND-CCA-secure, as defined in class.
   (*Hint*: consider a hybrid IND-CCA experiment in which the decryption oracle decrypts *only* ciphertexts that were already returned by the encryption oracle, and answers $\perp$ on all others. Use AE's unforgeability to prove that this experiment is indistinguishable from the real IND-CCA attack. Then show how to simulate the hybrid IND-CCA experiment given only the ability to mount an IND-CPA attack on AE.)

2. *(Collision-resistance potpourri.)* Prove or disprove (giving the simplest counterexample you can find) each of the following statements about collision-resistant hashing.
   (a) (5 points) A collision-resistant hash function family $\mathcal{H} = \{h_s \colon \{0,1\}^{2n} \to \{0,1\}^n\}$ is a one-way function family. (*Hint*: bound the number of inputs to h_s that do not collide with any other input.)
   (b) (5 points) Same as the previous part, but with $\mathcal{H} = \{h_s \colon \{0,1\}^{n+1} \to \{0,1\}^n\}$.
   (c) (5 points) Let $G = \langle g \rangle$ be a cyclic group of prime order q, and let fixed $t \geq 2$ be any fixed integer. Define the hash function family $\mathcal{H} = \{h_{g_1,\ldots,g_t} \colon \mathbb{Z}_q^t \to G \mid g_i \in G\}$ as

$$h_{g_1,\ldots,g_t}(x_1, \ldots, x_t) = \prod_{i \in [t]} g_i^{x_i} \in G.$$

   If solving the discrete logarithm problem in G is hard, then $\mathcal{H}$ is a collision-resistant hash function family. (*Hint*: given a discrete logarithm challenge (g, y), let $g_i = g^{a_i} \cdot y^{b_i} \in G$ for uniformly random $a_i, b_i \leftarrow \mathbb{Z}_q$. How does a collision help you compute $\log_g(y)$? Be careful!)