Winter 2018 CS 485/585 Introduction to Cryptography

Homework 3

Portland State University — *Feb. 1, 2018*
Lecturer: Fang Song — *Due: Feb. 15, 2018*

Instructions. Your solutions will be graded on *correctness* and *clarity*. 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. Problems marked with "**[G]**" are required for graduate students. Undergraduate students will get bonus points for solving them. The .tex source is provided on course webpage as a template if you want to typeset your solutions in Latex.

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

1. (More MACs)
   (a) (10 points) Let F be a pseudorandom function. Decide if the following MACs are secure for authenticating fixed-length messages. Prove it or show an attack.
      1. To authenticate $m = m[1], \ldots, m[\ell]$ where $m[i] \in \{0,1\}^n$, compute $t := F_k(m[1]) \oplus \cdots \oplus F_k(m[\ell])$.
      2. To authenticate $m = m[1], \ldots, m[\ell]$ where $m[i] \in \{0,1\}^{n/2}$, compute $t := F_k(\langle 1 \rangle \| m[1]) \oplus \cdots \oplus F_k(\langle \ell \rangle \| m[\ell])$. $\langle i \rangle$ denotes the encoding of integer i to a $n/2$-bit string.

   (b) (10 points) Read the basic construction of CBC-MAC [KL: Section 4.4.1], and do [KL: Exercise 4.13].

2. (Hash functions)
   (a) (10 points) [KL: Exercise 5.2]
   (b) (10 points) Merkle-Damgård.
      i. Modify the Merkle-Damgård construction so that in the last block, instead of outputting $z := h(z_B \| L)$, output $z_B \| L$. Is this construction collision resistant? Prove it or show an attack.
      ii. [KL: Exercise 5.8] Prove or disprove: if h is preimage-resistant, then the hash function H by applying the Merkle-Damgård transformation on h is also preimage-resistant.
   (c) (5 Bonus points. Proof of work) Let $H : \{0,1\}^{2n} \to \{0,1\}^n$ be a hash function modeled as a truly random function. Suppose one can evaluate H on one input each computer cycle. Given some $id \in \{0,1\}^n$ and an integer $T \leq 2^n$, how many cycles does it need to find an x such that the first $\lceil \log T \rceil$ bits of $H(id \| x)$ are 0?

3. (10 points) (Authenticated Encryption) [KL: Exercise 4.22].

4. (Foundations)

   (a) (5 points) (Computational indistinguishability) Recall the definition of computational indistinguishability [KL: Def. 7.30]. Two probability ensembles $\mathcal{X} = \{X_n\}_{n\in\mathbb{N}}$ and $\mathcal{Y} = \{Y_n\}_{n\in\mathbb{N}}$ are computationally indistinguishable, denoted $\mathcal{X} \approx_c \mathcal{Y}$, if for any probabilistic polynomial-time distinguisher D,

   $$\left| \Pr_{x\leftarrow X_n}[D(1^n, x) = 1] - \Pr_{y\leftarrow Y_n}[D(1^n, y) = 1] \right| \leq \text{negl}(n)\,.$$

   Prove that the relation of computational indistinguishability is transitive: if $\mathcal{X} \approx_c \mathcal{Y}$ and $\mathcal{Y} \approx_c \mathcal{Z}$, then $\mathcal{X} \approx_c \mathcal{Z}$.

   (b) (10 points) Let G be a pseudorandom generator with expansion factor $\ell(n) = n + 1$.

      i. Prove that G is a one-way function.

      ii. (Exercise. Do not turn it.) Construct $G'(s) = G(s_1)\|G(s_2)$. Is G' a secure pseudorandom generator?

      iii. Let $G(s) = t_0, \ldots, t_{n-1}t_n$. Construct $G''(s) = G(t_0, \ldots, t_{n-1})\|t_n$, i.e., use the first n-bit output as the seed in the second application of G. Is G'' a PRG? Prove or disprove it.