Foundations of Computer Security September 17, 2021
Massachusetts Institute of Technology 6.S060 Fall 2021
Henry Corrigan-Gibbs, Srini Devadas, Yael Kalai, Nickolai Zeldovich Lab 1 Theory

Lab 1 Theory

This assignment is due **at 10:00pm ET** on **Thursday, September 30, 2021**.

Please make note of the following instructions:

- Remember that your solutions must be submitted on Gradescope. Please sign-up for 6.S060 Fall 2021 on Gradescope, with the entry code `KYRBPK`, using your MIT email.
- We require that the solution to the problems is submitted as a PDF file, **typeset on LaTeX**, using the template available on the course website (`https://6s060.csail.mit.edu/2021/`). Each submitted solution should start with your name, the course number, the problem number, the date, and the names of any students with whom you collaborated.

Problem 1-1. Hash Function Properties [50 points]

Let $h : \{0,1\}^{\leq 2n} \rightarrow \{0,1\}^n$ be a hash function that is collision resistant. Let $h' : \{0,1\}^{\leq n+1} \rightarrow \{0,1\}^{n+1}$ be the hash function given by the rule

$$h'(x) = \begin{cases} 0||x & \text{if } x \in \{0,1\}^n \\ 1||h(x) & \text{otherwise} \end{cases}$$

(a) Prove that h' is not one-way. [15 points]

Definition 1 *A function $f : X_n \rightarrow Y_n$ is said to be one-way if for every efficient adversary $\mathcal{A}$, the probability that $\mathcal{A}$, on input n and $y = f(x)$ for a random $x \in X_n$, outputs any x' such that $f(x') = y$, is negligible.*

(b) Prove that h' is collision resistant. [20 points]

Definition 2 *A function $f : X_n \rightarrow Y_n$ is said to be collision resistant if for every efficient adversary $\mathcal{A}$, the probability that $\mathcal{A}$ on input n, outputs any distinct $x, x' \in X_n$ such that $f(x) = f(x')$, is negligible.*

(c) Prove that h' is target collision resistant if h is target collision resistant. [15 points]

Definition 3 *A function $f : X_n \rightarrow Y_n$ is said to be target collision resistant if for every efficient adversary $\mathcal{A}$, the probability that $\mathcal{A}$ on input n and a random $x \in X_n$, outputs $x' \in X_n$ such that $x' \neq x$ and $f(x) = f(x')$, is negligible.*

Problem 1-2. Message Authentication [50 points]

The material for this problem will be covered in class on Monday, September 20th.

(a) Let MAC be a secure message authentication code. Suppose Alice and Bob send authenticated messages to each other. Namely, every time one of them sends a message M they send it together with $\mathsf{MAC}(K, M)$ where K is their shared secret key. On day 1, Alice asks Bob if he wants to go to the movies, and Bob replies "yes". On day 2, Alice asks Bob if he wants to go to ice cream and Bob replies "no". On day 3, Alice asks Bob if he wants to rob a bank and Bob replies "no". Can an adversary Eve observing the communication on the first two days, corrupt Bob's message on the third day (in an authenticated way)? If so, how would you use a secure MAC so that the adversary cannot corrupt Bob's message? [15 points]

(b) Recall that the CMAC construction we saw in class is a sequential construction. Namely, to MAC a very long message that consists of L blocks (each of 128 bits), we need to do L sequential steps. Consider the following parallel construction: Let $F : K \times X \to \{0,1\}^k$ be a pseudorandom function (PRF). Let

$$\mathsf{MAC}(K, (M_1, \ldots, M_L)) = \oplus_{i=1}^{L} F(K, M_i),$$

where each $M_i \in X$. Is this a secure MAC (i.e., existentially unforgeable against adaptive chosen message attacks)? [15 points]

(c) Recall that to apply the CMAC construction we need to assume that the message length is a multiple of 128, since we partition the message into blocks, each of length 128. If the length of the message is not a multiple of 128 then we need to pad it to ensure that it's length is divisible by 128.

- Consider the padding which simply pads the message M with 0's to make it of length that is divisible by 128. Argue that the resulting (CMAC+padding) scheme is insecure by providing an attack.
- Suggest a padding scheme that will make the resulting (CMAC+padding) scheme secure. What property does such a padding scheme need to have in order to ensure that the resulting scheme is secure? **Hint:** You may need to add a dummy block. [20 points]