CSIC 4331/6331 October 21, 2019

Homework Assigment 4

Due Nov. 4

Please answer each of the below questions. Remember, you may work together, but everyone MUST type up and understand their solutions. Solutions that appear copied will be considered a violation of the academic honesty code. Also, you must list all people you work with on this homework as well as any outside resources (e.g., web search, books, etc.) that you use.

Note, problems 4 - 6 require material we will cover in class on Monday, October 28th.

1. Exercise 5.3 in the book
   Let (Gen, H) be a collision-resistant hash function. Is $(Gen, \hat{H})$ defined by $\hat{H}_s(x) = H_s(H_s(x))$ necessarily collision resistant?
   Either provide a counter-example or sketch a proof (i.e. a reduction) that this is so.

2. Explain why the output of a collision-resistant hash function $t = H_s(m)$ is *not* a good MAC on m.
   Hint: Read Section 5.3.1 for a discussion on how to construct a MAC (for unbounded length messages) using a collision-resistant hash function.

3. Exercise 5.13 in the book
   Show how to find a collision in the Merkle tree construction if t (the number of items stored) is not fixed. Specifically, show how to find two sets of inputs $x_1, \ldots, x_t$ and $x'_1, \ldots, x'_{2t}$ such that $\mathcal{MT}_t(x_1, \ldots, x_t) = \mathcal{MT}_{2t}(x'_1, \ldots, x'_{2t})$.

4. Exercise 6.7 in the book
   What is the output of an r-round Feistel network when the input is (L_0, R_0) in all of the following cases:

   (a) Each round function outputs all 0s, regardless of the input.

   (b) Each round function is the identity function (i.e., $f(x) = x$)

5. Exercise 6.8 in the book
   Let $Feistel_{f_1,f_2}(\cdot)$ denote a two-round Feistel network using functions f_1 and f_2 (in that order). Show that if $Feistel_{f_1,f_2}(L_0, R_0) = (L_2, R_2)$, then $Feistel_{f_2,f_1}(R_2, L_2) = (R_0, L_0)$.

6. Exercise 6.10 in the book
   Show that DES has the property that $DES_k(x) = \overline{DES_{\overline{k}}(\overline{x})}$ for every key k and input x (where $\overline{z}$ denotes the bitwise complement of z). (This is called the *complementarity property* of DES.). Does this represent a serious vulnerability in the use of triple-DES as a pseudorandom permutation? Explain.