CSIC 4331/6331 October 31, 2018

Homework Assigment 4

Due Nov. 12

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 5 and 6 require material we will cover in class on Monday, November 5th.

1. Exercise 5.6 in the book
   For each of the following modifications to the Merkle-Damgard transform (Construction 5.3), determine whether the result is collision resistant. If yes, sketch a proof; if not, demonstrate an attack.

   (a) Modify the construction so that the input length is not included at all (i.e., output z_B and not $z_{B+1} = h^s(z_B||L)$). (Assume the resulting hash function is only defined for inputs whose length is an integer multiple of the block length.)

   (b) Modify the construction so that instead of outputting $z = h^s(z_B||L)$, the algorithm outputs $z_B||L$

   (c) Instead of using an IV, just start the computation from x_1. That is, define $z_1 = x_1$ and then compute $z_i = h^s(z_{i-1}||x_i)$ for $i = 2, \ldots, B+1$ and output z_{B+1} as before.

   (d) Instead of using a fixed IV, set $z_0 = L$ and then compute $z_i = h^s(z_{i-1}||x_i)$ for $i = 1, \ldots, B$ and output z_B.

2. 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., $f(x) = x$)

3. 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 $Feistel_{f_2,f_1}(R_2, L_2) = (R_0, L_0)$.

4. 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.

5. (a) What is $\phi(85)$? (Note that $85 = 5 \cdot 17$.)

   (b) Find d such that $3d = 1 \bmod \phi(85)$.

(c) Find $x \in \mathbb{Z}_{85}^*$ such that $x^3 = 2 \bmod 85$.

6. Exercise 8.9 in the book
Let p, N be integers with $p|N$. Prove that for any integer X,

$$[[X \bmod N] \bmod p] = [X \bmod p].$$

Show that, in contrast, $[[X \bmod p] \bmod N]$ need not equal $[X \bmod N]$.