CSIC 4331/6331 October 11, 2018

Homework Assigment 3

Due Oct. 15

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.

1. Exercise 3.20 in the book
   Consider a stateful variant of CBC-mode encryption where the sender simply increments the IV by 1 each time a message is encrypted (rather than choosing IV at random each time). Show that the resulting scheme is *not* CPA-secure.

2. Exercise 3.28 in the book
   Show that CBC, OFB, and CTR modes of operation do not yield CCA-secure encryption (regardless of F).

3. Exercise 4.7 in the book. (**Note: I slightly modified part c of this problem from what is in the book**)
   Let F be a PRF. Show that each of the following MACs is insecure, even if used to authenticate fixed-length messages. (In each case Gen outputs a uniform $k \in \{0,1\}^n$. Let $\langle i \rangle$ denote an $n/2$-bit encoding of the integer i.)

   (a) To authenticate a message $m = m_1, \ldots, m_l$, where $m_i \in \{0,1\}^n$, compute $t = F_k(m_1) \oplus \cdots \oplus F_k(m_l)$.

   (b) To authenticate a message $m = m_1, \ldots, m_l$, where $m_i \in \{0,1\}^{n/2}$, compute $t = F_k(\langle 1 \rangle \,||m_1) \oplus \cdots \oplus F_k(\langle l \rangle \,||m_l)$.

   (c) To authenticate a message $m = m_1, \ldots, m_l$, where $m_i \in \{0,1\}^{n/2}$, choose uniform $r \leftarrow \{0,1\}^{n/2}$, let $r' = 0^{n/2}||r$, and compute

   $$t = F_k(r') \oplus F_k(\langle 0 \rangle \,||m_1) \oplus F_k(\langle 1 \rangle \,||m_2) \cdots \oplus F_k(\langle l-1 \rangle \,||m_l)$$

   and let the tag be (r, t).

4. Exercise 4.26 in the book
   Show a CPA-secure private-key encryption scheme that is unforgeable but is not CCA-secure.

5. 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.

6. 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 $\mathcal{MT}_t(x_1, \ldots, x_t) = \mathcal{MT}_{2t}(x'_1, \ldots, x'_{2t})$.