CSIC 4331/6331	September 30, 2019

Homework Assigment 3

Due Oct. 7

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 3.19 in the book
   Let F be a PRF and G be a PRG with expansion factor $l(n) = n + 1$. For each of the following encryption schemes, state whether the scheme has indistinguishable encryptions in the presence of an eavesdropper and whether it is CPA-secure. (In each case, the shared key is a uniform $k \in \{0,1\}^n$.) Explain your answer.

   (a) To encrypt $m \in \{0,1\}^{n+1}$, choose uniform $r \in \{0,1\}^n$ and output the ciphertext $(r, G(r) \oplus m)$.

   (b) To encrypt $m \in \{0,1\}^n$, output the ciphertext $m \oplus F_k(0^n)$.

   (c) To encrypt $m \in \{0,1\}^{2n}$, parse m as $m_1||m_2$ with $|m_1| = |m_2|$, then choose uniform $r \in \{0,1\}^n$ and send $(r, m_1 \oplus F_k(r), m_2 \oplus F_k(r+1))$.

2. 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.

3. Let $\Pi = (Gen, Enc, Dec)$ be an encryption scheme with message space $\mathcal{M} = \{0,1\}^n$. Define $\Pi' = (Gen', Enc', Dec')$ to be an encryption scheme with message space $\mathcal{M} = \{0,1\}^{2n}$ (we view $m \in \{0,1\}^{2n}$ as two n-bit messages m_1, m_2) defined as follows:
   (Note $m_1 = \perp$ means that decryption fails. $\perp$ is just a special fail symbol.)

$\underline{Gen'(1^n)}$	$\underline{Enc'_k(m_1, m_2)}$	$\underline{Dec'_k(c_1, c_2)}$
$k = \Pi.Gen(1^n)$	$c_1 = \Pi.Enc_k(m_1)$	$m_1 = \Pi.Dec_k(c_1)$
return k	$c_2 = \Pi.Enc_k(m_2)$	$m_2 = \Pi.Dec_k(c_2)$
	return (c_1, c_2)	If $m_1 = \perp$ or $m_2 = \perp$, return $\perp$
		Else return $m_1 \| m_2$

   (a) If Π is CPA-secure, is Π' CPA-secure? Justify your answer.

   (b) If Π is CCA-secure, is Π' also CCA-secure? Justify your answer.

4. 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).