CSIC 4331/6331 September 19, 2018

Homework Assigment 2

Due Sep. 24

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: In problems 3-5, you are asked to either argue that a scheme is secure or to argue that it is not. You should show insecurity by demonstrating an explicit attack or counter-example, but you can claim security by giving a convincing argument (a formal proof of security is welcome, but not required).

1. In cryptographic constructions, we often need a source of unbiased and independent random bits. Suppose I only have a biased coin that comes up heads with probability 1/4, and tails with probability 3/4. Describe how this coin can be used to produce an unbiased random bit.

2. Exercise 3.1 in the book.
   Let $negl_1$ and $negl_2$ be negligible functions. Then,
   (a) The function $negl_3$ defined by $negl_3(n) = negl_1(n) + negl_2(n)$ is negligible.
   (b) For any positive polynomial p, the function $negl_4$ defined by $negl_4(n) = p(n) \cdot negl_1(n)$ is negligible.

3. Let G be a pseudorandom generator that maps n-bit inputs to $(n+1)$-bit outputs, and define $G'(s_1, \ldots, s_n) = G(s_1, \ldots, s_n)||(s_1 \wedge s_2)$. Here $s_1, \ldots, s_n$ are the bits of the seed s, and $||$ denotes concatenation. Is G' a pseudorandom generator?

4. Exercise 3.6 in the book.
   Let G be a pseudorandom generator with expansion factor $l(n) > 2n$. In each of the following cases, say whether G' is necessarily a pseudorandom generator. If yes, give a proof; if not, show a counterexample.
   (a) Define $G'(s) = G(s_1 \cdots s_{\lfloor n/2 \rfloor})$, where $s = s_1 \cdots s_n$.
   (b) Define $G'(s) = G(0^{|s|}||s)$.
   (c) Define $G'(s) = G(s)||G(s+1)$.

5. Let F be a pseudorandom permutation. (We will cover pseudorandom functions in class on September 17th.)
   (a) Consider the encryption scheme for message space $\mathcal{M} = \{0,1\}^n$ defined as follows: $Gen(1^n)$ chooses two random keys $k_1, k_2 \leftarrow \{0,1\}^n$. Encryption works by computing $c = Enc_{k_1,k_2}(m) = F_{k_1}(k_2 \oplus m)$, and decryption is done by computing $m = k_2 \oplus (F_{k_1}^{-1}(c))$. Does this scheme have indistinguishable encryptions in the presence of an eavesdropper? Is this scheme CPA-secure?

(b) Consider the encryption scheme where the message space $\mathcal{M} = \{0,1\}^{n/2}$ and encryption of a message is done by choosing a random $n/2$-bit string $r \leftarrow \{0,1\}^{n/2}$, and then computing $c = F_k(r||m)$. Decryption is done by computing $m = F_k^{-1}(c)\Big]_{n/2+1}^{n}$ (the last $n/2$ bits of $F_k^{-1}(c)$).
Does this scheme have indistinguishable encryptions in the presence of an eavesdropper? Is this scheme CPA-secure?