CSIC 4331/6331 September 11, 2019

Homework Assigment 2

Due September 23

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 (e.g., an informal sketch of a reduction proof). 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. Prove that

   (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 $G'(s) = G(s_1 \cdots s_{\lceil n/2 \rceil})$, 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 function (PRF) that takes an n-bit key and maps n-bit inputs to n-bit outputs. (We will cover pseudorandom functions in class on September 17th.) Which of the following derived PRFs are secure? Justify your answer.

   (a) $F^1_k(x) = F_k(x)||0$

   (b) $F^2_k(x, y) = F_k(x) \oplus F_k(y)$

   (c) $F^3_{k_1,k_2}(x) = F_{k_1}(x) \oplus F_{k_2}(x)$

   (d) $F^4_k(x) = F_k(x)||F_k(F_k(x))$