University of Maryland
CMSC858K — Introduction to Cryptography
Professor Jonathan Katz

Problem Set 1

Due at the *beginning* of class on Feb. 8

Please type your solutions, preferably using latex (you can ask for my help getting started with latex if you are unfamiliar with it). I will accept handwritten solutions but will not spend time trying to read illegible handwriting!

1. **(Perfect secrecy.)** In class we defined perfect secrecy and perfect indistinguishability, and showed that any scheme satisfying the former also satisfies the latter. Give a formal proof of the converse: namely, show that any scheme that is perfectly indistinguishable is also perfectly secret.

2. **(Perfect PRGs?)** Let $G : \{0,1\}^* \to \{0,1\}^*$ be a function that doubles the length of its input, i.e., $|G(s)| = 2 \cdot |s|$. Show an algorithm A (that does not necessarily run in polynomial time) for which
$$|\Pr[A(G(s)) = 1] - \Pr[A(r) = 1]| \geq \frac{1}{2}$$
for n large enough. (As in class, the first probability is taken over random choice of $s \in \{0,1\}^n$ and random tape of A, and the second probability is taken over random choice of $r \in \{0,1\}^{2n}$ and random tape of A.) Conclude that "perfect PRGs" do not exist.

3. **(An alternate definition of PRGs.)** Given an efficiently-computable function $G : \{0,1\}^* \to \{0,1\}^*$ with $|G(x)| = \ell(|x|)$, consider the following experiment defined for an algorithm A and parameter n:

   (a) Choose random $s \in \{0,1\}^n$ and set $y_0 = G(s)$. Choose random $y_1 \in \{0,1\}^{\ell(n)}$.
   (b) Choose a random bit $b \in \{0,1\}$.
   (c) Give y_b to A, who outputs a bit b'.

   Say G is an *indistinguishable PRG* if for all probabilistic, polynomial-time algorithms A, there exists a negligible function ϵ such that
$$\Pr[b' = b] \leq \frac{1}{2} + \epsilon(n)$$
   in the experiment above.

   Prove that this definition is equivalent to the definition of a pseudorandom generator given in class.