University of Maryland
CMSC858K — Introduction to Cryptography
Professor Jonathan Katz

Problem Set 3

Due at the *beginning* of class on March 8

Please type your solutions, preferably using latex.

1. Let f, g be length-preserving one-way functions (so, e.g., $|f(x)| = |x|$). For each of the following functions f', decide whether it is *necessarily* a one-way function (for arbitrary f, g) or not. If it is, prove it. If not, show a counterexample.

   (a) $f'(x) \stackrel{\text{def}}{=} f(x) \oplus g(x)$.

   (b) $f'(x) \stackrel{\text{def}}{=} f(f(x))$.

   (c) $f'(x_1 \| x_2) \stackrel{\text{def}}{=} f(x_1) \| g(x_2)$.

   ("$\|$" means concatenation.)

2. Let f be a length-preserving one-way function. Let $\mathsf{bit}(i, x) \stackrel{\text{def}}{=} x_i$, the ith bit of x (defined for $1 \leq i \leq |x|$).

   (a) Prove that the function f' defined by
   $$f'(x) = f(x) \| \mathsf{bit}(1, x) \| 1$$
   is one-way, but that the predicate $\mathsf{bit}(1, \cdot) : \{0,1\}^* \rightarrow \{0,1\}$ is not hard-core for f'.

   (b) Construct a function g that is one-way, but such that *no* bit of the input is hard-core.

3. Let G be a pseudorandom generator that expands its input by a single bit. Define
   $$G'(x_1 \| x_2) \stackrel{\text{def}}{=} G(x_1) \| G(x_2).$$
   Prove that G' is a pseudorandom generator.

4. Let G be a length-doubling pseudorandom generator. Prove that G is a one-way function.