University of Maryland
CMSC456—Introduction to Cryptography
Professor Jonathan Katz

Homework 3

Due at the *beginning* of class on Oct. 6

1. Define $G : \{0,1\}^n \rightarrow \{0,1\}^{2n}$ by $G(s) = s \| \bar{s}$ (where $\bar{s}$ denotes the bitwise complement of s). Prove that G is not a pseudorandom generator by describing and analyzing a concrete distinguisher.

2. Define the length-preserving, keyed function F by $F_k(x) = k \oplus x$. Prove that F is not a pseudorandom function by describing and analyzing a concrete distinguisher.

3. In class we discussed the encryption scheme in which a message $M = m_1, m_2, \ldots$ is encrypted to give
$$\langle r_1,\, F_k(r_1) \oplus m_1,\, r_2,\, F_k(r_2) \oplus m_2,\, \ldots \rangle,$$
where $r_1, r_2, \ldots$ are uniform and independent. We prove that this scheme is CPA-secure if F is a pseudorandom function.

   Consider the keyed function F defined by $F_k(x) = k \oplus x$ from the previous problem. Describe how if this F is used in the above encryption scheme, the entire message can be recovered using a ciphertext-only attack and observing a single (sufficiently long) ciphertext.

4. Exercise 3.15. You should provide a short explanation of your answers, but no proofs are needed.