University of Maryland
CMSC456—Introduction to Cryptography
Professor Jonathan Katz

Homework 4

Due at the *beginning* of class on Mar. 11

All numbered exercises refer to the second edition of the book.

1. Let $G : \{0,1\}^n \to \{0,1\}^{2n}$ be a pseudorandom generator. Define the keyed function $F : \{0,1\}^{2n} \times \{0,1\}^n \to \{0,1\}^{2n}$ as $F_k(x) = G(x) \oplus k$. Prove that F is not a pseudorandom function by describing and analyzing a concrete distinguisher D.

2. Exercise 3.20. You should describe and analyze a concrete attacker.

3. Exercise 4.7.

4. Exercise 4.14.

5. Implement the padding-oracle attack discussed in class. The necessary files are available online. Please turn in any code you write, plus the plaintext that was encrypted to give the challenge ciphertext.