University of Maryland
CMSC456 — Introduction to Cryptography
Professor Jonathan Katz

Homework 4

Due at the *beginning* of class on Nov. 15

Note: The exercises below are from the *second edition* of the book.

1. Exercise 6.1.
2. Exercise 6.3.
3. Exercise 6.4.
4. Exercise 6.6.
5. On the webpage you will find code for a 2-round SPN `cipher` and a "wrapper" function `cipher_hiddenkey` that runs the cipher with a uniform key.

   (a) Write a function `inverse` that takes as input a 16-byte key and an 8-byte block, and such that for any key k and any x, `inverse`$(k,$ `cipher`$(k, x)) = x$.

   (b) Implement a key-recovery attack on the cipher. The program implementing your attack should call `cipher_hiddenkey`, and recover the key it is using.

   In addition to submitting your working code, for part (a) please submit the value of `inverse`(k, x) for $k = 0x4C\,4C \cdots 4C$ and $x = 0x00\,00 \cdots 00$, and for part (b) please submit a description of your attack in high-level pseudocode.