

## COMS W4261: Introduction to Cryptography.

Instructor: Tal Malkin

### Problem Set 4

Due: Thur 11/19/09, by the beginning of class (preferably electronically)

Reading: Chapter 4

1. (a) Problem 4.2 in text.  
(b) Problem 4.4(b) in text.
2. Problem 4.7 in text.
3. Problem 4.9(a) in text (proving that CBC-MAC with a random IV is not a secure MAC).

Note the contrast to CBC-mode encryption, where the IV has to be randomized for secure encryption (e.g., see problem 3.16), while here for authentication you are proving that it cannot be randomized.

4. Let  $(Gen, H)$  be a CRHF, and consider the construction  $(Gen, \hat{H})$  defined as follows:  $\hat{H}^s(x) = H^s(H^s(x))$  (that is, applying the original H twice). Prove that  $(Gen, \hat{H})$  is a CRHF.