University of Maryland
CMSC456—Introduction to Cryptography
Professor Jonathan Katz

Homework 4

Due at the *beginning* of class on Oct. 31

1. On the course webpage you will find a challenge ciphertext encrypted using CBC-mode with padding and an unknown key k. (Other useful files are also available.) Your goal is to determine the underlying message that was encrypted. There is a server running that will decrypt any ciphertext you send it, using the same key k; unfortunately, the server does not return the *entire* result of the decryption—instead, it only tells you whether or not the padding was done correctly.

   Please turn in any code you write, as well as (1) the length of the underlying message (before padding is appended), in bytes, and (2) the underlying message, written in ASCII.

2. Exercise 4.4.

3. Exercise 4.9.