

## Homework 5

Due at the *beginning* of class on March 30

1. Implement an attack against basic CBC-MAC showing that it is not secure when used to authenticate/verify messages of different lengths. Here, you will be given the ability to obtain tags (with respect to some unknown key) for any 2-block (32-byte) messages of your choice; your goal is to forge a valid tag (with respect to the same key) on the 4-block (64-byte) message “I, the server, hereby agree that I will pay \$100 to this student.” (Omit the final period and the quotation marks. You should verify that the message contains exactly 64 ASCII characters.) You will also be given access to a verification routine that you can use to verify your solution.

Turn in your code as well as the tag (in hex) for the 64-byte message above.