The University of North Carolina at Greensboro
CSC 580: Cryptography and Security in Computing
Prof. Stephen R. Tate

Handout 10
February 16, 2017

Homework 5 – Due Tuesday, February 21

1. Recall that cipher "modes" are ways of using block ciphers when the input is larger than a single block. Describe ECB mode and CBC mode encryption ("describe" can mean just giving either a clear diagram or formulas). What is the advantage of CBC mode over ECB mode? Is there any advantage of ECB over CBC?

2. You are developing an application in which you have to regularly send packets that are 36 bytes (288 bits) long using AES. If you use CBC mode, how much data do you need to transmit? Be sure to explain the reasoning behind your answer (show your work).

3. Joe Crypto always loved playing the "guess which hand is holding a prize" game, so proposes the following guessing game: You can give him two files, containing whatever data you want them to contain, but with the restriction that they must be the same length. He will then pick one of them, encrypt it with a secret key, and then give you the resulting ciphertext. You have to guess which file he encrypted! Joe's crypto knowledge isn't so great, however, and he uses AES in ECB mode. How can you play this game so that you can win? Be very specific, including a clear explanation of why your strategy allows you to win. The number of bonus points you get depends as much on the clarity of your description as it does the technical quality of your strategy. (*Hint: What is the main weakness of ECB mode, and how can you create a file that displays this weakness?*)