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

Handout 21
April 13, 2017

Homework 11 – Due Tuesday, April 18

1. In this problem, we revisit the DAA MAC scheme from the previous homework: if the input message is $D_1, \ldots, D_N$, and $E(K, M)$ is the encryption function for any block cipher, such as DES or AES, we first compute

$$\begin{aligned} O_1 &= E(K, D_1) \\ O_2 &= E(K, D_2 \oplus O_1) \\ &\cdots \\ O_N &= E(K, D_N \oplus O_{N-1})\,. \end{aligned}$$

   The final MAC is O_N. If we know that the MAC of a single block message D_1 is T, it is possible to figure out what the MAC of the two block message $D_1, T \oplus D_1$ is, even if you don't know the key. What is it? Justify your answer (show your work).

2. There are two main authenticated encryption techniques described in the book, CCM and GCM. Describe at least two advantages of GCM over CCM.

3. Both MACs and digital signature schemes are designed with the goal of being resistant to "existential forgery." Describe what this means and why this is an important property.