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

Handout 5
January 19, 2017

Homework 2 – Due Tuesday, January 31

1. What is the closest power of two to
   (a) 16 million
   (b) 4 billion
   (c) number of nanoseconds in one week
   (d) number of seconds in 8 years

2. This is the "extreme, over-the-top, super-secure keysize security" estimation problem. Consider if you could convert *an entire planet* into one big computer (suggestion: read *The Hitchhiker's Guide to the Galaxy* if you haven't) — look in the table of large numbers and find how many atoms are in the Earth, and assume that you can make a logic gate out of every 8 atoms in the planet. Next, assume that you can clock those gates at the fastest imaginable speed, the frequency of ultraviolet light, which would be a 1,000 THz computer, and testing a key takes at least 1000 Boolean operations. Finally, a "super-secure" cipher is one that cannot be brute-forced in under 128 years. What keysize would need to be used so that a cipher is "super-secure" against attacks using this ultra-fast full-planet computer? You can (and should!) estimate all values as powers of two when you solve this problem.

3. You have found out that a bank sends money transfer messages encrypted with a one-time pad using XOR on bytes. You know that if you transfer $1000 from branch A to branch B, branch A encrypts and sends a message that says "Add 1000 dollars to Steve's balance." Explain, with as much detail as you can, how you can intercept and tamper with this message so that 9,999 dollars is added to my account instead of 1,000 dollars.