Homework 02

ECE 443/518, Fall 2022

Due Date: 11:00am 09/21 Chicago time

1. *(4 points)* Solve Problem 1.4 (p25 in Understanding Cryptography).

2. *(3 points)*

   A. Calculate $2x \bmod 13$ for $x = 1, 2, \ldots, 12$.

   B. Calculate $3x \bmod 13$ for $x = 1, 2, \ldots, 12$.

   C. Argue that if p is a prime number and $1 \leq x < y \leq p - 1$ are two integers, then for any integer $1 \leq a \leq p - 1$, $ax \bmod p$ and $ay \bmod p$ cannot be the same.

3. *(3 points)*

   A. Calculate $2^x \bmod 13$ for $x = 1, 2, \ldots, 12$.

   B. Calculate $3^x \bmod 13$ for $x = 1, 2, \ldots, 12$.

   C. What do the infinite sequences $2^x \bmod 13$ and $3^x \bmod 13$ look like for $x = 1, 2, \ldots,?$

4. *(2 points)* Solve Problem 2.4 (p52 in Understanding Cryptography).

5. *(2 points)* Solve Problem 4.16 (p121 in Understanding Cryptography).
   For Moore's Law, simply assume that computer power doubles every 18 months.

6. *(1 points)* Solve Problem 5.9 (p146 in Understanding Cryptography).