Homework 01

ECE 443/518, Fall 2025

Due Date: 09/14 (Sun.) by the end of the day (Chicago time)

1. *(1 point)* Solve Problem 1.4 (p25 in Understanding Cryptography).
2. *(0.5 point)*
   A. Calculate $2x \bmod 13$ for $x = 1, 2, \ldots, 12$.
   B. Calculate $3x \bmod 13$ for $x = 1, 2, \ldots, 12$.
   C. Do results from A and B show similar properties? 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. *(0.5 point)*
   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 $x = 1, 2, \ldots,$? Are you expecting the same for $a^x \bmod n$ for any integer a and n?
4. *(1 point)* Solve Problem 2.4 (p52 in Understanding Cryptography).
5. *(0.5 point)* Solve Problem 4.16 (p121 in Understanding Cryptography).
   For Moore's Law, simply assume that computer power doubles every 18 months.
6. *(0.5 point)* Solve Problem 5.9 (p146 in Understanding Cryptography).
7. *(1 point)* Solve Problem 11.2 (p315 in Understanding Cryptography).