MCS 425: Codes and Cryptography (Spring 2020)

Homework 2

Due in class, Friday, Feb 21

If you solve a homework question by code, you have to write your own code.

**Extended Euclidean algorithm:**

1a) Compute gcd(425, 2020) by hand. Show your work.

1b) Compute $46^{-1}$ mod 191 by hand. Show your work.

2) Write or print (pseudo)code for the extended Euclidean algorithm. That is, given two positive integers $a$ and $b$, find integers $x$ and $y$ such that $ax + by = \gcd(a, b)$. Your code should use $O(\log(a+b))$ arithmetic operations.

3) Find all solutions of $102x \equiv 15 \pmod{141}$.

**Modular exponentiation:**

4a) Compute $5^{64} \mod 7$ by hand. Show your work.

4b) Find the last 3 digits of $143^{399}$.

5) Write or print (pseudo)code for fast modular exponentiation. That is, given positive integers $x, a, \text{ and } n$, compute $x^a \mod n$. Your code should use $O(\log(a))$ arithmetic operations.

**Chinese remainder theorem:**

6) Suppose $x \equiv 1 \pmod{16}$ and $x \equiv 8 \pmod{31}$. Compute $x \mod 124$. 