SCI 2000
Introduction to Encryption, Assignment 2
Due February 25th at the start of class.

Questions will be marked both on correctness and clarity of presentation. Poor writing and sloppy/illegible presentation both impact the clarity of your work and so will be penalized. You must show all steps in your computations to get credit.

Question 1: Recall that for an affine cipher $f_{a,b}(x)$ to be $1-1$ and onto, the integer a has to be relatively prime to 26, and when a is not relatively prime to 26 the function is NOT $1-1$ and onto. Show that $f_{8,3}(x) = 8x+3 \mod 26$, considered as a function from $\{0,\ldots,25\}$ to $\{0,\ldots,25\}$, is not $1-1$ and is not onto.

Question 2: When an integer a is relatively prime to 26, it means that a has an inverse modulo 26, which is a number x in $\{0,1,\ldots,25\}$ such that $ax = 1 \mod 26$. This is what makes $f_{a,b}(x)$ turn out to work as a cipher. We will prove that this works later in the course, but in this question we'll cover an easy special case.

In this question you will prove why, if p is a prime ($p > 2$), every integer a in $\{0,1,\ldots,p-1\}$ has an inverse modulo p—that is, there's a number x in $\{0,1,\ldots,p-1\}$ such that $ax = 1 \mod p$. Here is how the argument goes:

For a fixed number a in $\{0,1,\ldots,p-1\}$, consider all the products $a\cdot 0 \mod p$, $a\cdot 1 \mod p$, $a\cdot 2 \mod p$, $\ldots$, $a\cdot(p-1) \mod p$.. If the number 1 appears somewhere in this list, then a has an inverse modulo p. **Finish the argument by:**

(a) Explaining why, if $a\cdot k \mod p$ and $a\cdot \ell \mod p$ are different whenever $k,\ell \in \{0,1,\ldots,p-1\}$ are distinct, then 1 must appear in the list above.

(b) Explaining why $a\cdot k = a\cdot \ell \mod p$ can never happen when k and ℓ are distinct.

Hint for proofwriting: The argument for each of these steps does not need to be long! Two or three very clear, concise, logical sentences will do the trick.

Question 3: This is Exercise 5.6.12 from the textbook, part (a). We often counted how many keys there were for different ciphers as a measure of their strength.

For the 2×2 Hill cipher, a key is a 2×2 matrix with entries from $\{0,\ldots,25\}$ that has an inverse mod 26. How many such matrices are there? **Hint: For such a matrix to have an inverse, no column can be zero and the columns cannot be multiples of one another mod 26. How many choices are there for each column? Why?**

Question 4: Encrypt the message "HI" using a stream cipher using the LFSR given by $b_5 \leftarrow b'_1 + b'_4$ and seeded with 11011. If you use an online ASCII converter, you'll find that "HI" in binary is 0100100001001001. Given this, what is the binary ciphertext?

Question 5: For each of the parts below, give an example of a 4-bit LFSR and a choice of seed such that:

(a) The LFSR returns to its original state after 8 iterations, and not sooner.

(b) The LFSR returns to its original state after 16 iterations, and not sooner.

For each example of LSFR in each of the four parts above, compute all of the states of the LFSR that arise before repetition. Please do not use examples from class or the textbook.