1. (26 points = 17+9) (a) Suppose a message is encrypted using the function $y \equiv 7x \pmod{26}$, so $a = 0$ encrypts to $A = 0$, and $b = 1$ encrypts to $H = 7$, etc. The ciphertext is $CD$. Find the plaintext. (Recall that $a = 0, b = 1, b = 2, \ldots, z = 25$.)

(b) Why is the function $y \equiv 13x \pmod{26}$ not a good choice for an encryption function?

2. (18 points) You may assume the fact that $m^{270300} \equiv 1 \pmod{1113121}$ for all $m$ with $\gcd(m, 1113121) = 1$. Let $e$ and $d$ satisfy $ed \equiv 1 \pmod{270300}$. Suppose $m$ is a message with $0 < m < 1113121$ and $\gcd(m, 1113121) = 1$. Encrypt $m$ as $c \equiv m^e \pmod{1113121}$. Show that $m \equiv c^d \pmod{1113121}$. Show explicitly how you use the fact that $ed \equiv 1 \pmod{270300}$ and the fact that $m^{270300} \equiv 1 \pmod{1113121}$. (Note: $\phi(1113121) \neq 2703000$, so Euler’s theorem does not apply.)

3. (27 points = 9+9+9) The operator of a Vigenère encryption machine is bored and encrypts a plaintext consisting of the same letter of the alphabet repeated several hundred times. The key is a six-letter English word, though Eve doesn’t know this yet.

(a) What property of the ciphertext will make Eve suspect that the plaintext is one repeated letter and will allow her to guess that the key length is six?

(b) Once Eve recognizes that the plaintext is one repeated letter, how can she determine the key? (Hint: you need the fact that no English word of length six is a shift of another English word.)

(c) Suppose Eve doesn’t notice the property needed in part (a), and therefore uses the method of displacing then counting matches for finding the length of the key. What will the number of matches be for the various displacements? In other words, why will the length of the key become very obvious by this method?

4. (15 points) Suppose we build an LFSR machine that works mod 3 instead of mod 2. It uses a recurrence of length 2 of the form

$$x_{n+2} \equiv c_0 x_n + c_1 x_{n+1} \pmod{3}$$

to generate the sequence 1, 1, 0, 2, 2, 0, 1, 1. Set up and solve the matrix equation to find the coefficients $c_0$ and $c_1$.

5. (14 points = 7+7) (a) State a way in which the one-time pad is superior to LFSR sequences. (10 words or fewer)

(b) State a way in which LFSR sequences are superior to the one-time pad. (10 words or fewer)