Midterm 1 practice problems

As you study for the first midterm, you might find it helpful to make sure you know how to do the following problems. There is no guarantee that all midterm problems will look like problems from this list.

(1) Decide if each statement below is true or false. If false, provide a counterexample or explain why; if true, explain why.
   (a) Every nonzero matrix defined mod 7 has an inverse.
   (b) If you have converted a message to bits and are using a random sequence of ones and zeros as a one time pad, then the encryption key is the same as the decryption key.
   (c) The substitution cipher is a symmetric cipher.
   (d) Kerckhoffs's principle is that one should always assume that the enemy knows the method of encryption being used, so that the security of the system is based on the key and not on keeping the algorithm secret.

(2) Suppose we use an affine cipher with 96 symbols (26 uppercase and lowercase letters, plus a space, numerals, and punctuation), so that we are working mod 96. Find the number of different keys for this cipher.

(3) Find an integer matrix $\begin{pmatrix} a & b \\ 13 & 37 \end{pmatrix}$ with determinant 1.

(4) The ciphertext for a substitution cipher on English plaintext is

   `XCCZ ZBC KLCMM,`

   and you know that the middle word is one of the most common three–letter words (the, and, for, are, but, not). Which word do you think it is and why?

(5) What is a chosen ciphertext attack?

(6) You are using a block cipher such as AES with a block length of 128 bits. You divide the plaintext P into 128–bit blocks, $P = P_1P_2P_3\ldots$, and encrypt each block separately, so that the ciphertext $C = C_1C_2C_3\ldots$, with $C_i = E_K(P_i)$. Why is this a bad idea? How could Eve attack this system? Name two other modes of operation for block ciphers and describe advantages or disadvantages of each.

(7) (a) Prove that $X^3 + 2X + 1$ is irreducible in $\mathbb{Z}_5[X]$.
   (b) Find the inverse of $4x + 1$ in the field $GF(125) = \mathbb{Z}_5[X]/(X^3 + 2X + 1)$.

(8) Suppose we build a LFSR machine that works mod 3 instead of mod 2. If c_0 and c_1 are chosen to be integers (mod 3), it uses a recurrence of the form

$$x_{n+2} \equiv c_0x_n + c_1x_{n+1} \pmod 3$$

   to generate the sequence $2, 2, 0, 1$. Find the coefficients c_0 and c_1. Find the period of the sequence. Show your work.

(9) Find all solutions to the congruence $9x \equiv 6 \pmod{96}$.

(10) Suppose you have a language with only the 3 letters a, b, c, and they occur with frequencies $.7, .2, .1$, respectively. The following ciphertext was encrypted by the Vigenére method (shifts are mod 3 instead of mod 26 of course): `ABCBABBBAC`. Suppose you are told that the key length is 1, 2, or 3. Show that the key length is probably 2, and determine the most probable key.