Homework 9, due September 23

(1) (Page 146, problem 1) Consider the following DES–like encryption method. Start with a message of $2n$ bits. Divide it into two blocks of length n, a left half and a right half: M_0M_1. The key K consists of k bits, for some integer k. There is a function $f(K,M)$ that takes inputs of k and n bits and gives an output of n bits. One round of encryption starts with a pair M_jM_{j+1}. The output is the pair $M_{j+1}M_{j+2}$, where

$$M_{j+2} = M_j \oplus f(K, M_{j+1}).$$

(Here $\oplus$ means XOR, or addition mod 2 on each bit.) This is done for m rounds, so the ciphertext is M_mM_{m+1}.

If you have a machine that does the m-round encryption just described, how would you use the same machine to decrypt the ciphertext M_mM_{m+1} using the same key K?

(2) (Continued.)
  (a) Suppose K has n bits and $f(K,M) = K \oplus M$, and suppose that the encryption process consists of $m = 2$ rounds. If you know only a ciphertext, can you deduce the plaintext and the key? If you know a ciphertext and the corresponding plaintext, can you deduce the key? Justify your answers.
  (b) Suppose K has n bits and $f(K,M) = K \oplus M$, and suppose the encryption process consists of $m = 3$ rounds. Why is this system not secure?

(3) Find the number of different (good) keys there are for a 2 by 2 Hill cipher without counting them one by one, and find the number of keys with determinant 1. Remember that the determinant has to be relatively prime to 26. Here's one approach to solving the problem:
  (a) Show that the number of good keys mod 26 is equal to the number of good keys mod 13 times the number mod 2. (Find an explicit one–to–one map between matrices mod 26, and pairs of matrices, where the first is a matrix mod 2 and the second is a matrix mod 13.)
  (b) Show that the number of non-invertible matrices mod a prime p is $(2p-1)^2 + (p-1)^3$ by showing the following claims. Let $A = \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right)$. Then A is non-invertible if and only if $ad \equiv bc \pmod{p}$. There are two cases: $ad \equiv bc \equiv 0$ or $ad \equiv bc \not\equiv 0$.
    (i) The first case happens $(2p-1)^2$ times.
    (ii) The second case happens $(p-1)^3$ times.
  (c) From this conclude that the number of good keys is 157248.
  Now that you have the number of 2 by 2 Hill cipher keys whose determinant is relatively prime to 26, you can find the number which have determinant 1 as follows:
  (d) Find a 2 by 2 matrix with determinant a, for every number a relatively prime to 26.
  (e) Show that this matrix with determinant a has an inverse modulo 26.
  (f) Use this matrix to establish a pairing between matrices with determinant 1 and matrices with determinant a.
  (g) Now you know that there are the same number of matrices with determinant 1 as there are with determinant a, for every a which is relatively prime to 26. Find the number of matrices whose determinant is 1.