Math 4450/6450 Cryptography Test #2 -- April 23, 2010

For the following problems be sure to carefully explain your method of solution, and show all relevant work. No credit will be given for correct answers without justification.

1) Please give the precise definitions of the following terms:
   a) q-ary code of length n
   b) Hamming distance between two codewords
   c) Hamming weight of a codeword
   d) code rate R of a code

2) Suppose C is an [n, k, d] = [7, 4, d] linear binary code.
   a) What is the code rate of this code?
   b) How many code words are there?
   c) What is the maximal d allowed by the singleton bound?
   d) How many errors does this allow us to reliably correct?
   e) Can we find a linear [7, 4, d]-code which can correct this many errors?

3) Please carefully explain how to perform/implement the Baby-step Giant-step attack, and what “hard problem” it solves.

4) Please use Fermat factorization (mod n) to find a factorization of n = 51. (Please be sure to show every step of work for full credit!)

5) Please perform the Pollard p-1 attack to find a factorization of n = 55.

6) Please prove that an (n, M, 2t+1)-code can reliably detect 2t errors and reliably correct t errors.