NUMBER THEORY: PROJECT

Project due on Friday December 5, the last day of the class.

This project is an extra 5% credit adding to your overall score.

You are assigned to work as a team which listed below:
Red: Richard (captain), Casey, Criag, Erik
Blue: Jeff (captain), Zack, Olivia, Leigh

For problem 1 and 2, you are asked to fill out the details of Maple program that I posted on my web site.
Once you're done, send me your solution in paper and also send me your Maple code by email.

1. Project

Problem 1) The Lucas-Lehmer test is considered to be the fastest algorithm for finding Mersene primes. The proof of the algorithm requires the knowledge of complex number and algebraic number theory. But the algorithm is not hard to implement.

In this problem, you are asked to implement the Lucas-Lehmer test on the page 260 to rediscover as many Mersene primes as possible.

Problem 2) Write Maple problem to do problem 50,51,52,53 and 55 on page 33 in Andrews-Eriksson's book.

Problem 3) Suppose the 10-letter alphabet: 0-9 is used for plaintexts and ciphertexts. Suppose that the plaintext message units are 8-digits and the ciphertext message units are 9-digits.

Let my encryption key (n, e) be $(47067463, 2367)$.

a) For each of the team member: send your birth date to me (after you encrypt it of course).
If you born on January 2nd 1988, your plaintext message unit should

Date: Tuesday, November 25, 2008.

be 01021988.

b) Intercept my secret birth date which the ciphertext message unit is 44437822. Explain your process to break my code. Also include the decryption key (n, d).