Homework Assignment 5
CS 6104: Algorithmic Number Theory

Each problem in this assignment is worth 50 points. The assignment is due by 9:30AM on **June 25, 1998.** Prepare your solutions in LaTeX, preferably using this file as a starting point. You may submit your solutions in printed form or by email to `cs6104@ei.cs.vt.edu`. Explain your solution to each problem, including references to the appropriate theorems in the textbook.

Help is available by email as well as during my office hours. It is especially helpful to request clarification or hints by email to `cs6104@ei.cs.vt.edu`, so I can send the response to everyone.

The person assigned to present the solution to a problem is noted at the beginning of the problem.

Problem 1. [Hussein] Completely factor the polynomial

$$f(X) = X^8 + 4X^5 + 3X^2 + 5$$

over $\mathbb{Z}/(7)$ using both the Berlekamp and Cantor-Zassenhaus algorithms. You may use *Mathematica* to do the calculations at each intermediate step, but show the results of all the steps.

Problem 2. [Scott] Consider the following instance of the Merkle-Hellman public-key encryption scheme:

$$\begin{aligned} p &= 1239671 \\ y_1 &= 455933 \\ y_2 &= 735485 \\ y_3 &= 640682 \\ y_4 &= 878709 \\ y_5 &= 1102018 \\ y_6 &= 869434. \end{aligned}$$

Do the following.

A. Implement the algorithm for solving low density SUBSET SUM problems in *Mathematica*. Note that the lattice basis reduction algorithm is built into *Mathematica* as the function `LatticeReduce`.

B. Show how to use the algorithm to decrypt the message

$$t = 1238514.$$

C. **Bonus subproblem:** Recover the hidden keys c and d and the superincreasing sequence

$$x_1, x_2, x_3, x_4, x_5, x_6$$

used to construct the above scheme. THIS SUBPROBLEM IS OPTIONAL!
