MATH 800 Cryptography
Course Project, Fall 2008

Michael Monagan

The project is due Thursday December 11th at 5pm.
Late penalty: -20% for up to 24 hours late. Zero after that.

The Pohlig-Hellman algorithm.

Study the and the material in 6.2.3 on the Pohlig-Hellman algorithm for computing discrete logarithms. Do exercises 6.4 and 6.5 on page 276. Use your solution to 6.5 to answer 6.4 (d).

Elliptic curves cryptography.

Study the material in section 6.5.1, 6.5.2 and 6.5.3 on elliptic curves and the material in 6.5.4 describing the Elliptic Curve Integrated Encryption Scheme (ECIES). Do exercises 6.13 and 6.17 on page 278.

Notes on 6.13. To answer part (c) you need to write a Maple procedure that computes the order of an element in E. Now your answer to parts (a) and (c) will answer part (b). Also your answer to part (c) should be consistent with Theorem 6.1 on page 261. What is the group E that you get?

Notes on 6.17. Please verify that the order of $P = (2, 9)$ is 39 in E as claimed in the question. For part (a), you should use the equivalent of the SQUARE-AND-MULTIPLY algorithm in $E(+)$ which, since the group operation is addition, the book calls it the DOUBLE-AND-ADD algorithm in 6.5.5. For part (c), I get that the plaintext is a four letter word ending in "LE".