Final Exam -- Monday May 2 -- 8:00 to 10:00 AM -- 600 SEO

During the exam, you may use:

- Your completed Crypto Club Workbook
- Your list of all prime numbers less than 10,000
- Your calculator with any programs.

You may NOT share any of the above with other students during the exam.

1. Understanding arithmetic in different bases.

2. lcm and gcd and factoring

   Compute both in several ways AND explain why the method works.

3. Euclidean Algorithm and Extended Euclidean algorithm

   Know when to use them and how to use them and be able to carry through by hand for smaller numbers. Know how to explain why they work. Know how to use your calculator to carry through for larger numbers.

4. Solving linear Diophantine equations

   The arrow method is most welcome, especially if you can explain why it works, as are calculator programs.

5. Word problems: problem set #7:

   Solving equations in modular arithmetic.

6. Using Commutative, Associative and Distributive Properties

   Beckmann activities presented in class. Understanding negative numbers.

7. Modular arithmetic.

   Explain basic facts – cancellation in particular. TRUE and FALSE. Find inverses -- know when they exist or not. Reduce large powers.

8. Prime numbers.

   Sieve of Eratosthenes, prime factorization, anything from the teaching projects.

9. Cryptography

   Know how to encrypt and decrypt: Caesar, keyword, Vigenère, multiplicative, affine and RSA. Know techniques for cracking. Know how to explain why things work. Extend to larger numbers and different alphabet schemes.