

Study Guide, Exam 2, Math 485

This list is not guaranteed to be complete.
Testing center calculators may be used on the exam.

Definitions/Concepts to know:

1. Chinese Remainder Theorem
2. Fast modular exponentiation
3. Fermat's Little Theorem
4. Euler phi function
5. Euler's theorem
6. Primitive roots mod p
7. Square roots mod n
8. Legendre and Jacobi symbols
9. Quadratic reciprocity
10. Continued fractions
11. Public key cryptosystems
12. RSA algorithm
13. Continued fraction low exponent attack on RSA
14. Fermat primality test
15. Solovay-Strassen primality test
16. Fermat factorization
17. Pollard $p-1$ factorization algorithm
18. Quadratic sieve
19. Discrete logarithms
20. Pohlig-Hellman algorithm
21. Baby step, giant step algorithm
22. Diffie-Hellman key exchange
23. ElGamal cryptosystem
24. Hash functions
25. Birthday attacks
26. Digital signatures (RSA, ElGamal)

Examples of problems you should be able to do:

1. Calculate Jacobi symbols
2. Calculate exponentials (modulo n)
3. Find square roots of a number (modulo n)
4. Encrypt or decrypt RSA and ElGamal messages, given appropriate public or private keys
5. Use principles and algorithms learned in class to test for primality
6. Use principles and algorithms learned in class to factor integers
7. Find simple discrete logarithms
8. Sign documents using RSA or ElGamal
9. Describe strengths, weaknesses, and attacks for algorithms we have studied in class
10. Given a cryptosystem that is similar (but not identical) to those we have studied in class, evaluate its weaknesses; for example, is it susceptible to birthday attacks?

Remember that the learning outcomes for the course state that students "should gain an understanding of [the core] topics. In particular this includes knowing the definitions, being familiar with standard examples, and being able to solve mathematical and algorithmic problems by directly using the material taught in the course."