Study Guide, Exam 1, Math 485

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

Definitions/Concepts to know:

1. Alice/Bob/Eve model
2. Types of attacks
3. Kerckhoffs's principle
4. Shift cipher and attacks
5. Affine cipher and attacks
6. Vigenère cipher and attacks
7. Substitution cipher and attacks
8. Block ciphers
9. Hill cipher and attacks
10. One-time pads
11. Pseudorandom bit generation
12. LFSRs and attacks
13. Divisibility and prime numbers
14. GCD
15. Euclidean algorithm
16. Solving ax+by=d
17. Congruences
18. Division (mod n)
19. Finite fields
20. Feistel systems
21. DES
22. Modes of operation, strengths and weaknesses of each
    a. ECB
    b. CBC
    c. CFB
    d. OFB
    e. CTR
23. Meet-in-the-middle attacks
24. AES

Examples of problems you should be able to do:

1. Use the Euclidean algorithm to find the inverse of a number (mod n)
2. Find the key length for a Vigenère cipher
3. Solve an affine cipher given two letters of plaintext
4. Find all solutions to a linear congruence (mod n)
5. Find a linear recurrence, given an output string
6. Decrypt a Hill cipher
7. Given a function f(K, M), a message M, and a key K, give the ciphertext if ECB, CBC, or CTR modes are used
8. Add, subtract, multiply, divide, and find inverses in finite fields
9. Describe strengths, weaknesses, and attacks for ciphers we have studied in class
10. Given a cipher that is similar (but not identical) to those we have studied in class, evaluate its weaknesses

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."