CSC 231 FINAL EXAMINATION STUDY GUIDE

PROFESSOR GODFREY C. MUGANDA

Consult all previous study guides and homework problems.

In addition, work problems 3 on page 549.

From the chapter on number theory and cryptography, you should be able do define and explain the following concepts. The division algorithm. Modular arithmetic, including addition, multiplication and exponentiation. The concepts of gcd and lcm. Existence of multiplicative inverses. Fermat's Little theorem. The Euler totient function $\phi(n)$. The RSA cryptosystem: how it to find the keys, and how to encrypt and decrypt. The Diffie-Hellman key exchange protocol and how it works.

Work the following problems for practice: page 244: problems 9, 11, and 14; page 286: problems 39(a); page 255: problems 1, 3, 7 without calculators; page 272: problem 21.

I will tell you on Thursday what else will be on the test from what is covered on Thursday.