Exam I Guide

Overview
Exam I will take place on Monday, October 17 (not on Wednesday, October 19 due to Ingram's talk). The exam will include homework 1–4 and all material covered up to and including the lecture on Monday October 10. Exam questions will be similar to quiz questions—most questions will evaluate your understanding by having you apply major course concepts to new situations. In addition, there may be pointed questions assessing your command of details from the readings and there may be questions relating to homework assignments. The exam will be a 75 minute, closed-book test (no calculators allowed).

Readings

1. Sinkov: Entire book.
2. Denning: Sections 1.1–1.3, 1.6 (not Chinese remainder theorem yet), 2.1–2.5 (not 2.4.5 yet), 3.6.
3. Sherman: "How we solved the $100,000 Decipher Puzzle (16 hours too late)," available over WWW from Sherman's home page.
4. Gaines (recommended): Sections on all hand ciphers that we studied.
5. Cormen, Leiserson, Rivest (recommended): "Chapter 33: Number-Theoretic Algorithms" in *Introduction to Algorithms*, MIT Press and McGraw-Hill (New York, 1990).

Major Concepts
Privacy and authentication, one-way function, one-way trapdoor function, unicity distance, conventional vs. public-key cryptosystems, confusion and diffusion, cryptographic combination, strengths and weaknesses of ciphers, perfect secrecy, Index of Coincidence, repeat rate, Kasiski method, bigram scoring methods, vowel-count method, cryptanalytic techniques for hand ciphers, language redundancy, key escrow.

Ciphers
One-time pad, substitution, transposition, single columnar transposition, polyalphabetic substitution, Vigenère, Beaufort, Playfair, Hill cipher, homophonic ciphers, Beale cipher, Decipher Puzzle, Clipper chip, RSA.

Math Tools
Elementary probability and number theory, modular arithmetic, linear Diophantine equations and how to solve them, law of large numbers, conditional probability.