UMBC — CMSC–443

Fall 1994 — Cryptography and Data Security

Exam II Guide

Overview

Exam I will take place Wednesday, November 23. The exam will cover all course material to date, focusing on topics discussed since Exam I. This material includes homeworks 1–7 and all lectures through November 16 (including Ingram's lecture). The three major topics since Exam I are information theory and its application to cryptology, the mathematics and security of RSA and Rabin's cryptosystem (including the proof that RSA works correctly and the proof that breaking Rabin's system is a hard as factoring the modulus), and factoring and primality-testing algorithms (including the Miller-Rabin test).

Exam II will be similar in construction to Exam I; in particular, 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). As a central part of your study, you should solve as many problems as possible.

Readings

1. Denning: Chapters 1 (especially Sections 1.4 and 1.6), and Sections 2.7 and 3.7.
2. Stinson, Chapter 4 (RSA and Factoring).
3. Kent, Stephen T., "Internet privacy enhanced mail," *CACM*, **36**:8 (August 1993), 48–59.
4. Cormen, Leiserson, Rivest (strongly 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, random function, random permutation, conventional vs. public-key cryptosystems, digital signatures, key escrow, unicity distance, self-information, entropy, equivocation, random ciphers, perfect secrecy, information-theoretic vs. computational complexity based security, proof of security relative to a hard problem, information and redundancy, coding theory vs. cryptography, factoring and primality testing, covert channels, zero-knowledge complexity.

Ciphers

RSA, Rabin, DES.

Algorithms

Extended Euclid, repeated squaring, trial division, Pollard's rho method, Fermat's primality test, Miller-Rabin primality test, Schönhage-Strassen integer multiplication algorithm based on the discrete fast Fourier transformation, Floyd's two-finger cycle-detection algorithm.

Math Tools
Modular arithmetic, additive and multiplicative groups modulo n, Chinese Remainder Theorem, Fermat's Little Theorem, Euler's Theorem, Prime Number Theorem, quadratic residuosity, Legendre symbol, Jacobi symbol, information theory, Bayes Theorem, proof by reduction, graphs of discrete functions.

Sample Questions

1. Explain how to apply the concepts of digital signatures and public-key cryptography in a given practical context.
2. Analyze the security of a given cryptographic application involving digital signatures and public-key cryptography.
3. Prove that RSA works correctly.
4. Prove that breaking Rabin's scheme is as hard as factoring the modulus.
5. State and prove the Chinese Remainder Theorem.
6. Carry out a "network attack" against Rabin's system.
7. Carry out and explain Pollard's rho factoring method for a given example.
8. Estimate the unicity distance of a given cipher.
9. Calculate the entropy, equivocation, and mutual information of various cryptographic random variables in a given practical setting.
10. Prove various properties of concepts from information theory.
11. Define the term *random cipher* and estimate its unicity distance. Carefully justify your calculations.
12. Analyze the time and space complexity of encrypting with RSA.