UMBC — CMSC–443
Fall 1994 — Cryptography and Data Security

# Final Exam Guide

## Overview

The final exam will take place Wednesday, December 21, 3:30–5:30pm in our usual classroom (MP 101). This comprehensive exam will be similar in construction to the previous exams. In particular, 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 and quizzes. The exam will be a two-hour, closed-book test (no calculators allowed). As a central part of your study, you should solve as many problems as possible, and you should review all previous homework, tests, and quizzes.

## Readings

1. Denning: Chapters 1–3 (complete).
2. Sinkov: Entire book.
3. Stinson, Chapter 4 (RSA and Factoring).
4. Kent, Stephen T., "Internet privacy enhanced mail," *CACM*, **36**:8 (August 1993), 48–59.
5. Baldwin and Sherman: "How we solved the $100,000 Decipher Puzzle (16 hours too late)," *Cryptologia*, **XXIV**:3 (July 1990), 258–284. Available over WWW from Sherman's home page.
6. Cormen, Leiserson, Rivest (strongly recommended): "Chapter 33: Number-Theoretic Algorithms" in *Introduction to Algorithms*, MIT Press and McGraw-Hill (New York, 1990).
7. Cain, Thomas; and Alan T. Sherman, "How to break Gifford's Cipher (extended abstract)," *Second Annual ACM Conference on Computer and Communications Security*, ACM Press (November 2–4, 1994), 198–209. (Recommended) Available over WWW from Sherman's home page.
8. Gaines (recommended): Sections on all hand ciphers that we studied.

## Major Concepts

In addition to the concepts from Exams 1–2: digital signatures, zero-knowledge complexity, factoring, primality testing, randomized algorithm, oblivious transfer, coin flipping into the well, block cipher, chaining methods, bignums, statistical cryptanalysis, time-space tradeoffs, impossibility proofs based on information theory, cryptographic protocols.

## Ciphers

In addition to the ciphers from Exams 1–2: DES (and related four modes of operation), Gifford's Cipher, Hagelin M-209B converter (see display in Kuhn Library special collections).

**Cryptographic Protocols**
Zero-knowledge authentication protocols based on three-coloring and on graph isomorphism, mental poker, Blum's oblivious transfer, Needham-Schroeder key distribution, Diffie-Hellman key exchange.

**Algorithms**
In addition to algorithms from Exams 1–2: Fermat's primality test, Miller-Rabin primality test, repeated squaring, Hellman time-space tradeoff.

**Math Tools**
In addition to the math tools from Exams 1–2: Prime Number Theorem, quadratic residuosity, Legendre symbol, Jacobi symbol, discrete logarithm, graph coloring, graph isomorphism, complexity classes.

**Sample Questions**
See also the sample questions from Exams 1–2.

1. Given a new practical application, explain how to apply the concepts of digital signatures and public-key cryptography in the application.
2. Given a new cryptographic protocol, analyze its security.
3. Given a new interactive protocol, prove whether or not it is zero-knowledge.
4. State and prove the complementation property of DES, and explain its cryptanalytic significance.
5. What are the so-called "weak keys" of DES, and explain how they arise.
6. Compare the error-propagation properties of the CBC, CFB, and OFB modes of operation for DES.
7. Given a new cipher, explain how to adapt the Hellman time-space tradeoff to this cipher.

**Two Major Difficulties from Exams 1–2**
Two serious difficulties occurred in the Exams 1–2: First, some students thoughtlessly listed course material in a shotgun fashion rather than specifically and directly answered exam questions through appropriate, selective use of facts. Be thoughtful and keep your answers succinct and focused. Second, many students demonstrated only a vague brush-stroke understanding of course concepts rather than a precise, detailed command of both the significant ideas and of the underlying details. Throughout the course, be sure to learn each and every topic, concept, and technique with deep understanding.