

Computer Science 349

Cryptography

Spring 2004

Instructor

Instructor: Randy Shull
Office: E120 Science Center
Extension: 3102
Office: Wednesday, 10:00 – 12:00
Friday, 8:30 – 10:00

Overview

The course begins with an introduction to classical symmetric-key cryptography. We will examine several of the most famous cryptographic systems and learn how to break them. The security of each of these systems depended to a large degree on the ingenuity of its creator. Everyone is convinced of the absolute security of their own cipher. Unfortunately nearly everyone is wrong. We spend several weeks studying Claude Shannon's *Theory of Secrecy Systems* to order to help us evaluate the security of cryptographic systems. A short detour into the realm of steganography gives us the opportunity to try out Shannon's ideas. Once we finish this section, the course will be about a third over and it will be time for the first midterm examination.

The second third of the course starts with an introduction to modern block ciphers in general and the Data Encryption Standard and Advance Encryption Standard in particular. Differential and linear cryptanalysis attacks against block ciphers are investigated. We spend several more weeks studying hash families and Message Authentication Codes. For many applications, including authentication, integrity, nonrepudiation and access control, it is not necessary for encrypted text to be recoverable. In other words, sometimes cryptographic system can be one-way. Our discussion of hash function is followed by an introduction to public key cryptology. By this time, two thirds of the course will be over and it will be time for another midterm examination.

The final third of the course refocuses on practical issues. How do computer scientists use cryptography to design and implement secure systems? It is not easy to get it right. The course examines several security applications that claim they do. These include Kerberos, X.509 authentication service, and PGP. We close with a discussion of alternative cryptosystems and current research.

Prerequisites

The prerequisite for this course is CS231 or by permission of the instructor. If you have any questions about your preparedness for this course, please do not hesitate to see your instructor.

Textbooks

Required and relatively inexpensive is a short introduction to the art and science of secret communications by Simon Singh entitled *The Code Book: The Science of Secrecy from Ancient Egypt to Quantum Cryptography*. It is an entertaining overview of everything that we will be covering this semester. Singh discusses a number of topics that will not explicitly be covered in lecture. Several of these topics, for example, statistical attacks on simple monoalphabetic substitution ciphers, will be required for homework assignments.

Although the title of Douglas R. Stinson's introductory text is *Cryptography: Theory and Practice*, the text is more theory than practice. It is not required, but very highly recommended. We will cover approximately the first two-thirds of the text. Several copies of the Stinson text are on reserve in the library. Both Singh and Stinson texts are available in the Wellesley College Bookstore.

The remainder of the course will be taught from a number of different sources all of which will be placed on reserve in the Science Center Library.

Additional Resources

The following books, in addition to those listed above, were used during the preparation of this course. Most are on reserve in the library.

F.L. Bauer, *Decrypted Secrets: Methods and Maxims of Cryptology*, Springer (3rd Edition), 2001.

Simson Garfinkel, *Database Nation: The Death of Privacy in the 21st Century*, O'Reilly and Associates, 2001.

David Kahn, *The Codebreakers: The Story of Secret Writing*, Scribner, 1996.

Stefan Katzenbeisser and Fabien A. P. Petitcolas, Editors, *Information Hiding: Techniques for Steganography and Digital Watermarking*, Artech House, 2000.

Charlie Kaufman, Radia Perlman, Mike Speciner, *Network Security: Private Communication in a Public World*, Prentice Hall, 2002

Bruce Schneier, *Secrets and Lies: Digital Security in a Networked World*, John Wiley and Sons, 2000.

Bruce Schneier, *Applied Cryptography: Protocols, Algorithms, and Source Code in C (2nd Edition)* John Wiley and Sons, 1995.

William Stallings, *Cryptography and Network Security: Principles and Practice (3rd edition)*, Prentice-Hall, 2003

Peter Wayner, Disappearing Cryptography - Information Hiding: Steganography and Watermarking (Second Edition), Morgan Kaufmann, 2002.

Course Requirements

Problem sets: During the term, there will be regular homework assignments.

Midterm Examinations: There will be two midterm examinations. The first will be on Monday, March 8 and the second will be on Thursday, April 15. Please note these dates in your calendar. There will be no extensions without prior arrangement with the instructor.

Final Examination: There will be a comprehensive final examination at the end of the semester.

All examinations are in class and are open book, open notes.

Class participation. Reading assignments will be made during each class session. You should come to the next class prepared to ask questions about and/or discuss the reading assigned during the previous session. Not everyone is equally comfortable speaking in class. You may fulfill the participation requirement by doing a subset of the extra readings and problems that will be made available during the semester.

Assignment Policy

All assignments are due in class/laboratory on the due date announced when the assignments are distributed. Once graded homework is returned (usually on the class following the day the assignment was due), no further late work for that assignment will be accepted.

Collaboration Policy

I encourage you to talk with other students about the course and to form study groups. Unless otherwise instructed, feel free to discuss problem sets with other students and exchange ideas about how to solve them. However, I require that *you must compose your own solution to each assignment*. In particular, while you may discuss problems with your classmates, you must always write up your own solutions from scratch.

Please acknowledge and collaborative work. If you make use of an idea that was developed by (or jointly with) others, please reference them appropriately in your work.

When working on homework problems, it is perfectly reasonable to consult public literature (books, articles, etc.) for hints, techniques, and even solutions. However, you must reference any sources that contribute to your solution.

Grading Policy

The final grade will be computed as a weighted average of each of the following requirements described above. The relative weight of each component is:

Participation	05%
Homework Assignments	20%
Midterm Examination 1	20%
Midterm Examination 2	25%
<u>Final Examination</u>	<u>30%</u>
Total	100%