Course Information

Cryptography and Data Security

`http://ece.wpi.edu/~christof/578`

Goals and Prerequisites

The course gives a comprehensive introduction into the field of cryptology. We will cover the theoretical aspects as well as practical ones. The mathematical background will be developed throughout the course as needed. The specific learning goals of the course are:

- Broad overview over the field of cryptography.
- Understanding of the theory of the most important private and public key schemes.
- Learning about current security estimations of important algorithms.
- Capability to design a crypto protocol for a given application and assess its security.
- Learning about soft and hardware implementation issues and the trade-offs involved.

There are no formal prerequisites, except that students are expected to have a working knowledge of the C programming language. C will be needed for some of the homework assignments. If you do not have the background, please consult immediately with me.

Communication with the Instructor

I can be reached as follows:

Prof. Christof Paar
Electrical and Computer Engineering Department
Worcester Polytechnic Institute
Atwater Kent 102
phone: (508) 831–5061
fax: (508) 831–5491
email: christof@ece.wpi.edu
web: http://ece.wpi.edu/People/faculty/cxp.html

A very good communication vehicle is email. It is a good idea to pose any course related questions by using email. You can also arrange special meetings before/after the course through email.

Grading

The grading is slightly different for graduate and undergraduate students:

graduate students	*undergraduate students*
Homework (10 %)	Homework (20 %)
Project (25 %)	Project (25 %)
Midterm Exam (25 %)	Midterm Exam (20 %)
Final Exam (40 %)	Final Exam (35 %)

Textbook

D.R. Stinson, Cryptography: Theory and Practice. CRC Press, 1995.

Note: During the Fall 2000 semester, this book and the other ones recommended below are put on reserve in Gordon Library — You can use them in the library and make copies but you can't take them out. You have to ask for the books at the reference desk.

Homework

Homework assignments are due Wednesdays after the class. They will be graded and returned the following Wednesday. All assignments are posted on the course web page. Some homework assignment will involve programming tasks. For some of those problems programs or source code will be provided on the web pages.

You can work together on the problems. However, every student has to hand in her/his solutions. Also, you **must clearly state with whom you participated**.

The TA for the course is Adam Woodbury, email adw@ece.wpi.edu.

Project

An important part of this course is a term project. You will have a relatively large amount of freedom with respect to selecting your project topic. Possible areas are software implementations of (full-size) crypto algorithms, protocols, or attacks treated in the lecture; study of schemes not treated in the lecture; research/literature study on selected advanced topics; standards; network security; etc.

On October 11 (that is the 6th lecture week), you should submit a one page project proposal. You are welcome to discuss possible topics with me before handing it in. The proposal will briefly be discussed. The project should then be conducted throughout the second half of the semester. Group projects are possible. However, on reports of group projects it must be **clearly marked which student is responsible for which part of the project** in order to allow a fair grading. More information about the project is on the course web page.

Additional Sources of Information on Cryptography

Further Reading

The following books are excellent supplements to our textbook. During the Fall 2000 semester, these books are put on reserve in Gordon Library.

[1] *A. Menezes, P. van Oorschot, S. Vanstone, Handbook of Applied Cryptography. CRC Press, October 1996.* Great compilation of theoretical and implementational aspects of many crypto schemes. Unique since it includes many theoretical topics that are hard to find otherwise. Highly recommended.

[2] *B. Schneier, Applied Cryptography. 2nd ed., Wiley, 1995.* Very accessible treatment of protocols and algorithms. Gives also a very nice introduction to cryptography as a discipline.

[3] *W. Stallings, Cryptography and Network Security. Prentice Hall.* Very accessible textbook on cryptography. Well suited for undergraduates. It also has a good introduction to IPsec and SSL.

[4] *D. Kahn, The Codebreakers: The Comprehensive History of Secret Communication from Ancient Times to the Internet. 2nd edition, Scribner, 1996.* Entertaining 1200 pages on the history of cryptography. Despite a recent update, strong emphasis on material from the pre-public-key area.

Online Information

There is a wealth of web pages with collections of crypto-related links. Here is one to start with (from Ron Rivest, the “R” in RSA):

`http://theory.lcs.mit.edu/~rivest/crypto-security.html`

There are also two relevant Internet newsgroups, `sci.crypt` and `sci.crypt.research`. The former one is unmoderated and gets lots of postings every day, the latter one is moderated, more theoretical, and with far fewer postings, perhaps a few per week.

Research Literature

The most important conferences are CRYPTO, annually held in Santa Barbara and EUROCRYPT, annually held in Europe. A great deal of the new results in theoretical cryptology is published at these two conferences. Other important conferences include ASIACRYPT (in Asia and Australia), the Fast Software Encryption Workshop (FSE), and the Workshop on Selected Areas in Cryptography (SAC) in Canada. In August 1999, the first Workshop on Cryptographic Hardware and Embedded Systems (CHES) was held at WPI. Proceedings of all of these conference are published in Springer-Verlag’s “Lecture Notes in Computer Science” series.

This year, a CD has become available from Springer-Verlag which contains almost all CRYPTO and EUROCRYPT proceedings at a reasonable price (around $100).