Cryptography, Fall 2011

EECE 405/560: UU111, MWF 3:30-4:30 PM

- Syllabus
- Assignments
- Etc

Syllabus

Cryptology -- Fall 2011 Syllabus

Textbook: Introduction to Cryptography with Coding Theory by Wade Trappe and Lawrence C. Washington. This is an excellent textbook that closely follows the material presented in this class.

Other books: here are some books I recommend for further reading.

- Cryptography: Theory and Practice by Douglas Stinson.
- Security Engineering, by Ross Anderson (Wiley, 2001.) This is a very informative book about security in practice, from community swimming pool passes to nuclear command and control.
- The Handbook of Applied Cryptography, by Alfred J. Menezes, Paul C. Van Oorschot, and Scott A. Vanstone. All chapters of this book are available for free online.
- Applied Cryptography: Protocols, Algorithms, and Source Code in C, by Bruce Schneier (Wiley, 1995.) This is a standard reference book for people who want to implement security systems. Its several chapters on cryptographic protocols are very useful.
- Public-Key Cryptography, by Arto Salomaa (Springer-Verlag Text in Theoretical Computer Science, 1996.) Salomaa's book is a great reference for public-key systems. I would have used it as a textbook if only it was more diverse. For some strange reason, all of his plaintext examples are essays about saunas; what a sauna is, where to find a sauna, etc.
- A Course in Number Theory and Cryptography, by Neal Koblitz (Springer-Verlag Graduate Texts in Mathematics, 1994.) Koblitz focusses on public-key cryptosystems based on number theory (yes, there are systems that aren't based on number theory.)
- Elements of Information Theory, by Thomas Cover and Joy Thomas (Wiley Interscience, 1991.) Just a fantastic introduction to Information Theory.

Prerequisites: ISE261 or MATH 327, and I will expect you to be able to write a simple computer program (you are a senior or graduate student in electrical engineering.)

The student will be introduced to some higher mathematics, including introductory amounts of number theory, graph theory, computational complexity, and information theory. A sufficient mathematical background to absorb this material is all that is needed. Knowledge of some programming language, however, is a necessity.

Grading: Grades are based on written assignments, a midterm and a final exam. The grade distribution is roughly 30% assignments, 25% midterm, 35% final and 10% class participation.

Written assignments will occasionally require some coding.

Graduate students will be graded on a different scale, and will receive extra homework.

Tentative Schedule

This schedule covers roughly the subject matter that will be presented in class. We could very easily spend more time or less time on certain subjects.

Week 1	Intro to cryptography
Week 2	Probability
Week 3	Classical cryptanalysis
Week 4	More cryptanalysis
Week 5	The Enigma Machine and modern ciphers
Week 6	Information Theory
Week 7	Information Theory
Week 8	Information Theory
Week 9	Review and Midterm
Week 10	Number Theory
Week 11	RSA and Diffie Hellmann
Week 12	Cryptographic Protocols
Week 13	Cryptographic Protocols
Week 14	Cryptographic Protocols
Week 15	Steganography
Week 16	Security engineering

- ## Links
  - Binghamton University
  - Textbook
- ## Other stuff
  - Bruce Schneier on security
  - Ed Felten's technology policy blog

Created in VI

This course is also offered under the articulation agreement between Binghamton University and SUNYIT. It is available to qualified students at Binghamton University via the distance learning system Enginet.