

Course Description Math 133. The Art and Science of Secret Writing. This freshman seminar will study the mathematics of encryption, a science known as cryptology. Considerable attention will be given to the military and social history of cryptology and the public-policy questions raised by its increasing use in conjunction with the Internet. However, the focus will be on the use of mathematics to create and analyze encryption algorithms, so the student will need the equivalent of four years of high school mathematics. A variety of practical exercises will require the use of specialized software and email programs, so the student should be willing to use unpolished programs on the Windows platform.

Aims Students in this course will make a sustained, focused and in-depth exploration of cryptology — its history, its practice and its future. They will gain an appreciation of the exacting nature of mathematics; the power of mathematics, especially when combined with advances in computing power; and they will wrestle with the larger societal questions wrought by advances in technology. The seminar format will allow for customized assignments and spirited discussions. Substantive written work in mathematics and in position papers will develop and demonstrate their intellectual independence.

Beyond the general purposes of freshman seminars, this course will have several more specific goals.

To introduce the student to the power of discrete mathematics and to become comfortable with learning new modes of mathematical thought.

To become familiar with the two-thousand year history of cryptology, and to therefore more fully appreciate the revolutionary nature of the debut of public-key cryptography in the 1970's.

To consider critically the societal implications created by recent advances in this field.

To become a more informed consumer of encryption technologies, and a more savvy user of electronic communications.

Prerequisites This mathematics employed in this course is accessible to any student with four years of high school mathematics. Practicums will use software written for the Windows platform, so students should be comfortable using unpolished programs with this operating system. In cases where programs interoperate, other platforms (Mac, Linux) are acceptable.

Texts Six books will be required reading. The first is *The Code Book*, by Simon Singh. This is written for a general audience and describes the major events in the history of cryptology, along with very readable accounts of the underlying technical aspects of these events. It begins with Mary Queen of Scots' trial for treason on October 15, 1586 and

concludes with a presentation on quantum cryptography. Along the way are discussions of historical ciphers, the German Enigma machine in World War II, the US Federal Data Encryption Standard (DES), public-key cryptography, and Pretty Good Privacy (PGP). This book is one of the best popular accounts I have ever read dealing with mathematics and computer science, since the examples are both non-trivial and accurate, yet are written so that they are understandable by an educated nonspecialist.

Invitation to Cryptology, by Thomas H. Barr, is a textbook of cryptology, written for the “beginning” mathematics student. More accurately, the preface says:

This book is directed toward those whose mathematical background includes college-preparatory courses such as high school algebra and geometry. In earlier drafts, I have used it as the basis for a course [at Rhodes College] for which there were no formal mathematical prerequisites at the college level. Students majoring in areas from Art History to Zoology took the course. Many had not taken mathematics in four or five years.

Cryptonomicon, by Neal Stephenson, is an historical, and futuristic, novel that features encryption and networks prominently. *Codes and Ciphers*, by Mark Fowler, is really a children’s puzzle book, but the puzzles are based on classical codes and ciphers and solving them will be a good (and fun) way to understand those codes and ciphers.

Crypto, by Steven Levy, is a fascinating account of the origins of modern cryptography. Bruce Schneier’s *Secrets and Lies* is an excellent discussion of how cryptography fits into the wider arena of computer security and should be required reading for any modern professional who uses computers in their work or business.

Course Outline

Unit 1 History, Classical Ciphers

Singh, *The Code Book*

Chapter 1 The Cipher of Mary Queen of Scots

Chapter 2 Le Chiffre Indéchiffrable

Chapter 3 The Mechanisation of Secrecy

Chapter 4 Cracking the Enigma

Chapter 5 The Language Barrier

Barr, *Invitation to Cryptology*

Chapter 1 Origins, Examples, and Ideas in Cryptology.

A Crypto-Chronology. Functions. Crypto: Models, Maxims, and Mystique.

Chapter 2 Classical Cryptographic Techniques.

Shift Ciphers and Modular Arithmetic. Affine Ciphers; More Modular Arithmetic. Substitution Ciphers. Transposition Ciphers. Polyalphabetic Substitutions. Probability and Expectation. The Friedman and Kasiski Tests. Cryptanalysis of the Vigenere Cipher. The Hill Cipher; Matrices.

Unit 2 Revolution, Modern Ciphers

Barr, *Invitation to Cryptology*

Chapter 3 Symmetric Computer-Based Cryptology.

Number Representation. Computational Complexity. Stream Ciphers and Feedback Shift Registers. Block Ciphers. Hash Functions.

Chapter 4 Public-Key Cryptography.

Primes, Factorization, and the Euclidean Algorithm. The Merkle-Hellman Knapsack. A Little Number Theory: Fermat's Little Theorem. The RSA Public-Key Cryptosystem. Key Agreement and the ElGamal Cryptosystem. Digital Signatures. Zero-Knowledge Identification Protocols.

Singh, *The Code Book*

Chapter 6 Alice and Bob Go Public

Chapter 7 Pretty Good Privacy

Unit 3 The Future, Public Policy, Computer Security

Singh, *The Code Book*

Chapter 8 A Quantum Leap into the Future

Barr, *Invitation to Cryptology*

Chapter 5 Present Practice, Issues, and the Future.

A Cryptographic Standard: DES. Electronic Mail Security. Public Key Infrastructure. Policy, Privacy, and International Issues.

Levy, *Crypto*

Schneier, *Secrets and Lies*

Practicums This course will include a variety of practical examples for the students to work themselves. Some aspects of cryptography sound simple when explained, but seem harder when performed, while other aspects never seem very clear until practiced.

Steganography Hide an encrypted message in an image, using a software tool designed for this purpose.

Monoalphabetic Ciphers Decode a classic text that is encrypted using a monoalphabetic cipher, using software tools to make the task more manageable.

Solitaire Practice the Solitaire (Pontifex) algorithm, as described in the novel *Cryptonomicon*.

Simplified DES Encode and decode messages by hand using an educational version of the Data Encryption Standard (DES). Participate in a mock distributed brute-force attack.

Pretty Good Privacy Become proficient in using the encryption program Pretty Good Privacy (PGP) for public-key encryption and digital signatures. Understand the basics of key management. There will be three practicums using this protocol.

Digital Time Stamping Learn to use Stamper to digitally time-stamp a message.

Anonymous Remailers Learn to frustrate traffic analysis by using anonymous remailers and mixmasters to camouflage message traffic.

Evaluation Student achievement and progress will be evaluated by a variety of instruments. Practicums will be graded on a pass/fail basis. There will be four in-class exams where students will write to display their understanding of the readings, and the mathematics and protocols of encryption. Some questions will be computational, some will be short answer or essay questions.

The final material on social and public policy material will require students to craft a research paper on a topic of their choosing, which at that point they could study with the requisite technical understandings. These papers will be the basis for in-class presentations, which will lend themselves to further debates among the students.

Bibliography

The vast majority of the books listed in the following annotated bibliography are available in the UPS Library.

History

1. Alvarez, David J. *Secret messages : codebreaking and American diplomacy, 1930-1945*. Lawrence, KS, University Press of Kansas. 2000. A good history, especially for its coverage of the pre-WWII time period.
2. Benson, Robert Louis and Michael Warner, Eds. *Venona: Soviet espionage and the American response, 1939-1957*. Washington, D.C., National Security Agency, Central Intelligence Agency. 1996. Cold War era cryptanalysis.
3. Calvocoressi, Peter. *Top secret ultra*. New York, Pantheon Books. 1980. A memoir of WWII-era cryptanalysis in Europe.
4. Clark, Ronald William. *The man who broke Purple : the life of Colonel William F. Friedman, who deciphered the Japanese code in World War II*. Boston, Little, Brown. 1977.
5. Farago, Ladislas. *The broken seal; the story of Operation Magic and the Pearl Harbor disaster*. New York, Random House. 1967. WWII-era cryptanalysis in the Pacific.
6. Garlinski, Jozef. *The Enigma war*. New York, Scribner. 1980. WWII-era cryptanalysis in Europe.
7. Hinsley, F.H. and Alan Stripp, eds. *Codebreakers : the inside story of Bletchley Park*. Oxford, New York, Oxford University Press. 1993. The history of Bletchley Park, where English and American codebreakers helped win WWII.
8. Kahn, David. *The codebreakers; the story of secret writing*. London, Weidenfeld and Nicolson. 1967. The most comprehensive history of cryptology, though insufficient for modern topics.
9. Kozaczuk, Wadysaw. *Enigma : how the German machine cipher was broken, and how it was read by the Allies in World War Two*. Frederick, Md., University Publications of America. 1984. An account of the Polish efforts to break Enigma, which laid the groundwork for Bletchley Park to eventually succeed.
10. Kippenhahn, Rudolf. *Code breaking : a history and exploration*. Woodstock, N.Y., Overlook Press. 1999. The runner-up (to Singh's *The Code Book*) as best choice for a history that also contains some simplified technical explanations.

11. Singh, Simon. *The code book : the evolution of secrecy from Mary Queen of Scots to quantum cryptography*. New York, Doubleday. 1999. A well-written popular account of the history of cryptology, with excellent technical descriptions.
12. Thompson, James Westfall. *Secret diplomacy; espionage and cryptography, 1500-1815*. New York, F. Ungar Pub. Co. 1963. A good account of classical cryptology in Europe.
13. United States Army Air Forces. *ULTRA and the history of the United States Strategic Air Force in Europe vs. the German Air Force*. Frederick, MD, University Publications of America. 1980. An official report on WWII-era cryptanalysis in Europe.
14. Van Der Rhoer, Edward. *Deadly magic : a personal account of communications intelligence in World War II in the Pacific*. New York, Scribner. 1978. WWII-era cryptanalysis in the Pacific.
15. Winterbotham, F. W. *The Ultra secret*. New York, Harper & Row. 1974. WWII-era cryptanalysis in Europe.
16. Yardley, Herbert O. *The American Black Chamber*. Indianapolis, Bobbs-Merrill. 1931. A classic. Yardley was the first cryptologist officially in the employ of the United States.

Texts — Elementary

1. Barr, Thomas H. *Invitation to Cryptology*. Upper Saddle River, NJ, Prentice Hall. 2002. Best choice for a textbook to use at the freshman level for students with normal high school preparation in mathematics.
2. Beutelspacher, Albrecht. *Cryptology*. Washington, DC, Mathematical Association of America. 1994. An entertaining elementary treatment.
3. Klugerman, Ira H. and Dan Rose. *Cracking the code*. Lexington, Mass., COMAP. 1993. Instructional videotape.
4. Davis, Donald M. *The nature and power of mathematics*. Princeton, N.J., Princeton University Press. 1993. Contains a short, elementary section on cryptology.
5. Garfinkel, Simson *PGP: pretty good privacy*. Sebastopol, CA, O'Reilly & Associates. 1995. How-to book on how to use the most popular personal encryption software available.
6. Lewand, Robert. *Cryptological mathematics*. Washington, DC, Mathematical Society of America. 2000. Written for an audience of high school students, this might be the runner-up for the mathematical text for this course.
7. Sinkov, Abraham. *Elementary cryptanalysis : a mathematical approach*. Washington, D.C., Mathematical Association of America. 1980. High-school level, classical techniques only.

8. Smith, Laurence Dwight. *Cryptography, the science of secret writing*. New York, W. W. Norton. 1943. Dated. Only covers techniques for classical methods.

Texts — Advanced

1. Bauer, Friedrich Ludwig. *Decrypted secrets: methods and maxims of cryptology* New York, Springer. 2000. An advanced textbook.
2. Biham, Eli. *Differential cryptanalysis of the data encryption standard*. New York, Springer-Verlag. 1993. Detailed mathematical treatment of the first successful application of differential cryptanalysis.
3. Bouwmeester, Dirk and Artur Ekert and Anton Zeilinger, Eds. *The physics of quantum information : quantum cryptography, quantum teleportation, quantum computation*. New York, Springer. 2000. Good account of possibilities for quantum computing in cryptographic applications.
4. Brassard, Gilles. *Modern cryptology: a tutorial*. New York, Springer-Verlag. 1988. Very short, very advanced.
5. Electronic Frontier Foundation. *Cracking DES : secrets of encryption research, wiretap politics & chip design*. Sebastopol, CA, O'Reilly & Associates, Inc. 1998. Fantastic break of DES with cheap hardware, with this report prepared for distribution simultaneous with the announcement of the break.
6. Friedman, William F. *The Riverbank publications*. Laguna Hills, Calif., Aegean Park Press. 1979. A bit odd, but written by one of the key figures in the history of American cryptanalysis.
7. Garrett, Paul. *Making, breaking codes: an introduction to cryptography* Upper Saddle River, NJ, Prentice Hall. 2001. An upper-division textbook.
8. Koblitz, Neal. *Algebraic aspects of cryptography*. New York, Springer. 1998. Beginning graduate level text.
9. Koblitz, Neal. *A course in number theory and cryptography*. New York, Springer-Verlag. 1994. An advanced textbook, with heavy doses of number theory.
10. Kullback, Solomon. *Statistical methods in cryptanalysis*. Laguna Hills, Calif., Aegean Park Press. 1976. Serious applications of statistics in the service of cryptanalysis.
11. Menezes, A. J. and Paul van Oorschot and Scott Vanstone. *Handbook of applied cryptography*. Boca Raton, FL, CRC Press. 1997. Reference work of choice for professionals.

12. Patterson, Wayne, 1945- *Mathematical cryptology for computer scientists and mathematicians*. Totowa, N.J., Rowman & Littlefield. 1987. A very nice upper-division text, but quickly becoming outdated.
13. Schneier, Bruce. *Applied cryptography : protocols, algorithms, and source code in C*. New York, Wiley. 1996. The most popular technical reference on the topic. Includes mathematics, algorithms and protocols.
14. Stallings, William. *Cryptography and network security: principles and practice*. Upper Saddle River, N.J., Prentice Hall. 1999. Very good textbook for an upper-division audience.
15. Stinson, Douglas R. *Cryptography: theory and practice*. Boca Raton, CRC Press. 1995. A good choice for an upper-division text.
16. Williams, Colin P. *Explorations in quantum computing*. Santa Clara, Calif., TELOS. 1998.

Public Policy

1. Agre, Philip E. and Marc Rotenberg, Eds. *Technology and privacy: the new landscape*. Cambridge, Mass., MIT Press. 1997. Essays from a variety of perspectives about privacy with regard to technological changes (such as progress in cryptology).
2. Bamford, James. *The puzzle palace : a report on America's most secret agency*. Boston, Houghton Mifflin. 1982. A classic history of the National Security Agency.
3. Bamford, James. *Body of secrets: anatomy of the ultra-secret National Security Agency*. New York, Doubleday. 2001. An updated critique of the National Security Agency.
4. Dam, Kenneth W. and Herbert S. Lin, eds. *Cryptography's role in securing the information society*. Washington, DC, National Academy Press. 1996. A report of the National Research Council's Computer Science and Telecommunications Board's Committee to Study National Cryptography Policy.
5. Diffie, Whitfield and Susan Landau. *Privacy on the line: the politics of wiretapping and encryption*. Boston, MIT Press. 1998. Public policy, as viewed by one of the pioneers of public-key cryptography (Diffie), and one of today's leading industrial cryptologists (Landau).
6. Hoffman, Lance J., ed. *Building in big brother: the cryptographic policy debate*. New York, Springer-Verlag. 1995. Fifty-four essays on a variety of topics. An excellent source of a wide range of opinions, though some of it is now out of date.

Cryptologic Puzzle Books

1. Fowler, Mark and Sarah Dixon and Radhi Parekh. *The Usborne Book of Superpuzzles* Usborne Publishing Limited, London. 1994. A collection containing *Codes and Ciphers* by Mark Fowler, with numerous puzzles based on historical codes and ciphers.

Miscellaneous

1. Budd, Louis J. and Edwin H. Cady, Eds. *On Poe*. Durham, Duke University Press. 1993. Essay on pages 40-54 by Friedman details Poe as a cryptologist.
2. Friedman, William F. *The Shakespearean ciphers examined*. Cambridge, Cambridge University Press. 1957. A hobby of one of the key figures in the history of American cryptanalysis.
3. Harris, Robert *Enigma* Ivy Books. 1996. A novel set at Bletchly Park in 1943.
4. Stephenson, Neal. *Cryptonomicon*. New York, Avon Press. 1999. A novel whose settings alternate between WWII cryptography and modern-day Internet cryptography. Includes the Solitaire algorithm, which uses a deck of playing cards for its keystream.