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 the convergence of strong encryption, cheap computers and ubiquitous computers.

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 a variety of software, so students should be willing to learn new tools and techniques.

Texts  Five 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.

*Mathematics and Cryptography*, by Robert A. Beezer, is a collection of notes about the relevant mathematics needed to understand classical cryptography and the basics of modern cryptography.

*Cryptonomicon*, by Neal Stephenson, is an historical, and futuristic, novel that features encryption and networks prominently. I will provide notes to accompany your reading of this novel.

_Crypto_, by Steven Levy, is a fascinating account of the origins of modern cryptography. James Bamford’s *Shadow Factory* is an excellent discussion of recent events involving the US National Security Agency.

**Course Outline**

**Unit 1  History, Classical Cryptography**

_**Singh, The Code Book**_

**Chapter 1** The Cipher of Mary Queen of Scots  
**Chapter 2** Le Chiffre Indechiffreable  
**Chapter 3** The Mechanisation of Secrecy  
**Chapter 4** Cracking the Enigma  
**Chapter 5** The Language Barrier

_**Beezer, Mathematics and Cryptography**_

**Chapter MA** Modular Arithmetic  
**Chapter B** Bases  
**Chapter BA** Binary Arithmetic  
**Chapter SS** Sharing a Secret

**Unit 2  Revolution, Modern Ciphers**

_**Beezer, Mathematics and Cryptography**_

**Chapter DHKE** Diffie-Hellman Key Exchange  
**Chapter DL** Discrete Logarithms  
**Chapter DHKS** Diffie-Hellman Knapsack Encryption  
**Chapter NT** Number Theory  
**Chapter RSA** RSA (Rivest-Shamir-Adelman) Cryptography

_**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  
_**Levy, Crypto**_

_**Bamford, Shadow Factory**_
Practicums  This course will include a variety of practical examples for 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.

EM Email  Set up addresses for electronic communication. Experiment with HushMail’s encrypted email.

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

MONO Monoalphabetic Substitution Cipher  Decode a classic text that is encrypted using a classical monoalphabetic substitution cipher, using software tools to make the task more manageable.

VIG Vigenère Cipher  Decode a classic text that is encrypted using a classical Vigenère cipher, using software tools to make the task more manageable.

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

SDES 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.

PGP1-3 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. Three separate practicums (key generation, encryption, digital signatures).

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

ANON Anonymous Remailers  Learn to frustrate traffic analysis by using anonymous remailers and mixmasters to camouflague 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 two 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 can 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


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.


**Texts — Elementary**


17. Wayner, Peter. *Disappearing Cryptography.* Morgan Kaufmann. 2002. How-to on steganography, watermarking, mimicry, etc.


**Public 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).


Cryptologic Puzzle Books


Miscellaneous


