

Course description: Modern cryptography (making secret codes) and cryptanalysis (breaking secret codes) make use of number theory and the structure of finite fields. For example, the security of RSA (the public key cryptosystem at the heart of electronic credit card payment systems) relies on the difficulty of factoring a product of two large carefully chosen prime numbers. After learning the RSA encryption and decryption algorithms, we examine an attack on the cryptosystem known as quadratic sieve. We then explore the Advanced Encryption Standard (a private key cryptosystem approved by NIST). Our study of both RSA and AES is informed by theory and computation. The only prerequisite for the course is Math 333, the first semester of abstract algebra.

Resources: The required text is the second edition of *A Course in Number Theory and Cryptography* by Neal Koblitz. A reference for AES is *The Design of Rijndael* by Joan Daemen and Vincent Rijmen. We will use the software *Mathematica*, which may be downloaded for campus use from <http://www2.haverford.edu/acc/software/index.html#academic>.

Weekly assignments: Weekly assignments will be posted by Monday on Blackboard (see www2.haverford.edu/acc/docs/network/blackboard/studentbasic/studentbbbasic.htm), and are due the following Monday at 3 pm under the door of Hilles 212. No late papers are accepted. Solutions will be posted on Blackboard.

You are encouraged to discuss your ideas on homework problems with peers and instructors, but you are not permitted to refer to any notes from such discussions while preparing the solutions you plan to submit for grading. Divide the time you spend solving a homework problem into 3 stages: first work alone and record your preliminary ideas on white paper; then work with peers and instructors and record shared ideas on colored paper; finally resume working alone on white paper without looking at anything written on colored paper. So, if you wish to write something down while reading a solution in the text by Neal Koblitz, you must write on colored paper since you are consulting with him.

The problems sets are meant to be challenging; you should plan to spend six hours on each assignment. If you find yourself spending more than six hours, please ask for assistance. You should also spend an hour each weekend reading required texts to prepare for the next week's lectures and reading solutions to the previous week's assignment.

Tests and Grades: The midterm will be on the number theory (I.1, I.2 and I.3) and group theory used to understand the algorithms used to encipher plaintext and decipher ciphertext in the RSA cryptosystem (IV.2), the theory of finite fields (II.1) used to understand primality tests for key generation in RSA (V.1 and V.2), and how factor bases are used in attacks on RSA (V.3, V.4 and V.5). It will be given in two parts, in class on March 5 and 7. The self-scheduled final will be on sieving methods used to factor RSA keys, Markov models used in language modeling, and the algorithm used to reestimate parameters in a Hidden Markov Model. Grades will be determined by performance on assignments (20%), the midterm (40%), and the final (40%).

Class meetings and office hours: Class meetings are MWF 10:35–11:30 am in Koshland E309. **Lynne Butler** will be available MF 2:05–3 pm in her office (Hilles 212). To schedule an alternative meeting, contact Lynne by email (lbutler@haverford.edu), at her home (609-818-9540), or in her office (610-896-1300).

Jan 21	Jan 23 RSA public key cryptography	Jan 25 Modular exponentiation by repeated squaring
Jan 28 The Euclidean algorithm is polynomial time	Jan 30 The Chinese Remainder Theorem	Feb 1 RSA key generation
Feb 4 Primality testing	Feb 6 Fermat Factorization	Feb 8 Newton's Method
Feb 11 The Miller-Rabin primality test	Feb 13 Pollard's $p - 1$ test	Feb 15 Weak RSA keys
Feb 18 Pollard's rho test	Feb 20 Timing Pollard's rho	Feb 22 Factor Bases
Feb 25 Continued Fraction Factorization	Feb 27 Quadratic Reciprocity	Feb 29 Square roots mod p
Mar 3 How Quadratic Sieve factors an RSA key	Mar 5 Midterm: Part I	Mar 7 Midterm: Part II
Mar 17 Sieving in Quadratic Sieve	Mar 19 The matrix step in Quadratic Sieve	Mar 21 Comparison of CFF, QS and NFS
Mar 24 Finite Fields	Mar 26 Advanced Encryption Standard	Mar 28 Proof of Quadratic Reciprocity
Mar 31 Language models in cryptography	Apr 2 Markov models	Apr 4 Scoring rates
Apr 7 Hidden Markov Models	Apr 9 The Baum-Welch reestimation algorithm	Apr 11 An application of HMMs to finance
Apr 14 Diffie-Helman key exchange	Apr 16 The discrete log problem	Apr 18 Quantum computing
Apr 21 Complex n -space	Apr 23 Discrete Fourier Transform	Apr 25 Application of DFT to factoring
Apr 28 Designing an attack	Apr 30 Implementing an attack	May 2 Evaluating an attack