

# Mathematics 103

## Honors Section (H1)

Fall 2006

[Prof. Stephen Miller](#)

### Topics in Mathematics for Liberal Arts: Cryptography and Voting Machines

Meets TF3 at 11:30A-12:50 in [Scott Hall](#) room 219, on the [College Avenue Campus](#)

Currently many states are considering proposals to replace old-fashioned ballot boxes and punchcards with computer kiosks. This poses both an opportunity to enhance democracy (by reducing counting errors and other human error), yet at the same time a very dangerous possibility of fraud if the machines are poorly designed. Our democracy crucially depends on uncorruptible machines, so this is a serious matter. Mathematics has a surprising amount to say about this, as well as other important topics in information security. The connection will be the main theme of the course.

#### Course Requirements and Grading Guidelines:

The grade will be based homework assignments, a short paper assignment, and quizzes (together 30%), two midterms (each 20%), and a final exam or project (30%). The midterms will be held in class on Tuesday October 17th and Tuesday November 28th.

#### Syllabus:

##### Part A: Historical Principles of Cryptography

1. Brief history of cryptography
2. Caesar cipher
3. Vigenere cipher
4. Language attacks

##### Part B: Some Important Modern Questions

1. Can mathematics guarantee secure conversations despite eavesdroppers?
2. Why is it safe to use an ATM machine in the USA? What about Europe?
3. Is it safe to use your credit card online?
4. Are Diebold's voting machines as secure as they claim, or insecure as many academic experts insist. Can an election be stolen by hackers?

5. Besides cryptography, what else does internet security require?

Part C: Mathematical aspects of modern cryptosystems

1. Diffie-Hellman key exchange and discrete logarithms
2. RSA cryptosystem
3. Hash functions and their security

**Course Materials/Links:**

- Rivest [article](#) on voting machines.
- Professor Greenfield's 1999-2000 [course](#).
- External [site about e-voting](#), with information about the Maryland case.
- [Article](#) in Discover Magazine about e-voting.
- RSA Security's excellent [Crypto FAQ](#).
- Ron Rivest's [Cryptography and Security](#) page.
- Microsoft Research [Cryptography and Anti-Piracy homepage](#).