MATH 404, Discrete Math and Cryptography
Fall 2005

Instructor Info

Instructor:	Ismar Volic
Meeting times:	Mondays and Wednesdays 5:00 – 6:15, in CLK 102
Office hours:	Mondays 3-4, Tuesdays 1-2, and by appointment, in Kerchof 327
Phone:	924-4948
Email:	ismar@virginia.edu

Textbook and Webpage

Text: *Discrete Mathematics and Its Applications*, by K. Rosen, 5th edition, McGraw-Hill, 2003.

This is our main, required textbook.

A Friendly Introduction to Number Theory, by Joseph Silverman, 2nd edition, Prentice Hall, 2001.

This book is not required. I will copy and upload relevant sections to Toolkit (see webpage below) so you can access them there.

Webpage: https://toolkit.itc.virginia.edu:443/cgi-local/tk/UVa_CLAS_2005_Fall_MATH404-1

Please check this page often. It will contain various important announcements and information about the course. You can also join discussion groups, provide feedback about the course, etc.

Other Resources

- http://www.mhhe.com/math/advmath/rosen/r5/

This is the companion website to the textbook. It contains a number of helpful resources, including extra examples, elaborations on textbook's explanations, online tutorials, self-assessment tools, links to many other discrete math sites, etc.

- *Shaum's Outline of Discrete Mathematics*, by S. Lipschutz and L. Lipson, McGraw-Hill.

Contains lots of worked examples.

- *Discrete Mathematics*, by R. Johnsonbaugh, Prentice Hall.

A good textbook, with different takes on some of the topics we'll be covering.

- *The Code Book*, by S. Singh, Anchor Books.

A fun read on the history of cryptography.

- *Elementary Number Theory*, by K. Rosen, Addison-Wesley.

Has a good chapter on basic cryptography.

Prerequisites and Policies

Prerequisites: One semester of calculus. Some familiarity with linear algebra and group theory is desired but not necessary.

Attendance: It is not required that you come to class, although it is doubtful that you will do well in the course if you miss too many lectures. If you do decide to attend, *please be on time*.

Makeup exams: Makeup exams will not be given except in emergencies. If you miss an exam, we will arrange a makeup only if you are able to present a note from a doctor or a school official stating that you were not able to take the exam at the scheduled time.

Warning: *This is not a cryptography course!* It is first and foremost a demanding discrete math course intended for advanced undergraduates. I plan to spend at most 3—4 weeks on cryptography.

Course Outline

Here is a tentative list of topics we will cover:

Discrete Math:

1.1—1.8	Basic logic, methods of proof, sets, functions;
2.1—2.3	Algorithms and complexity;
3.1—3.4	Proof strategies, sequences, sums, induction, recursion;
4.1—4.5	Counting, Pigeonhole Principle, permutations, combinations, binomial coefficients;
5.1—5.2	Discrete probability;
7.1—7.3, 7.5	Relations;
Parts of Chapter 8	Graphs, connectivity, shortest-path problems.

Cryptography:

2.4—2.6 and Silverman Chapters 16—18	Integers, division, Euclidean algorithm, Chinese Remainder Theorem, powers and roots in modular arithmetic;
Silverman Chapter 19 and other sources	Block ciphers, public-key cryptography, RSA cryptosystem, Diffie-Hellman key exchange, digital signatures and certificates, secret sharing, Data Encryption Standard (DES).

Assignments, Exams, and Grading

Homework: Homework will be assigned weekly and collected every Monday. It is very important that you keep up with the assigned work since the exams will be based on the homework problems. Feel free to work on the homework assignments together.

Exams: There will be one in-class midterm and a final. Dates of the exams will be announced later.

Project: You will be required to research and write a short (3—4 pages) expository paper on one of the topics below. You should start researching a topic within a few weeks, but before you do so, please talk to me so I can tell you exactly what I expect you to do (this will vary from topic to topic). You might start by quickly Googling the topics to see which one sounds most interesting. The paper will be due near the end of the semester. More details, as well as short descriptions of the topics, will be given in class. I might add more topics as the semester goes on. For now, they are

1. The Apportionment Problem
2. Godel's Undecidability Theorem
3. Scheduling problems and bin packing
4. Traveling Salesmen Problem
5. Modeling with trees
6. Finite-state automata
7. Pretty Good Privacy (PGP)

8. Secure Socket Layer (SSL)
9. Hash functions
10. Quantum cryptography

Grading:

20%	homework
20%	midterm
20%	project
40%	final

Important Dates

Wednesday, August 24	First day of class
Wednesday, September 7	Last day to drop
Friday, September 9	Last day to add
Monday, October 3	No class (reading break)
Wednesday, October 19	Last day to withdraw
Monday, November 21	No class (Thanksgiving)
Wednesday, November 23	No class (Thanksgiving)
Monday, December 5	Last class