Course Guidelines Math 133
Dr. R. Beezer Fall 2003

Texts We will be using the following texts, which are available in the Bookstore.

The Code Book, by Simon Singh
Invitation to Cryptology, by Thomas H. Barr
Secrets and Lies, by Bruce Schneier
Crypto, by Steven Levy
Cryptonomicon, by Neal Stephenson
Codes and Ciphers, by Mark Fowler

Home Page Start at `http://buzzard.ups.edu/courses.html` to locate the WWW page for this course.

Office Hours My office is Thompson 321G; the telephone number is 879–3564. Making appointments or simple, non-mathematical questions can be handled via electronic mail — my address is `beezer@ups.edu`. Office hours will be 10:00–10:50 on Monday, Wednesday and Friday, and 9:30–10:50 on Tuesday. I will always be available during these times on a first-come, first-served basis. If these times are not convenient, please do not hesitate to make an appointment with me for another time. You are also welcome to drop by my office without an appointment at any time that I am in (2 P.M. to 4 P.M. is a good time to try). Office hours are your opportunity to receive extra help or clarification on material from class, or to discuss any other aspect of the course.

Practicums There will be nine practical exercises in cryptology through the course. You will be provided with a written explanantion for each, and they will be graded on a pass/fail basis. Tentative due dates are given on the schedule.

> I hear, I forget.
> I see, I remember.
> I do, I understand.
> — Chinese Proverb

Reading We will work through *The Code Book* and *Invitation to Cryptology* deliberately, and dates for sections of these books are listed on the schedule. We will discuss *Secrets and Lies* and *Crypto* near the end of the semester, so you will want to be reading these two books in advance of those discussions. Reading these two books early will be of some assistance as you formulate topics for your research project. *Cryptonomicon* is a novel, and you will be expectred to be reading it uniformly through the semester. For example, you should be one-fourth of the way through by the time we have the first examination.

Puzzles The *Codes and Ciphers* book has 20 puzzles. The schedule indicates on every other Monday just where you should be in working through this book.

Discussions You will be organized into groups for weekly email discussions. Original submissions are due by midnight Friday each week, and conscientious efforts are worth three points. Replies to others' postings are worth 1 point each, and are due by midnight on Sunday. Please begin the subject line of each message with "Math 133" and be sure to include me on your distribution. Your discussion may concern any of the readings assigned to date.

Research Project A major portion of this course will be a research project on some public-policy or societal aspect of cryptology. It will include both written and oral presentations, along with early drafts. A more detailed description of the assignment will be distributed.

Examinations There will be four one-hour exams — see the attached sheet for tentative dates. The final exam will be given at 4 P.M. on Wednesday, December 17. The final exam cannot be given at any other time, so be certain that you do not make any travel plans that conflict, and also be aware that I will allow you to work longer on the final exam than just the two-hour scheduled block of time.

Grades Grades will be based on the following breakdown: Exams — 35%; Discussions — 20%; Practicums — 10%; Research Project — 20%; Final — 15%. Homework, attendance and improvement will be considered for borderline grades. Scores will be posted on the World Wide Web at `http://buzzard.ups.edu/courses.html`. No work will be accepted late. A reminder about withdrawals — a Withdrawal Passing grade (W) can only be given during the third or fourth weeks of the semester, after that time (barring unusual circumstances), the appropriate grade is a Withdrawal Failing (WF), *even if your work has been of passing quality.* See the attached schedule for the last day to drop with an automatic 'W' and please read *The Logger* about these often misunderstood grades.

Attendance Daily attendance is required and expected, and is a pretty good idea.

Syllabus Please read the distributed syllabus for a discussion of the purpose of this course — both as a freshman seminar within the core curriculum and as a course in cryptology for the educated citizen.

Tentative Daily Schedule

Monday	Wednesday	Friday
Sep 1 Labor Day	Sep 3 Introduction Syllabus	Sep 5 Singh, Chap 1
Sep 8 Singh, Chap 2 Puzzles, p. 57	Sep 10 Barr, Chap 1	Sep 12 Barr, Sec 2.1, 2.2 Practicum #1
Sep 15 Barr, Sec 2.3, 2.4	Sep 17 Barr, Sec 2.5, 2.6	Sep 19 Barr, Sec 2.7, 2.8
Sep 22 Singh, Chap 3 Puzzles, p. 63	Sep 24 Singh, Chap 4	Sep 26 Singh, Chap 5 Practicum #2
Sep 29 Exam #1 Last day to drop	Oct 1 Barr, Sec 3.1—3.3	Oct 3 Barr, Sec 3.4 Practicum #3 Due
Oct 6 Barr, Sec 3.5 Puzzles, p. 69	Oct 8 Barr, Sec 5.1	Oct 10 Barr, Sec 3.6
Oct 13 Singh, Chap 6 Position Paper, Proposal Due	Oct 15 Singh, Chap 7 Practicum #4 Due	Oct 17 Exam #2

Mid-Term

Monday	Wednesday	Friday
Oct 20 Fall Break Puzzles, p. 74	Oct 22 Barr, Sec 4.1	Oct 24 Barr, Sec 4.2 Practicum #5 Due
Oct 27 Barr, Sec 4.3	Oct 29 Barr, Sec 4.4	Oct 31 Barr, Sec 4.5 Practicum #6 Due
Nov 3 Barr, Sec 4.6 Puzzles, p. 79	Nov 5 Barr, Sec 4.7	Nov 7 No class Practicum #7 Due
Nov 10 Exam #3	Nov 12 Levy Schneier Position Papers, Draft Due	Nov 14 Levy Schneier Practicum #8 Due
Nov 17 Singh, Chap 8 Puzzles, p. 85	Nov 19 Levy Schneier	Nov 21 Levy Schneier Practicum #9 Due
Nov 24 Levy Schneier Position Papers Due	Nov 26 Exam #4	Nov 28 Thanksgiving
Dec 1 Position Papers, Oral Presentations Puzzles, p. 89	Dec 3 Position Papers, Oral Presentations	Dec 5 Position Papers Oral Presentations
Dec 8 Position Papers, Oral Presentations	Dec 10 Position Papers, Oral Presentations	

Final Examinations

Wednesday, December 17 at 4 P.M.