Course Guidelines Math 133 A & B
Dr. R. Beezer Spring 2006

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

The Code Book, by Simon Singh
Mathematics of Cryptography, by Robert A. Beezer
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. The course web page has a variety of resources. In some cases these are necessary for working the practicums, in other cases they might be useful as you begin to consider a topic for your position paper.

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 11:00–11:50 on Monday, Wednesday and Friday. 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 (good times to try are 2 P.M. to 4 P.M. on Monday, Wednesday and Friday, and most all of Tuesday). 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 ten practical exercises in cryptology through the course. You will be provided with a written description of each on the Friday a week before they are due, and they will be graded on a pass/fail basis. Due dates are given on the schedule — they are due before the start of class on Fridays, and will not be accepted late. We will have significant time on Mondays to discuss how the practicums are to be worked, so I suggest you review them over the weekend in preparation for Monday's session. We will not be able to take class time later in the week to discuss them and I generally do not have office hours on Thursdays.

Practicums require using a variety of computer resources. These are provided in the computer lab in Thompson 120, which you will have access to. Attempting practicums on your personal machine, mis-addressing email, and off-campus travel are not excuses for a failure to complete a practicum.

> Mathematics is not a spectator sport.
> — Anonymous

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

> An education is not received. It is achieved.
> — Anonymous

Reading We will work through Singh's *The Code Book* and Beezer's *Mathematics of Cryptography* deliberately, and dates for discussing sections of these books are listed on the schedule. Please be prepared for these discussions *in advance*. Generally we will cover mathematical topics on Wednesdays, with five lectures in the first few weeks, then in-class worksheets for several more weeks. Fridays will be discussions throughout almost the entire semester, with Singh being the primary topic for the first half.

We will discuss *Crypto* and *Secrets and Lies* 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 also be of some assistance as you formulate topics for your position paper. *Cryptonomicon* is a novel, and you will be expected to be reading it uniformly through the semester. For example, you should be one-third 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 most every Monday just where you should be in working through this book at a two-puzzle-per-week pace (excepting weeks when we have exams and presentations). Mondays will be a time to discuss each set of two puzzles. Examinations will include problems similar in spirit to the puzzles.

Discussions You will be organized into groups for weekly email discussions. Original submissions are due by 11:59 PM Thursday each week, prior to our Friday discussions. You then have until 11:59 PM Sunday night to reply to postings by other members of your group. Conscientious efforts on Thursday postings are worth three points. Replies to others' postings are worth one point each.

You must include me as a recipient on your postings in order to receive credit. Your replies over the weekend should be a response to a single classmate's original posting and should be sent to everybody in your group, and should of course include me also. These discussions will take place on `hushmail.com`. Discussion groups will be realigned after each exam, with new groups formed from individuals with similar levels of participation in prior weeks.

Postings should be thoughtful commentary or opinions on topics relevant to the course. Difficulties with practicums, how busy you are, why your boyfriend/girlfiend is mad at you, or what party you went to last night are not relevant topics. Discussions of topics described in Singh, thoughts on new mathematics, revelations from practicums or plot twists in *Cryptonomicom* are relevant. Your postings do not need to be excessively long, a normal-sized paragraph per point is a good guideline.

Position Paper 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 with due dates. No portion of this project will be accepted late.

Examinations There will be three exams — see the attached sheet for tentative dates. One of these is the final exam, which will be given at 10 AM on Friday, May 12 for Section A (10:00 class) and at Noon on Wednesday, May 10 for Section B (12:00 class). The final exam cannot be given at any other time, so be certain that you do not make any travel plans that conflict.

The exams neatly divide the course into three portions. Part I is classical cryptology and the basic mathematics required for both classical and modern cryptology. Part II considers modern cryptology, since the revolutionary events of the 1970's. Part III considers the societal and public-policy issues wrought by the combination of advanced cryptology, cheap computers and ubiquitous networks.

Grades Grades will be based on the following recipe: Discussions — 1 part; Practicums — 2 parts; Research Project — 2 parts; Exams — 3 parts. 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.

Electronic Mail This course has many components and many small assignments. Much of the course is also about electronic communications. So we will be sending each other a lot of email. I have three addresses I will read for this course, as described in Practicum EM. Please be careful about what you send me, and where you send it. If using a non-UPS email system please identify your real name someplace (header or body of the message). In particular, do not send me attachements unless it is absolutely necessary and try to avoid sending email in HTML format.

Attendance Daily attendance is required and expected, and is a pretty good idea. Unfortunately, I have found it necessary to track and encourage attendance. Every four absences (for any reason) will result in a grade penalty equal to reduction of 0.33 grade points (e.g. a B would become a B-), and two tardies will equal an absence. You are tardy if you are not present when I begin to check attendance.

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

Part I Classical Cryptology

Monday	Wednesday	Friday
Jan 16 MLK Day	Jan 18 Syllabus Preview EM	Jan 20 Singh, Chap 1 Practicum EM Due
Jan 23 Puzzles to p. 55 Preview STEG	Jan 25 Beezer Chap MA	Jan 27 Singh, Chap 2 Practicum STEG Due
Jan 30 Puzzles to p. 59 Preview MONO	Feb 1 Beezer, Chap B	Feb 3 Singh, Chap 3 Practicum MONO Due
Feb 6 Puzzles to p. 63 Preview VIG	Feb 8 Beezer, Chap BA, SS	Feb 10 Singh, Chap 4 Practicum VIG Due
Feb 13 Puzzles to p. 67 Preview PONT Last day to drop	Feb 15 Beezer, Chap DL	Feb 17 Singh, Chap 5 Practicum PONT Due

Part II Modern Cryptology

Feb 20 Exam #1 Classical Cryptology	Feb 22 Beezer, Chap NT	Feb 24 Singh, Chap 6
Feb 27 Puzzles to p. 71 Preview SDES	Mar 1 Beezer, Chap DHKE Key Exchange Worksheet	Mar 3 Singh, Chap 7 Practicum SDES Due
Mar 6 Puzzles to p. 74 Preview PGP1	Mar 8 Beezer, Chap DHKS Knapsack Worksheet	Mar 10 Levy, First Half Practicum PGP1 Due PP Proposal Due

Mid-Term

Monday	Wednesday	Friday
Mar 20 Puzzles to p. 77 Preview PGP2	Mar 22 Beezer, Chap RSA RSA Worksheet	Mar 24 Levy, Second Half Practicum PGP2 Due
Mar 27 Puzzles to p. 81 Preview PGP3	Mar 29 Singh, Chap 8	Mar 31 Quantum Worksheet Practicum PGP3 Due PP Rough Draft Due

Part III Society, Public Policy, Cryptology

Apr 3 Exam #2 Modern Cryptology	Apr 5 Policy: Free Crypto?	Apr 7 Policy: DRM
Apr 10 Puzzles to p. 85 Preview TIME	Apr 12 Policy: Patriot Act	Apr 14 Policy: NSA Practicum TIME Due Position Paper Due
Apr 17 Puzzles to p. 89 Preview ANON	Apr 19 Policy: Key Escrow	Apr 21 Policy: Computer Security Schneier Practicum ANON Due
Apr 24 Position Paper Presentations	Apr 26 Position Paper Presentations	Apr 28 Position Paper Presentations
May 1 Position Paper Presentations	May 3 Position Paper Presentations PP Letter Due	

Final Examinations

Section A (10:00): 8 AM, Friday, May 12
Section B (12:00): Noon, Wednesday, May 10