Course Guidelines
Dr. R. Beezer

Math 133
Spring 2013

Texts We will be using the following texts, which are available in the Bookstore or for download from the course page.

The Code Book, by Simon Singh
Mathematics of Cryptography, by Robert A. Beezer
Shadow Factory, by James Bamford
Crypto, by Steven Levy
Cryptonomicon, by Neal Stephenson

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 in Thompson 303; 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 are 1:30–3:00 on Monday, Wednesday and Friday. You may make an appointment for other times, or just drop by my office. 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 eleven practical exercises in cryptology through the course. You will be provided with a written description of each one, we will discuss them on Fridays, and they will be due on the next Wednesday prior to the start of class. They will be graded on a pass/fail basis and will not be accepted late. We will have significant time on Fridays to discuss how the practicums are to be worked.

Practicums require using a variety of computer resources. These are generally computer exercises, so difficulties using computers are not an excuse for not completing them. Mis-addressing email and off-campus travel are also 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.*

We will discuss *Crypto* and *Shadow Factory* 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 first part of semester. Target page numbers are given for each week on the calendar.

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 two exams — see the attached sheet for tentative dates. The final exam will be given at Noon on Friday, May 17. The final exam cannot be given at any other time, so be certain that you do not make any travel plans that conflict.

Grades Grades will be based on the following recipe: Practicums — 2 parts; Research Project — 2 parts; Exams — 3 parts. Attendance and improvement will be considered for borderline grades. Scores will be posted at `http://buzzard.ups.edu/courses.html`. No work will be accepted late.

Email 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.

Reminders Three reminders about university policies contained in the *Academic Handbook*. These are described thoroughly online, or a printed copy may be requested from the Registrar's Office (basement of Jones Hall).

"Regular class attendance is expected of all students. When non-attendance is in the instructors judgment excessive, the instructor may levy a grade penalty or may direct the Registrar to drop the student from the course."
See `http://www.pugetsound.edu/student-life/student-resources/student-handbook/academic-handbook/registration-for-courses-of-in/#Attendance`.

Withdrawal grades are often misunderstood. A Withdrawal grade (W) can only be given during the third through sixth 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'.
See `http://www.pugetsound.edu/student-life/student-resources/student-handbook/academic-handbook/grade-information-and-policy/#withdrawal`.

All of your graded work is expected to be entirely your own work, this includes homework. Anything to the contrary is a violation of the university's comprehensive policy on Academic Integrity (cheating and plagiarism). Discovered incidents will be handled strictly, in accordance with this policy. Penalties can include failing the course and range up to being expelled from the university.
See `http://www.pugetsound.edu/student-life/student-resources/student-handbook/academic-handbook/academic-integrity/`.

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

Monday	Wednesday	Friday
Jan 21 MLK Day	Jan 23	Jan 25 Cryptonomicon 150
Jan 28 Discussion Singh 1	Jan 30 Beezer MA	Feb 1 Preview EM Cryptonomicon 300
Feb 4 Discussion Singh 2	Feb 6 Beezer B	Feb 8 Preview STEG Cryptonomicon 450
Feb 11 Discussion Singh 3	Feb 13 Beezer BA	Feb 15 Preview MONO Cryptonomicon 600
Feb 18 Discussion Singh 4	Feb 20 Beezer SS	Feb 22 Preview VIG Cryptonomicon 750
Feb 25 Discussion Singh 5	Feb 27 Exam #1	Mar 1 Preview PONT Cryptonomicon 875
Mar 4 Discussion Singh 6 Last day to drop	Mar 6 Discussion Shadow Factory	Mar 8 Preview SDES Cryptonomicon 1000
Mar 11 Discussion Singh 7	Mar 13 Discussion Crypto (Levy)	Mar 15 Preview PGP1 Cryptonomicon 1150

Midterm Break

Monday	Wednesday	Friday
Mar 25 Beezer DHKE	Mar 27 Discussion Shadow Factory	Mar 29 PP Proposal Due Preview PGP2 Cryptonomicon 1000
Apr 1 Beezer DL	Apr 3 Discussion Crypto (Levy)	Apr 5 Preview PGP3 Cryptonomicon 1150
Apr 8 Beezer DHKS	Apr 10 Exam #2	Apr 12 Preview TIME
Apr 15 Beezer NT	Apr 17 Discussion Shadow Factory	Apr 19 Preview ANON Draft PP Due
Apr 22 Beezer RSA	Apr 24 Discussion Singh 8	Apr 26 Final PP Due Position Paper Presentations
Apr 29 Position Paper Presentations	May 1 Position Paper Presentations	May 3 Position Paper Presentations
May 6 Position Paper Presentations	May 8 Position Paper Presentations PP Letter Due	

Final Examinations
Noon, Friday, May 17