Mathematics 56H, T-Th 11:00-12:15, Phillips 228   
Karl Petersen, Mathematics

Fall 2014

Satisfies QI Math Requirement. Students in the Honors Program have priority in registration for this seminar.

**Texts:**   
Simon Singh, *The Code Book*, Doubleday, 1999  
Hans Christian von Baeyer, *Information, The New Language of Science,* Phoenix, 2004 James Gleick, *The Information*, Vintage, 2011

Also of interest: Hal Abelson, Ken Leeden, and Harry Lewis, *Blown to Bits: Your Life, Liberty, and Happiness after the Digital Explosion,* Addison-Wesley, 2008

**E-Reserve:**

1. *For All Practical Purposes*, COMAP, W.H. Freeman, 2000: Chs. 9 & 10; 331-381  
2. *Masked Dispatches*, US Government (NSA), 1992: Chs. 1,2,9,10; 11-24, 71-82  
3. *Invitation to Cryptology*, Thomas H. Barr, Prentice Hall, 2002, Sections 2.7 and 2.8, 134-158.  
4. *Modern Cryptology: A Tutorial,* Gilles Brassard, Springer-Verlag, Lecture Notes in Computer Science 325, 1988: parts of Ch. 5, 40-53, 70-78, Bibliography (91-107)  
5. *Privacy on the Line*, W. Diffie and S. Landau, MIT Press, 1998: Ch. 6, 125-150; Ch. 8, 183-203; Ch. 10, 225-245  
6. *Symbols, Signals and Noise: The Nature and Process of  Communication*, J. R. Pierce, Harper Torchbooks, Harper & Row, New York, 1961:  Ch. III, A Mathematical Model, pp. 45-63;  Ch. IV, Encoding and Binary Digits, 64-77;  Ch. V, Entropy, 78-106;  Ch. VIII, The Noisy Channel, 145-165  
   
 **Online Notes by KEP at http://www.math.unc.edu/Faculty/petersen/:**

1*.**Counting*   
2*. Number Theory and Cryptography*3*. Elementary Probability*4*. Shannon’s Information Theory*

**Office Hours:** T, Th 12:30-2 and by appointment, Phillips 300A. E-mail address: [petersen@math.unc.edu](mailto:petersen@math.unc.edu),

It is common to say that we are now living in the information age. What are the ways in which information is stored, transmitted, presented, and protected? What is information anyway? Topics for this seminar will be drawn from cryptography (secret writing throughout history, including Thomas Jefferson's cipher machine, the German Enigma machine, public-key systems, and security and privacy on the internet) and information theory (entropy, information compression, and error correction). Further topics may include symbolic dynamics (study of symbol streams and associated dynamical systems and formal languages); applications like image compression and processing (compact disks, MP3 and JPEG, transforms, error correction, noise removal); the manipulation and analysis of the huge reams of data now being collected by science, industry, and government (genomes, consumer research, intelligence data); and visualization (how can different kinds of information be vividly and usefully presented, combined, and compared?). These topics are mathematically accessible to anyone with a high-school background and offer many possibilities for experimentation and theoretical exploration.

We will begin by reading, discussing, and working on the texts. There will be some mathematical and computer exercises. (We will use software such as Matlab and Mathematica, but no previous knowledge or experience of software or of programming is assumed.) After developing this background, students will select individual or group projects that could involve encoding and decoding messages, enhancing and compressing images, transforming and filtering signals, measuring properties of information sources (including analysis of artistic and literary objects), investigating current information-related discoveries and issues, and so on. Each project should involve some independent research, experimentation, and exploration and should contain a significant mathematical component. For group projects, the contributions of each individual should be identifiable. Students will present their proposals and results to the seminar orally and in writing.

In this research-exposure course, you will be working with a Graduate Research Consultant, Colin Thomson, who will assist you with the research project. [The GRC Program is sponsored by the Office for Undergraduate Research ([www.unc.edu/depts/our](file:///C:\KEPDATA\Petersen%20Documents%20from%20D\LaptopDocuments11-08\KEP\Teach\Fall14\www.unc.edu\depts\our)), and you may be able to use this research-exposure course to meet a requirement of the Carolina Research Scholars Program (<http://www.unc.edu/depts/our/students/students_crsp.html>).] I encourage you to visit the OUR website to learn about how you can engage in research, scholarship and creative performance while you are at Carolina.

There will be a Quiz Tues. Sept. 16 and an Exam Tues. Nov. 18. The Final Exam is scheduled for Thurs. Dec. 11 at 12 PM. However, in view of the special seminar nature of this course, where the students are intensively involved throughout the semester and prepare and present substantial individual research projects, the scheduled final exam will be replaced by an alternative final assessment. The nature of this assessment will be specified later in the semester. Part of the final exam time may be used for final project presentations.

We will agree on an extra regular weekly meeting time (such as late afternoon, say 5-7, Wednesdays) for out-of-class experiences, such as installing Matlab and Mathematica, working on assignments together, viewing films and videos, and so on.  
 

|  |  |  |  |
| --- | --- | --- | --- |
| **Week** | **Topics** | **Readings** | **Comment, Assignment** |
| Aug. 19 | Information, coding, history, mathematics. Mary, Queen of Scots. Overview of ciphers. | Singh 1; Counting 1-3; Gleick Prologue | Classes start Tues. Aug. 19. Counting 2.1-2.4. |
| Aug. 26 | Vigenère (polyalphabetic) ciphers, cipher machines. | Singh 2-3; Counting 4-5 | Counting 3.1-3.3, 4.1-4.4. |
| Sept. 2 | Modular arithmetic, Enigma machine | Singh 4; Number Theory 1 | Counting 5.1-5.4. Number Theory 1.1. No classes Mon. Sept. 1. |
| Sept. 9 | Friedman and Kasiski tests, probability, languages | Singh 5 ; Barr 2.7; Prob Notes 1-2; Gleick 2-4 | Prob 1.1-1.8, 2.1-2.5. Matlab Assgt. 1 (basics). Barr 2.7: 2. |
| Sept. 16 | Cryptanalysis of Vigenère | Barr 2.8: pp. 143-top of 149 | Barr 2.8: 1-3 (use M-files and Caesar spreadsheet). Quiz Tues. Sept. 16. Movie Wed. Sept. 17. |
| Sept. 23 | Euclidean algorithm, primes, modular inverses. Information, physics, philosophy. | Number Theory Notes 2, 3; vB 1-6,8; Gleick 8-12 | Number Theory, Ex. 2-8. Project proposals. |
| Sept. 30 | Public keys, RSA | Singh 6; FAPP 370-376; Number Theory Notes 4, 5, 6 | Number Theory Notes Ex. 10, 11, 13, 14. FAPP p. 379, 15-18. |
| Oct. 7 | Applications of one-way functions, policy issues | Singh 7; Number Theory Notes 7; Diffie-Landau 6, 8; Abelson et al. Ch. 2; Gleick 14, 15 | Matlab Assgt. 1 Challenges. Univ. Day Sun. Oct. 12. |
| Oct. 14 | Quantum computing | Singh 8, vB 19-23, Gleick 13 | Fall Break Oct. 16-17. |
| Oct. 21 | Probability and information | vB 9-14; Prob Notes 3-7. | Prob. Notes 3.1, 4.1, 4.2,5.1, 5.2, 6.1-6.3. Project progress reports. Due Tues. Oct. 21. |
| Oct. 28 | Stationary sources, data compression | Pierce 3, 4; Info Notes 1,2; Gleick 1,5; FAPP 358-370, 331-350. | FAPP p. 379, 20-24. Info Notes 1.1. Prob. Notes 7.1. |
| Nov. 4 | Entropy and error correction | Pierce 5; Info Notes 3-5; Gleick 6 | FAPP p. 353: 7, 11, 12; p. 378, 7-11. |
| Nov. 11 | Shannon's theorems | Info Notes 7; Gleick 7 | Info Notes 3.1, 3.2, 4.1, 5.1 |
| Nov. 18 | Exam |  | Exam Tues. Nov. 18 |
| Nov. 25 | Presentations start Tues. Nov. 25 |  | Project papers due Tues. Nov. 25. TG Nov. 27 and 28. |
| Dec. 2 | Presentations |  | Classes end Wed. Dec. 3. Revised project papers due Thurs. Dec. 4 (Reading Day) |
| Dec. 9 |  |  | Final exam time: Thurs. Dec. 11, 12 PM. |

**Honor System:** Students in this course are bound by the UNC Honor System. You may (and probably should) work together on class preparation, homework, projects, and exam preparation, but papers should clearly indicate the contributions of each individual and should properly credit any sources used. Exams will be closed-book individual efforts. Students are asked to sign the Pledge at the end of each exam to attest that they followed the Honor System while taking it.

**Homework Problems:** Due Fridays (with exceptions for holidays, etc.). Papers are to be left in the wooden mailbox marked K. Petersen opposite Ph348 (not the metal mailbox in Ph327) before 1:00. Late papers will be given some credit at the discretion of the grader--just leave them in the box whenever they are ready. Please turn in papers that are neat and written so as to be coherent and easily readable, not first drafts with scribbles and scratch-outs. We want correct, clear, and efficient write-ups. Even for problems (or parts of problems) that require just direct calculations, include explanations, in grammatical English, of what you are doing, citing supporting formulas or theorems for the most significant steps. To achieve an acceptably high level of presentation, you will usually have to revise your paper after an initial draft, which already may be following several attempts at solving a problem. See the notes “Writing up Mathematics” on the instructor’s website for an example and more details.

**Discussion Leading:** We will establish a rotation of teams of two (maybe sometimes one or three) students to animate our discussions of the reading and work that we do outside of class. The leaders will be prepared to raise questions, which may be open-ended or about details. They will also seek to go beyond the assigned reading to other sources and will try to come up with examples, activities, or commentaries related to the ideas involved. Each week's leaders should *meet with the instructor in advance on Friday or Monday* to discuss ideas for questions and activities.

**About the Instructor:** Karl Petersen was born in Tallinn, Estonia, and grew up in East Orange, New Jersey. His degrees are from Princeton and Yale, and he has held visiting positions at universities in Austria, Chile, France, and India. Petersen's research area is ergodic theory, a fairly new branch of mathematics which applies probability and analysis to study the long-term average behavior of complicated systems, with applications ranging from celestial dynamics through interactions of biological populations to the efficient transmission and recording of information. Favorite activities include tennis and hiking.   
 