A First-Year Seminar in Cryptology

“The Art and Science of Secret Writing”

Rob Beezer
`beezer@ups.edu`

Department of Mathematics and Computer Science
University of Puget Sound

MAA Session on Cryptology for Undergraduates
Joint Mathematics Meetings
New Orleans, Louisiana
January 6, 2011

Posted at `http://buzzard.ups.edu/talks.html`

Outline

- Course Characteristics
- Texts
- Assignments
- Software
- Worksheets

A First-Year Seminar

- A “Scholarly and Creative Inquiry Seminar”
- One half of replacement for English & Communications sequence
- Every first-year student takes one
- Offered by any member of the faculty on any topic
- Minimal prerequisites, if any (4 years high school mathematics)
- Significant writing component (one large research paper, presentation)
- Fall: Populated by Advising Director
  Spring: more self-selection, more CS majors
- Not a *creative* writing course!

Course Outline

- Fall 2003, Spring 2005, Spring 2006
- 50 minutes, 3 days a week, 14 weeks
- 5 weeks: History, Classical Crypto (substitution, Vignere, Enigma)
- 5 weeks: Modern Crypto (DES, RSA, PGP)
- 4 weeks: Public Policy (Clipper Chip, NSA, DMCA), Presentations

Texts

- Simon Singh, *The Code Book* ∗
- Custom notes on basic mathematics (≈50 pages) ∗
  - Modular arithmetic
  - Bases, radix notation, binary
  - Discrete logarithm
  - Diffie-Hellman key exchange
  - Knapsack public-key algorithm
  - RSA public-key algorithm
- Neal Stephenson, *Cryptonomicon* ∗
  - WWII crypto: Alan Turing, Bletchley Park, Navajo Code Talkers
  - Modern crypto: "FINIX", Electrical Till Corporation (ETC)
  - Custom two page guide to historical and modern references
- Mark Fowler, *Codes and Ciphers*
  - Cumulative puzzles
  - Some are busy work, some employ classical algorithms
- Steven Levy, *Crypto*
- Bruce Schneier, *Secrets and Lies*

Assignments

- Python scripts create and email custom exercises
- Scripts also provide me with solutions for grading
- Example "Practicum": monoalphabetic substitution cipher
  - Different permutation for each student
  - Different plaintext for each student (≈5 KB from Project Gutenberg)
  - "Answer": email me back the author of the text
  - Provide a "guess-and-check" command-line tool
  - Better (more complete, thorough) tools exist on web (unfortunately)
- Research Project: A public-policy "position" paper

Practicums

- Steganography: send me a message in a JPEG, shared-key
- Vignere cipher: crack a message with software tools
- Pontiflex: Decode stream cipher with playing cards (Cyptonomicon)
- SDES: Distributed brute-force attack
  (1024 keys, 64 keys per students, Java applet)
- PGP: three exercises
  - Key generation and signing (by me)
  - I send encrypted text, they return the author encrypted
  - Each student gets five signed messages, only one signed by me
- Anonymous remailers
- PGP Timestamping with Stamper

Software

- Various command-line tools available
- Various web/Javascript tools also available
- Hushmail: free public-key email, discussion groups
- PGP is always a hassle, GnuPG now?
- Run my own email server?
- OS-specific? Or email and web tools?
- Mutt/Pine/command-line versus Facebook/Twitter/tablet?

Worksheets

- In-class worksheets in teams
- Illustrate public/private communications
- Toy versions of:
  - Diffie-Hellman key exchange
  - Knapsack public-key
  - RSA public-key

Talk: `http://buzzard.ups.edu/talks.html`

Archived Math 133's: `http://buzzard.ups.edu/courses.html`