INQ 110: Intellectual Inquiry
Cryptography: Secrets and Security
Fall 2009

Instructor: Dr. Jane Ingram
Office: 365 – A Trexler Hall
Phone: 375 – 2446
E-mail: ingram@roanoke.edu

Office Hours:
Mon, Wed: 1:30 – 3:00 pm
Tu, Th: 1:30 – 2:30 pm
Also by appointment or drop-in

Course Description: Every day vast amounts of private information such as bank account numbers, credit card numbers, medical records, company financial reports, and confidential emails are sent over networks from one computer to another and stored in vast databases. How secure are these transactions and databases? Cryptography, often called the science of secret writing, has been used for thousands of years to keep communications and information secure and is one of the primary technologies in use today. This course will examine the history, mathematics, and modern day applications of cryptography. We will address the role of cryptography, its limitations, and some of the political, social, and ethical considerations that come into play as we strive to ensure security and privacy in our electronic age.

Intended Learning Outcomes: At the end of the course, the successful student will be able to:

- Describe the role of cryptography throughout history.
- Describe and apply various cryptographic algorithms and some means of cryptanalysis.
- Describe the issues, both technological and non-technological, surrounding security of network communications; identify the role of cryptography and its limitations.
- Analyze current security issues in terms of cryptographic needs and social, ethical and political considerations.

In addition students will improve their skills in
- reading material with technical content
- writing clearly
- locating and evaluating source material and
- properly incorporating source material in written work.

Required Materials:

Additional Readings will be taken from several sources including:
- The Codebreakers (Revised and Updated), by David Kahn, Scribner, 1996.
- Articles from Scientific American, September 2008 issue on “The Future of Privacy”
Attendance  Class attendance is a critical factor for your success in this course. This is a seminar that requires students to come to class every class period prepared, ready to discuss the reading of the day and participate in other activities. Almost every class period will have some graded work either to be completed in class or to be turned in at the beginning of class – reading quizzes, writing activities, cryptography activities. **If you miss more than 3 classes for any reason, you will be dropped from the course.** If you miss a Peer Review/Workshop day, your grade on that paper will be reduced by one full letter grade.

Grading Policy  Your grade in this course will be based on the following:

- 3 "Major" papers  50%
  (Grade includes drafts, peer responses; first two papers 15% each; last paper 20%)
- Reading quizzes  15%
- 2 Major quizzes  10%
- Writing Portfolio  12%
  (Includes reading responses & short papers)
- Co-curricular Requirement  3%
- Daily Activities & Homework  10%
  (Includes cryptography activities & class participation)

Grading Scale:

<table>
<thead>
<tr>
<th>Grade</th>
<th>Percentage</th>
</tr>
</thead>
<tbody>
<tr>
<td>A</td>
<td>93-100</td>
</tr>
<tr>
<td>A-</td>
<td>83-86</td>
</tr>
<tr>
<td>B</td>
<td>73-76</td>
</tr>
<tr>
<td>B-</td>
<td>63-66</td>
</tr>
<tr>
<td>C</td>
<td>70-72</td>
</tr>
<tr>
<td>C-</td>
<td>60-62</td>
</tr>
<tr>
<td>D</td>
<td>67-69</td>
</tr>
<tr>
<td>D-</td>
<td>below 60</td>
</tr>
</tbody>
</table>

"Major" Papers:  You will be required to write three significant papers in the course. The paper assignments will be broken down into steps that will include at least one draft (a well-thought out draft, not a "rough" draft), a peer-review process, consultation with the instructor, and a final draft. Topics and details of each assignment will be handed out well in advance of the due dates. The first paper will be based on a single source while the second and third papers will involve some research on the part of the student. The first two papers will be 5 pages in length; the third approximately 8 – 10 pages.

Reading Quizzes:  You will be given a quiz almost every class period on the reading for that day. These quizzes will test your understanding of the key concepts in the reading. They will consist primarily of short-answer questions asking you to describe, explain, or apply some concept from the reading. **You may not make up reading quizzes; the two lowest reading quiz scores will be dropped.**

Reading Responses and Short Papers:  For most of the readings, you will write notes and responses. Reading guides will often, but not always, be provided to focus your responses. These reading responses will be collected on the day they are due and should all be included in the writing portfolio. Sometimes the responses will be written in class. Several times during the semester short 1 – 2 page papers will be assigned. Occasionally an assignment will ask you to revisit and revise earlier work.

"Major" Quizzes/"Mini" Tests:  You will be given two 30 – 45 minute quizzes that test your understanding of the course concepts and your ability to apply the cryptographic techniques covered in the course.

Co-Curricular Requirement:  Roanoke College sponsors many lectures and other opportunities to enrich your educational experience. In this course you are required to attend at least two approved events
and write a two page reflection paper on each. The papers must be turned in within one week of the event. The following lectures will meet this requirement – others will be announced as the semester progresses and posted on Blackboard.

- September 8, 7:30 (Olin Theater), Susan Jacoby, author of *The Age of American Unreason*
- September 17, 7:30 (Bast Gym), Constitution Day Speaker Justice Sandra Day O’Connor – log onto http://www.roanoke.edu/tickets
- Any lecture in the Department of Mathematics, Computer Science, and Physics Conversation Series. A list is posted at http://cs.roanoke.edu/MCSPSeries.

**Writing Portfolio:** All of your written work for this course, including reading responses, papers, and co-curricular reflection papers, must be kept in a folder or binder. This portfolio will be turned in at the end of the semester along with a final short paper. When you submit the final version of each "major" paper, you will also submit the drafts and peer-responses for that paper.

**Daily Activities and Homework:** In addition to reading, taking reading notes, and writing reading responses, there will be in-class cryptographic activities and homework assignments to give you a better understanding of the mathematical concepts. You will occasionally be responsible for leading a discussion of the day's reading.

**Academic Integrity:** Doing your own work and properly acknowledging the work of others is of utmost importance in the academic setting. It is your responsibility to understand and abide by the policies outlined in the booklet "Academic Integrity at Roanoke College" that you were given during orientation. Those policies will be strictly enforced in this course.

**Electronic Devices:** Cell phones and other electronic devices must be turned off prior to entering the classroom. The use of any electronic device during a quiz is strictly prohibited; any such use will be considered a breach of academic integrity.

**The Writing Center @ Roanoke College:** The Writing Center @ Roanoke College, located in the Goode-Pasfield Center for Learning and Teaching in Fintel Library, is a place where writers working in any academic discipline, at any level of competence, and at any stage of the writing process meet with trained peer writing tutors in informal, one-on-one sessions focused on writing. The Writing Center is open Sunday through Thursday from 4 to 9 pm starting Sunday, September 6. You may simply stop in, or schedule an appointment ahead of time by going to MyRC: Academics and looking for the Writing Center Schedule link. If you have questions, email the Writing Center at writingcenter@roanoke.edu or call the CLT at 375-4949. The Writing Center also sponsors writing workshops, grammar crammers, and creative writing playshops on writing related issues. You may be required to participate in one or more workshops or individual sessions during the semester. The Fall 2009 schedule will be posted on the RC website at www.roanoke.edu/writingcenter.

**Special Needs:** If you are on record with the College's Office of Special Services as having special academic or physical needs requiring accommodations, please meet with me as soon as possible. We need to discuss your accommodations before they can be implemented. If you believe you are eligible for accommodations but have not yet formally contacted Special Services, please contact Pam Vickers at 375-2247 or email vickers@roanoke.edu.

---

**Tentative Course Schedule – Subject to Change**
Overview of issues & terminology/A fascination with cryptography

Thursday, August 27  
Introduction to the Course  
Hacker, Guidelines for Active Reading, pages 57 – 62

Tuesday, September 1  
Levy, Preface and "The Loner"

Early History & Methods

Thursday, September 3  
Singh, "The Cipher of Mary Queen of Scots" (Chapter 1)  
Transposition & Substitution, Frequency Analysis

Tuesday, September 8  
Singh, "Le Chiffre Inde chiff rable" (Chapter 2)  
Vigenere Cipher

Thursday, September 10  
Singh, Chapter 2 continued  
Additional Reading

Cryptography in World War I & II

Tuesday, September 15  
Singh, "The Mechanization of Secrecy" (Chapter 3)

Thursday, September 17  
Peer Review & Workshop – Major Paper #1

Tuesday, September 22  
Major Quiz #1  
Singh, "Cracking the Enigma" (Chapter 4)

Thursday, September 24  
Chapter 4 Singh, continued  
Excerpts from Hinsley & Stripp, "Code Breakers: The Inside Story of Bletchley Park"

Friday, September 25 by 4 pm  
Major Paper #1 Due

Tuesday, September 29  
Singh, "The Language Barrier" (Chapter 5)

Thursday, October 1  
Library Research (Rebecca Heller, Research Librarian)

Modern Cryptography

Tuesday, October 6  
Singh, "Alice and Bob Go Public" (Chapter 6)

Thursday, October 8  
Public Key Cryptography, continued  
Modular arithmetic, RSA algorithm, Diffie-Hellman key exchange

FALL BREAK
<table>
<thead>
<tr>
<th>Date</th>
<th>Reading/Assignment</th>
</tr>
</thead>
<tbody>
<tr>
<td>Tuesday, October 20</td>
<td>Singh, &quot;Pretty Good Privacy&quot; (Chapter 7)</td>
</tr>
<tr>
<td>Thursday, October 22</td>
<td>Diffie/Landau, &quot;Introduction&quot; (Chapter 1)</td>
</tr>
<tr>
<td></td>
<td>and &quot;Cryptography&quot; (Chapter 2)</td>
</tr>
<tr>
<td>Tuesday, October 27</td>
<td>Peer Review Workshop – Major Paper #2</td>
</tr>
<tr>
<td></td>
<td><strong>Cryptography and Policy Issues</strong></td>
</tr>
<tr>
<td>Thursday, October 29</td>
<td>Major Quiz #2</td>
</tr>
<tr>
<td></td>
<td>Schneier, &quot;Security Needs&quot; (Chapter 5)</td>
</tr>
<tr>
<td>Friday, October 30 by 4 pm</td>
<td>Major Paper #2 Due</td>
</tr>
<tr>
<td>Tuesday, November 3</td>
<td>Selected readings from September 2008 <em>Scientific American</em> on RFID chips, wiretapping, Genetic Confidentiality) Work on paper #3 topic selection</td>
</tr>
<tr>
<td>Thursday, November 5</td>
<td>Diffie/Landau, &quot;Cryptography and Public Policy&quot; (Chapter 3), &quot;National Security&quot; (Chapter 4)</td>
</tr>
<tr>
<td>Tuesday, November 10</td>
<td>Diffie/Landau, &quot;Privacy: Protections and Threats&quot; (Chapter 6) Bibliography for Research Paper due</td>
</tr>
<tr>
<td>Thursday, November 12</td>
<td>Diffie/Landau, &quot;Communications in the 1990s&quot; (Chapter 8) &quot;Cryptography in the 1990s&quot; (Chapter 9)</td>
</tr>
<tr>
<td>Tuesday, November 17</td>
<td>Diffie/Landau, &quot;And Then It All Changed&quot; (Chapter 10) &quot;Apres le Deluge&quot; (Chapter 11)</td>
</tr>
<tr>
<td>Thursday, November 19</td>
<td>Singh, &quot;A Quantum Leap into the Future&quot; (Chapter 8)</td>
</tr>
<tr>
<td>Tuesday, November 24</td>
<td>Peer Review Workshop – Major Paper #3 (Research)</td>
</tr>
<tr>
<td></td>
<td><strong>THANKSGIVING BREAK</strong></td>
</tr>
</tbody>
</table>

**Roundtable Discussions of Current Issues (from Research Papers)**

<table>
<thead>
<tr>
<th>Date</th>
<th>Event</th>
</tr>
</thead>
<tbody>
<tr>
<td>Tuesday, December 1</td>
<td>Student Presentations &amp; Discussions</td>
</tr>
<tr>
<td>Thursday, December 3</td>
<td>Student Presentations &amp; Discussions</td>
</tr>
<tr>
<td>EXAM DAY</td>
<td>Major Paper #3 Due; Portfolio including final short paper due</td>
</tr>
</tbody>
</table>