Secrecy: Science and Fiction

General description

Common description
This course examines the evolution of secret communications, code making, and code breaking from ancient times to today. The role of secret communications in history, modern society, and development of computing technology will be examined. During the trip to UK, students will visit a number of historic sites where many of the events discussed in the course took place. During the visit to Bletchley Park, a focal point of this course, students will obtain hands-on experience with the machinery used for breaking secret communications during World War II.

CS 290 - Topics in Computer Science (catalog description)
Topics in Computer Science Irregular. [c] Prereq.: CS 151 or equivalent, and permission of instructor. This course will provide an opportunity to introduce into the curriculum elementary topics of current interest.

ENG 214 – Studies in International Literature (catalog description)
Studies in International Literature Study Area I [I] [L] An exploration of select subjects, techniques, and themes in British and world literature. Topics to be announced each semester. Students may not take this course under the same topic more than once. Does not count toward the English major.

Textbook and other reference materials

Neal Stephenson, Cryptonomicon.
Cory Doctorow, Little Brother.
William Gibson, Pattern Recognition.

Learning outcomes

CS program objectives and outcomes (http://www.cs.ccsu.edu/mission.html#objectives) are supported by the following learning outcomes achieved by students upon a successful completion of this course:

• Understand the basic role of secret communications in the development of modern society (g);
• Understand the role of cryptography in the development of modern computing technology (b,g);
• Understand ethical, legal, and societal implications of secret communications and code breaking (e);
- Be able to discuss cryptography-related issues at a technical level accessible to a broad audience (f);
- Work as a member of a team to design and implement a software project (a,b,c,d,i);
- Be able to apply mathematical and algorithmic problem-solving methods to implement a basic substitution cipher (a,b,i,j);
- Be able to apply mathematical and algorithmic problem-solving methods to decrypt messages encoded using a basic substitution cipher (a,b,i,j).

ENG program outcomes: Students will
- Understand the complex relationship between literature and its historical contexts, including geography (i.e., London as a real and a literary city).
- Understand the similarities and differences between codebreaking and literary interpretation.
- Write effectively across a variety of genres and media about literature and the world.

Also see article IV.6 of the course proposal for a list of CIE-related learning outcomes.

**Course schedule**

This schedule assumes that the course will meet twice a week, e.g. Monday and Wednesday. Generally, class activities on Day 1 (Monday) will be conducted by Dr. Kurkovsky, and class activities on Day 2 (Wednesday) will be conducted by Dr. Jones.

Reading: S = Singh, The Code Book

<table>
<thead>
<tr>
<th>Week</th>
<th>Day 1</th>
<th>Day 2</th>
</tr>
</thead>
</table>
| 1 – Jan 25 | Introduction  
Code breakers (National Geographic video)  
Applicable to: all students | Intros, redux.  
Applicable to: all students |
| 2 – Feb 1 | Ancient ciphers: Caesar cipher, etc.  
Reading: S-1  
Applicable to: all students | Doctorow, *Little Brother*  
Applicable to: all students |
| 3 – Feb 8 | Vigenere: an unbreakable Victorian cipher  
Reading: S-2  
Applicable to: all students | Doctorow, cont.  
Applicable to: all students |
| 4 – Feb 15  
Feb 12-15 President’s Holiday | Mechanization of secrecy: Zimmerman telegram and World War I  
Reading: S-3  
Applicable to: all students | Stephenson, *Cryptonomicon*  
Applicable to: all students |
| 5 – Feb 22 | Secret communications during WWII  
Reading: S-4  
Applicable to: all students | Stephenson, *cont.*  
Applicable to: all students |
| 6 – Mar 1 | Enigma  
Reading: S-4  
Applicable to: all students | Stephenson, *cont.*  
Applicable to: all students |
| 7 – Mar 8 | Decoding Nazi Secrets (NOVA/PBS video)  
Applicable to: all students | Stephenson, cont.  
Applicable to: all students |
| 8 – Mar 15 | Language barrier: Rosetta stone  
Reading: S-5  
Applicable to: all students | Stephenson, cont.  
Applicable to: all students |
<table>
<thead>
<tr>
<th>Date</th>
<th>Event Description</th>
<th>Location</th>
<th>Reading/Assignments</th>
<th>Applicable to:</th>
</tr>
</thead>
<tbody>
<tr>
<td>9 – Mar 22</td>
<td>Spring break</td>
<td>LONDON</td>
<td></td>
<td></td>
</tr>
<tr>
<td>10 – Mar 29</td>
<td>Solving the key exchange problem</td>
<td></td>
<td>Gibson, <em>Pattern Recognition</em></td>
<td>ENG 214</td>
</tr>
<tr>
<td>Apr 2-3</td>
<td></td>
<td></td>
<td>Reading: S-6</td>
<td></td>
</tr>
<tr>
<td>Good Friday</td>
<td></td>
<td></td>
<td>Applicable to: CS 290</td>
<td></td>
</tr>
<tr>
<td>11 – Apr 5</td>
<td>Pretty good privacy</td>
<td></td>
<td>Gibson, <em>Pattern Recognition</em></td>
<td>ENG 214</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Reading: S-7</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Applicable to: CS 290</td>
<td></td>
</tr>
<tr>
<td>12 – Apr 12</td>
<td>Course project presentations</td>
<td></td>
<td>Presentations</td>
<td>all students</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Applicable to: all students</td>
<td></td>
</tr>
<tr>
<td>13 – Apr 19</td>
<td>Course project presentations</td>
<td></td>
<td>Presentations</td>
<td>all students</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Applicable to: all students</td>
<td></td>
</tr>
<tr>
<td>14 – Apr 26</td>
<td>Course project presentations</td>
<td></td>
<td>Presentations</td>
<td></td>
</tr>
<tr>
<td>15 – May 3</td>
<td></td>
<td></td>
<td>Presentations</td>
<td></td>
</tr>
<tr>
<td>16 – May 10</td>
<td>May 12 last day of classes</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

**Assessment**

Performance of all students will be assessed using several short quizzes, a variety of online writing projects, a final exam, and a course project (for CS 290) or a term paper (for ENG 214).

**Course project (CS 290 only)**

Working in small teams, all students enrolled in CS 290 will be required to complete a course project that will illustrate their understanding of the course material and their ability to apply theoretical concepts in practice by implementing an encryption/decryption software system. All students will also be required to make a class presentation describing their work and demonstrating the software they produced.

**Paper sequence (ENG 214 only)**

Students will complete a sequence of assignments: short exercises in close reading, followed by slightly longer papers linking those exercises to locations in London. While in London, students will complete a variety of online assignments across various media. Upon return, students will develop a collective bibliography on codes in literature, and make podcasts of their engagement with literary codes. Finally, they will complete a reflective self-assessment.