

HNR 304 - 002
Spring 2008
Cryptology (3 credits)

INSTRUCTOR: Chris Christensen
Office phone: 859-572-6672 Office: ST 353
E-mail: christensen@nku.edu
Website: <http://www.nku.edu/~christensen/>

OFFICE HOURS: M 9:00 – 10:00, T noon – 1:00, W 10:00 – 11:00, R 9:30 – 10:30, F 9:00 – 10:00, by appointment, and by capture.

CLASS TIME: TR 1:40 – 2:55, HR 111.

PREREQUISITE: Students should be accepted into the Honors Program.

TEXTS: *The Code Book: The Evolution of Secrecy from Mary Queen of Scots to Quantum Cryptography* by Simon Singh.

Cryptanalysis: A Study of Ciphers and Their Solutions by Helen Fouché Gaines

TOPICS: Course discussions will be based on the material in chapters 1, 2, 3, 4, 6, and 7 of *The Codebook* and most of the ideas in Gaines' *Cryptanalysis*.

GRADING:

Cryptography and cryptanalysis exercises and participation throughout the course	40%
Short paper (4 – 6 pages) about Alan Turing Due R April 17	20%
Medium length paper (7 – 10 pages) based upon a book Due R May 1	20%
Project Presented during the last 4 days	20%

Work missed during excused absences may be made up without penalty.

ATTENDANCE: Attendance and participation in class discussions is expected; participation in cryptography and cryptanalysis exercises will be a portion of the course grade.

WITHDRAWAL: The deadline for withdrawing from this course with a grade of W is Monday, March 31. Withdrawal after that date is not likely to be permitted.

Mid-Term grades for freshmen will be entered March 3 – March 18. They will be available until March 31.

The instructor reserves the right to alter the syllabus if circumstances dictate.

The work you will do in this course is subject to the Student Honor Code. The Honor Code is a commitment to the highest degree of ethical integrity in academic conduct, a commitment that, individually and collectively, the students of Northern Kentucky University will not lie, cheat, or plagiarize to gain an academic advantage over fellow students or avoid academic requirements.

Course learning objectives:

- The student will understand the cryptographic and cryptanalytic ideas that are the foundations of modern cryptology.
- The student will be able to construct and break a collection of classical ciphers.
- The student will be able to clearly and correctly express cryptological ideas orally and in writing.
- The student will learn how to search for the ghosts of patterns in seemingly meaningless ciphertext.

Attainment of course learning objectives will be measured by class discussions, two papers, and a presentation.