

**MAT 483 - 001**  
**Fall 2007**  
**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: MWF 12:00 – 12:50, T 12:00 – 1:00, R 3:30 – 4:30, by appointment, and by capture.

CLASS TIME: MWF 1:00 - 1:50. ST 250.

PREREQUISITE: C or better in MAT 225 or CSC 362 or CSC 364.

TEXT: *Classical and Contemporary Cryptology* by Richard J. Spillman.

TOPICS: We will cover most of the material in chapters 1 - 9.

GRADING: **The tests and the exam will be “take home.”**

Two tests worth 150 points each	300
Distributed c. M, September 24	
Distributed c. M, November 3	
Comprehensive final exam	200
Due F, December 14 before noon.	
Exercises	50
Project	
Due F, December 7	<u>50</u>
	600

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

Test grading scales will be announced when tests are returned.

ATTENDANCE: You are responsible for all material assigned or covered in class. Attendance will not be taken.

WITHDRAWAL: The deadline for withdrawing from this course with a grade of W is Monday, October 29. Withdrawal after that date is not likely to be permitted.

Mid-Term grades for freshmen will be entered October 8 – October 22.

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 apply mathematical ideas to construct and break a collection of classical ciphers, block ciphers, and public key ciphers.
- The student will be able to clearly and correctly express cryptological ideas orally and in writing.
- The student will apply ideas from number theory, linear algebra, algebra, and statistics to construct and break ciphers.
- The student will learn how to search for the ghosts of patterns in seemingly meaningless ciphertext.
- The student will use various pieces of software as tools for cryptography and cryptanalysis.

Attainment of course learning objectives will be measured by two tests, a comprehensive final exam, exercises, and a project.

### **Projects:**

Class projects from the Spring 2005 class are posted at

<http://www.nku.edu/~mcsc/mat494/>

### **Software:**

Much can be done by hand, but it is not necessary to do so.

CAP that comes with your text is good software.

Previous class projects include useful software. <http://www.nku.edu/~mcsc/mat494/>

<http://faculty.goucher.edu/blewand/cryptomath/>

<http://studenthome.nku.edu/~kohuss/content/crypt.html>

There is a lot of cryptological software on the web.

You will have access to *Mathematica* in the computer science lab.

### **References:**

The standard reference for historical aspects of cryptology is:

*The Codebreakers* by David Kahn.

For cryptological algorithms:

*Applied Cryptography* by Bruce Schneier.

*Handbook of Applied Cryptology* by Alfred J. Menezes, Paul C. van Oorschot and Scott A. Vanstone. Pdf's of the chapters may be downloaded at

<http://www.cacr.math.uwaterloo.ca/hac/>

A general textbook introduction to cryptology:

*An Introduction to Cryptography with Coding Theory* by Wade Trappe and Lawrence C. Washington.

Wikipedia is a good reference for cryptological topics.