Southeast Missouri State University

Department of Mathematics **Course Number: MA464/664**
Title of Course: Mathematical Cryptography **Date: January 15, 2011**

I. Catalog Description:
Basic concepts of secure communication, classical cryptography and cryptoanalysis, monoalphabetic and polyalphabetic ciphers. Shannon's theory of secrecy. Modern private-key cryptosystems such as DES, and public-key cryptosystems such as RSA. (3)

II. Prerequisites:
One of the following (with a minimum grade of 'C'):
1. MA223 Elementary Probability and Statistics
2. MA250 Foundations of Mathematics
3. MA338 Discrete Mathematics II
4. MA345 Linear Algebra
5. MA443 Elementary Number Theory

III. Objectives of Course:
1. To provide methods of constructing and breaking classical cryptosystems.
2. To show mathematical principles behind modern cryptosystems.
3. To implement some of these methods into computer projects.

IV. Expectations of Students:
Students are expected to attend class, participate in classroom discussions and presentations, to understand technical terms used in this course, prove theorems, solve exercises and computer labs, and pass tests.

V. Course Outline (Suggested class hours are shown at right):

1.	Classical Cryptography	8
2.	Shannon's Theory of Secrecy	7
3.	Private Key Cryptography	7
4.	Public Key Cryptography	14
5.	Signature Schemes	6
6.	Examinations	3
	Total	45

VI. Textbook:
Douglas R. Stinson, *Cryptography, Theory and Practice*, CRC Press, 3rd Edition, 2006

VII. Basis for Student Evaluation:
1. Assignments 60% (664 students will receive larger more in-depth assignments)
2. Hourly Examinations 20%
3. Final Examination 20%

VIII. Grading Scale

90% - 100% = A
80% - 89% = B
70% - 79% = C
0% - 69% = F

The weight of the evaluation criteria may vary according to each instructor and will be communicated at the beginning of the course.

IX. Academic Policy Statement:

Students will be expected to abide by the University Policy for Academic Honesty regarding plagiarism and academic honesty. Refer to:
http://www6.semo.edu/judaffairs/code.html

X. Student with Disabilities Statement:

If a student has a special need addressed by the Americans with Disabilities Act (ADA) and requires materials in an alternative format, please notify the instructor at the beginning of the course. Reasonable efforts will be made to accommodate special needs.