

CALIFORNIA STATE UNIVERSITY CHANNEL ISLANDS

NEW COURSE PROPOSAL

PROGRAM AREAS MATH

- 1. Catalog Description of the Course.** *[Include the course prefix, number, full title, and units. Provide a course narrative including prerequisites and corequisites. If any of the following apply, include in the description: Repeatability (May be repeated to a maximum of ___ units); time distribution (Lecture ___ hours, laboratory ___ hours); non-traditional grading system (Graded CR/NC, ABC/NC). Follow accepted catalog format.]*

MATH 582. NUMBER THEORY AND CRYPTOGRAPHY (3)

Three hours lecture per week

Prerequisite: Admission to the Computer Science or Mathematics Graduate Program

Topics include: Number theory, finite fields, polynomial rings, elliptic curves, public-key cryptography, zero-knowledge protocols, primality testing, factorization algorithms and applications.

2. Mode of Instruction.

	Units	Hours per Unit	Benchmark Enrollment
Lecture	<u>3</u>	<u>1</u>	<u>24</u>
Seminar	_____	_____	_____
Laboratory	_____	_____	_____
Activity	_____	_____	_____

- 3. Justification and Learning Objectives for the Course.** (Indicate whether required or elective, and whether it meets University Writing, and/or Language requirements) *[Use as much space as necessary]*

This course is an elective for the proposed MS in mathematics. Students in the course will learn recent advances in the areas of cryptography and primality testing.

Through this course, students will be able to

- Describe and apply security algorithms
- Test numbers for primality
- Discuss and use cryptographic methods
- Use properties of elliptic curves for theoretical and computational purposes
- Apply factorization algorithms
- Express ideas of Number Theory and its application in oral and written form.

This course is not designed to satisfy the University Writing or Language requirements.

- 4. Is this a General Education Course** **YES** **NO**

- 5. Course Content in Outline Form.** *[Be as brief as possible, but use as much space as necessary]*

Divisibility: Theoretical Definitions and first principles,

Prime Numbers: Basic theorems about primes

Unique factorization theorem: Proof and consequences

Congruences: Introduction to Congruence Calculus .

Solutions of congruence equations: Techniques for solving linear and quadratic equations

Fermat's Little Theorem, Wilson's Theorem, Euler's *phi* function

6. References. *[Provide 3 - 5 references on which this course is based and/or support it.]*

Course in Number Theory and Cryptography, Neal Koblitz Springer-Verlag 1994 3-540-94293-9

7. List Faculty Qualified to Teach This Course.

All Mathematics Faculty

8. Frequency.

a. Projected semesters to be offered: Fall X Spring X Summer

9. New Resources Required.

a. Computer (data processing), audio visual, broadcasting needs, other equipment

None

b. Library needs

None

c. Facility/space needs

None

10. Consultation.

Attach consultation sheet from all program areas, Library, and others (if necessary)

11. If this new course will alter any degree, credential, certificate, or minor in your program, attach a program modification.

Jesse Elliott 10/31/03

Proposer of Course

Date

Approvals

Program Coordinator	Date
---------------------	------

GE Committee Chair (If applicable)	Date
---------------------------------------	------

Curriculum Committee Chair	Date
----------------------------	------

Dean	Date
------	------

Effective Semester: _____

California State University Channel Islands
New Course Proposal Consultation Sheet

1. Course prefix, number, title, and units: _____ MATH 482 NUMBER THEORY AND CRYPTOGRAPHY (3)

2. Program Areas: _____ MATH

Recommend Approval

Program Area/Unit	Program/Unit Coordinator	YES	NO (attach objections)	Date
Art				
Business & Economics				
Education				
ESRM				
Humanities				
Liberal Studies				
Mathematics & CS				
Sciences				
Library*				
Information Technology*				

* If needed