MISCELLANEOUS CHANGE PROPOSAL

Please use this form to make minor changes to a program. Examples of such changes include the following:

- Changing the total number of credits for a degree
- Changing course pre-requisites, unit values, etc.
- Changes in the University General Education or designation of specific courses to satisfy General Education requirements
- Changing policies and procedures regarding Undergraduate Admissions criteria
- Policies on probation and disqualification with the various undergraduate programs
- Changes in programs, majors, concentrations, minors, and tracks, unless these are “major” changes (see below), in which case you should use a “Changes to Existing Programs” form

Note: a major revision is one involving the smaller of: a) more than 1/3 of the courses required for the program or b) 4 or more total courses, or re-conceptualizing the purpose of the course.

Before you proceed, please review the approval process in advance and leave time for each involved person or committee to review the proposal.

DATE: 11/15/06
DEPARTMENT/SCHOOL: Mathematics
CONTACT PERSON: Sarah Merz
PHONE: x63040
BLDG & ROOM NO: South Campus, 103d

1. School: College of the Pacific
   Program: Mathematics
   Degree: B.S. Applied Mathematics

2. What is being changed and what is the rationale for the change?
The addition of Math 148 Cryptography to the Applied Math elective list in the course catalog. This course was originally offered as a special topics course for applied math majors, and counted as an elective as a special topics course. When we petitioned to add the course as Math 148 we neglected to alter the major list of electives.

3. Existing policy (if applicable):

4. New policy (if applicable):

5. Catalog copy (if applicable):

Four Required Math Department Electives_With the consultation of a major adviser, select 4 math electives from the following:

Math 39: Probability with Applications to Statistics
Math 72: Operations Research or Math 74: Discrete and Combinatorial Mathematics
Math 110: Numerical Analysis
Math 130: Topics in Applied Statistics
Math 131: Probability and Mathematical Statistics I
Math 132: Probability and Mathematical Statistics II
Math 148: Cryptography
Math 152: Applied Analysis
Math 157: Applied Differential Equations II
Math 174: Graph Theory
Math 193: Special Topics (subject to the approval of the advisor)
Please remember to make the corresponding changes to your program's catalog copy when you receive page proofs for next year's catalog.

MISCELLANEOUS CHANGE PROPOSAL
APPROVAL SHEET

DATE: 11/15/06
DEPARTMENT/SCHOOL: Mathematics
CONTACT PERSON: Larry Langley
PHONE: x63030
BLDG & ROOM NO: South Campus, 101a

Please obtain signatures in the order they appear below, as applicable.

1. ☐ DEPARTMENT CHAIR:
   [Signature]
   DATE: 12/15/06

2. ☐ CHAIRS OF OTHER INVOLVED DEPARTMENTS (if applicable):
   [Signature]
   DATE:

3. ☐ CHAIR, SCHOOL/COLLEGE CURRICULUM COMMITTEE:
   [Signature]
   DATE: 12-2-06

4. ☐ DEAN OF SCHOOL/COLLEGE:
   [Signature]
   DATE: 12-20-06

5. ☐ GENERAL EDUCATION COMMITTEE (if applicable):
   [Signature]
   DATE:

6. ☐ GRADUATE STUDIES COMMITTEE (if applicable):
   [Signature]
   DATE:

7. ☐ REGISTRAR:
   [Signature]
   DATE: 01-16-07

☐ ACADEMIC AFFAIRS COMMITTEE:
   DATE:
Instructor: Larry Langley
Office: Classroom Building 101a
Telephone: 946-3030. The Mathematics Department may be contacted directly at 946-2347
E-mail: llangley@pacific.edu
Office Hours: Monday, Wednesday: 1:15 - 3:15 pm. Also by appointment.
Personal web page: www1.pacific.edu/~llangley/
Text: Introduction to Cryptography with Coding Theory, Trapp and Washington.
Calculator: A calculator which can handle basic arithmetic is suggested. Features which may make a calculator appealing: Modular arithmetic or a remainder function, matrix operations, conversion to binary, factoring of integers, ability to handle a large number of significant digits, although none of these features are required.
Software: For some several in-class and take home projects during the term we will be using the MAPLE computer algebra system. This is recommended but not required for the course.
Prerequisites: You should have at least two semesters of Calculus or permission of the instructor with other evidence of a strong mathematical background.

Course Material and Learning Objectives: This course covers topics in cryptography and coding theory. We will look at classical cryptosystems through the Enigma cipher, as well as more recent history such as DES and RSA cryptosystem. Other possible topics include hash functions, digital signatures, digital cash, honest games, and error correcting codes. We also cover the number theory and algebra required to understand the mathematics underlying these systems.

Students will become familiar with several topics in the history of the development of modern cryptography. Students will learn the algorithms underlying several classical and modern cryptosystems including DES and RSA and will be able both encrypt and decrypt messages in most of these systems. Students will learn the language of the field of cryptography as well as many issues involved in the design of secure cryptographic systems including common attacks upon cryptosystems. Students will become familiar with the difficulty of random number generation in cryptography and will learn about pseudo-random number generation. Students will be able to solve problems using number theory and algebra related to cryptographic systems as well as become familiar with some of the fundamental theorems of number theory.

Additional topics may include applications of cryptographic systems to computer security beyond encrypting messages. Students may learn how to apply cryptosystems to password protection, digital signatures, authentication, and error checking. Students may learn how cryptosystems may be used to develop electronic tools such as digital cash and honest games.

Calendar:
Last day to add classes: Monday, January 24
First Exam: Tuesday, February 8
Last day to drop classes: Thursday, March 3
Second Exam: Thursday, March 17
Spring Break: March 21-28
Third Exam: Tuesday, April 26
Student Evaluation:

1. Homework and Computer labs 30%
2. Quizzes 10%
3. Three mid-term exams (20% each) 60%

Note: Copies of student work may be retained for evaluative purposes.

Homework: Homework will be assigned approximately once a week, on Thursday and collected the following Thursday at the start of class. You are welcome to work with other students or seek assistance from me on the homework. It is the nature of these problems that you should attempt the problems early, and give the difficult problems extra time. I will drop two homework assignments with the lowest scores.

Some homework assignments may include problems which can only be done using the computer. In addition, Computer labs, both in class and take home, will be included in the homework grade. We will be working with the computer algebra system Maple for most of the labs. Make up labs will only be given with written, verifiable and compelling excuses.

Extra Credit: Although this course focuses mostly on encryption, there is nothing quite like a good decryption challenge. These will be given out approximately once every two to four weeks. Everyone will be given at least a week to solve the challenge. If the problem is unsolved by the end of the week, the deadline will be extended until the problem is solved, (or the date of the last midterm, which ever comes first).

Attendance: You are expected to attend class regularly and participate. If you miss a day of class, you are responsible for lecture material, class discussions and work, and any announcements concerning the course.

Midterm Exams: There are three midterm exams during the term. Exams generally will be closed book in-class, although a portion of any exam might be given as a take home exam or may require the use of Maple. Makeup exams will only be given for verifiable, documented reasons, and I must be notified in advance of the exam, or if an emergency makes that impossible, before the next class period. Makeup exams might not follow the same format as the standard exam.

Quizzes: Six quizzes will be administered during the term, and your lowest quiz score will be dropped. The date of a quiz will be announced the class day before the quiz will be administered. The format of the quiz will typically be closed book, but a quiz may take a different format. Makeup quizzes will only be given under the same circumstances as make up exams.

Grade Scale:

<table>
<thead>
<tr>
<th>Grade</th>
<th>Percentage</th>
</tr>
</thead>
<tbody>
<tr>
<td>A</td>
<td>93-100%</td>
</tr>
<tr>
<td>A-</td>
<td>90-92%</td>
</tr>
<tr>
<td>B+</td>
<td>87-89%</td>
</tr>
<tr>
<td>B</td>
<td>83-86%</td>
</tr>
<tr>
<td>B-</td>
<td>80-82%</td>
</tr>
<tr>
<td>C+</td>
<td>77-79%</td>
</tr>
<tr>
<td>C</td>
<td>73-76%</td>
</tr>
<tr>
<td>C-</td>
<td>70-72%</td>
</tr>
<tr>
<td>D+</td>
<td>67-69%</td>
</tr>
<tr>
<td>D</td>
<td>60-66%</td>
</tr>
<tr>
<td>F</td>
<td>0-59%</td>
</tr>
</tbody>
</table>

HONOR CODE (From Tiger Lore, University Policies): “Students are expected to: 1) Act honestly in all matters; 2) Actively encourage academic integrity; 3) Discourage any form of cheating or dishonesty by others; 4) Inform the instructor and appropriate university administrator if she or he has a reasonable and good faith belief and substantial evidence that a violation of the Academic Honesty Policy has occurred.”

Examples of conduct considered cheating can be found in the handbook. Students who violate the Honor Code may receive a failing grade for an assignment or for the course.