New Course

LEHMAN COLLEGE
OF THE
CITY UNIVERSITY OF NEW YORK

DEPARTMENT OF MATHEMATICS AND COMPUTER SCIENCE

CURRICULUM CHANGE

1. **Type of change:** New Course

2. **Course Description:**

MAT(CMP) 417: Cryptography, 4 hours, 4 credits
Methods for transforming information into cryptic messages and for deciphering secret code. Review of selected topics in elementary number theory. Construction of linear, quadratic, and exponential ciphers, as well as key exchange protocols.
PREREQ: MAT 313

3. **Rationale:**
Cryptography is a very important and useful topic for both Mathematics and Computer Science majors. This course has been offered as a topics course and has proven very popular. The prerequisite is needed to ensure that students have the necessary background.

4. **Academic Objectives and Justification for the Course:**
The aim of this course is to teach Mathematics and Computer Science majors the elements of modern cryptography, a tool which has many real-life applications (such as data and monetary transmissions).

5. **Syllabus/Sample Text:**
Syllabus:
1. Review of elementary number theory
2. Linear diophantine equations and linear congruences
3. Linear ciphers
4. Quadratic congruences
5. Quadratic ciphers
6. Primality testing
7. Factorization techniques
8. Exponential congruences
9. Exponential ciphers
10. Establishing keys and message exchange

6. **Effect on Curriculum Offering Outside of the Departments:** None

7. **Faculty:**
The course will be taught by faculty members currently in the department.

8. **Estimated Enrollment and Frequency:** Anticipated enrollment is 20 students per semester. The course will be offered once each year.

9. **Date of Departmental Approval:** April 30, 2003