Application for New Course

1. Submitted by the College of Engineering
   Department/Division offering the course: Computer Science
   Date: August 1, 2000

2. Proposed designation and Bulletin description of this course:
   (a) Prefix & Number: CS 678
   (b) Full Title: Cryptography
       Abbreviated Title (≤ 24 characters): Cryptography
   (c) Lecture/Discussion hours per week: 3
   (d) Laboratory hours per week: 0
   (e) Studio hours per week: 0
   (f) Credits: 3
   (g) Course description:
       The study of security in communications and electronic computing. The encryption of
data using public key systems, block ciphers, and stream ciphers. The basic tools for the
design and analysis of such systems. Topics may include information theory,
authentication, digital signatures, secret sharing schemes, complexity theoretic issues,
probabilistic encryption, electronic commerce and others.
   (h) Prerequisites (if any): CS 515 or consent of the instructor.
   (i) May be repeated to a maximum of: N/A

3. To be cross listed as: not applicable
   Signature of cross-listing chair: ____________________________

4. Effective date: Fall 2001

5. Course to be offered: Fall Spring Summer
   X

6. Will the course be offered annually; explain if not: Yes

7. Why is the course needed? Communication over public channels has become an
   essential part of our society. Much of what is communicated – for example, credit card
   numbers, medical records, and bank records – must be kept private. This course studies a
   variety of tools for providing privacy and various related security properties, and studies
   the mathematics of the nature of security. It is essential to the development of modern
   communication systems that people with knowledge of these subjects be available.

8. By whom will the course be taught? Andrew Klapper
   Are facilities for teaching this course now available? Yes
   If not, what plans have been made for providing them?

9. What enrollment may reasonably be expected? 10

10. FEB 14 2001
11. Will this course serve students in the Department primarily? Yes
   Will it be of service to a significant number of students outside the Department? No
   If yes, under what area?

12. Check the category most applicable to this course:
   ___ traditional; offered in corresponding departments elsewhere;
   ___ relatively new, now being widely established;
   ___ not yet found in many (or any) other universities

13. Is this course part of a new proposed program? No
    If yes, which?

14. Will adding this course change the degree requirements in any programs?¹ No
    If yes, explain:

15. Attach a list of the major teaching objectives of the proposed course and outline
    and/or a reference list to be used: See attached

16. If the course is a 100-200 level course, please submit evidence (e.g., correspondence)
    that the Community College System has been consulted.
    not applicable

17. Within the Department, who should be contacted for further information about the
    proposed course?
    Name: Andrew Klapper      Phone: 257-6743

¹Approval of this course will constitute approval of the program change unless other program modifications are
proposed.
Signatures of Approval:

Department Chair: [Signature] Date: 11/14/2001
Dean of the College: [Signature] Date: 2/8/01

Date of Notice to the Faculty: 1/26/01

Undergraduate Council\(^2\): __________________________ Date: ________
University Studies\(^2\): __________________________ Date: ________
Graduate Council\(^2\): __________________________ Date: 5/24/01
Senate Council\(^2\): __________________________ Date: ________

Date of Notice to the University Senate: ________

Action other than approval: __________________________

\(^2\)If applicable, as provided by the Rules of the University Senate
**Needed Skills**
Students must have a solid background in discrete mathematics and algorithm design and analysis.

**Learning Outcomes**
Successful students will learn:

- Basic issues of security in communication and computing
- Basic approaches to solving security problems
- Mathematical tools for analyzing cryptographic protocols, including the theory of finite fields
- A variety of protocols for providing security in different settings
- The background needed to read the current literature in cryptography

**Week by Week Course Outline**

<table>
<thead>
<tr>
<th>Week</th>
<th>Activities</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Introduction to cryptography: classical approaches</td>
</tr>
<tr>
<td>2-3</td>
<td>Block ciphers</td>
</tr>
<tr>
<td>4-6</td>
<td>Stream ciphers</td>
</tr>
<tr>
<td>7-9</td>
<td>Public key systems</td>
</tr>
<tr>
<td>10-11</td>
<td>Authentication and signature schemes</td>
</tr>
<tr>
<td>12</td>
<td>Probabilistic encryption</td>
</tr>
<tr>
<td>13</td>
<td>Electronic commerce</td>
</tr>
<tr>
<td>14-15</td>
<td>Student talks</td>
</tr>
</tbody>
</table>

**Graded work**
Exact details about graded work in this course will be determined by the instructor offering the course and will be made available in the syllabus during the first class meeting. Typically there will be a presentation of a paper in the recent literature by each student, bi-weekly homework, and a two-hour final examination.

**Grading**
A student's grade will be determined by a weighted average of homework assignments, presentation, and the final examination. The faculty offering the course will make the details available at the start of the course. A typical weighting is:

- Homeworks: 40%
- Paper presentation: 25%
- Final Examination: 35%

**Possible Textbooks**