02/10/02

RECEIVED
FEB 25 2002

LSC Use Only
Number:
Submission Date:
Action-Date:

UWUCC USE Only
Number: 01-57
Submission Date:
Action-Date:

Cryptography

Course Number and Full Title

Course Revision

Course Number and Full Name

Studies Approval +
or existing course

Course Number and Full Title

Course Number and Full Title

Course Number and Full Title

PROGRAM: Major Minor Track

New Program*

Department Curriculum Committee

Department Chair

Syllabus of Record: COSC 427 Cryptography

Format for Requesting New Course Proposals

Part I. **New Course Proposal Cover Sheet for COSC 427 Cryptography**

Part II. **Description of Curricular Change**

1. A detailed course proposal is attached.

2. Course Analysis Questionnaire. Detailed answers to each of the questions have been included in the attachments.

Part III. **Letters of Support**

Letters of support from:
1. Dean Eck, supporting need for additional complement, if required.
2. Louise Burkey, MIS Department Chair, supporting the new track in Information

Syllabus of Record: COSC 427 Cryptography

NEW COSC 427 Syllabus of Record **Attachment A**

3 lecture hours
0 lab hours
3 credits

I. Catalog Description:

COSC 427 Cryptography 3c-0l-3sh

Prerequisites: COSC 310, MATH 122 or 123

Fundamental concepts of encoding and/or encrypting information, cryptographic protocols and techniques, various cryptographic algorithms, and security of information will be covered in depth.

II. *Course Objectives:*

a. mathematical background

[redacted]

c. block ciphers- RC5
d. combining block ciphers- double & triple encryptions
e. stream ciphers and real random sequence generators- RC4

[redacted]

f. one-way hash functions- MD5, SHA (secure hash algorithm)

5. Public-key algorithms (3 hours)
   a. RSA algorithms
   b. public-key digital signature algorithms- DSA
   c. secret-sharing algorithms

6. Two Class Tests (3 hours)

Total hours in semester = (42 hours)

IV. *Evaluation Method:*

Evaluation: The final grade of the course will be determined as follows:

Two Class Tests	30%
Final Exam	20%
Projects	40%
Quizzes and Class Participation	10%

Grading Scale: The grading scale will be:

[redacted]

2. Menezes, Alfred J., van Oorschot, Paul C., and Vanstone, Scott A. (1997) *Handbook of Applied Cryptography*, CRC Press, ISBN# 0849385237.

3. Messerschmitt, David G. (1999) *Networked Applications*, Morgan Kaufmann Publishers, ISBN# 1-55860-536-3.

4. Stallings, William (1999) *Cryptography and Network Security: Principles and Practice*, Second Edition, Prentice Hall, ISBN# 0-13-869017-0.

5. Stinson, Douglas R. (1995) *Cryptography: Theory and Practice*, CRC Press, Boca Raton, ISBN# 0849385210.

Syllabus of Record: COSC 427 Cryptography

Course Analysis
COSC 427 Cryptography

Section A: Details of the Course

A1. How does this course fit into the programs of the department? For what students is the course designed? (Majors, students in other majors, liberal studies).

This course is a controlled elective for all Computer Science majors who will pursue the

A6. **Do other higher education institutions currently offer this course? If so, please list**

examples.

A similar course is offered in many institutions, for example:

1. University of Pennsylvania
2. Princeton University
3. James Madison University
4. Yale University

A7. **Is the content, or are the skills, of the proposed course recommended or required by a professional society, accrediting authority, law or other external agency? If so, please provide documentation. Explain why this content or these skills cannot be incorporated**

The Association for Computing Machinery (ACM) does not explicitly recommend this course. The National Colloquium for Information Sys3tems Security Education (NCISSE) includes this course in the list of courses that it accepts for granting an institution its designation as Center for Excellence in Information Assurance Education.

Section B: Interdisciplinary Implications

B1. **Will this course be taught by one instructor or will there be team-teaching? If the latter,**

Faculty resources may not be adequate. We have a letter from the Dean after consultation with the President and Provost supporting the hiring of new faculty should the need arise. (Please see attachment).

C2. **What other resources will be needed to teach this course and how adequate are the current resources? If not adequate, what plans exist for achieving adequacy? Reply in terms of the following:**

Resources needed for this course are available although they can be improved.

[redacted]

the NSF Cybersecurity grant.

c **Library Materials:** These are being purchased with funding from the NSF grant.