02/10/02

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

UWUCC USE Only
Number: 01-57e
Submission Date: ____________
Action-Date: ____________
UWUCC-App. 3/19/02
Senate App 5/7/02

CURRICULUM PROPOSAL COVER SHEET
University-Wide Undergraduate Curriculum Committee

I. CONTACT

Contact Person: Sanwar Ali Phone: 357-7994

Department: Computer Science

II. PROPOSAL TYPE (Check All Appropriate Lines)

______ COURSE Cryptography
Suggested 20 character title

X New Course* COSC 427 Cryptography
Course Number and Full Title

______ Course Revision ____________
Course Number and Full Name

______ Liberal Studies Approval + for new or existing course ____________
Course Number and Full Title

______ Course Deletion ____________
Course Number and Full Title

______ Number and/or Title Change ____________
Old Number and/or Full Old Title
____
New Number and/or Full New name

______ Course or Catalog Description Change ____________
Course Number and Full Title

______ PROGRAM: ______ Major ______ Minor ______ Track

______ New Program* ____________
Program Name

______ Program Revision* ____________
Program Name

______ Program Deletion* ____________
Program Name

______ Title Change ____________
Old Program Name
____
New Program Name

III. Approvals (signatures and date)

Sanwar Ali
Department Curriculum Committee

Department Chair

02/19/02
College Curriculum Committee

John D. Eck
College Dean

+ Director of Liberal Studies (where applicable)

*Provost (where applicable)

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**

I. 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 Assurance.

Syllabus of Record: COSC 427 Cryptography

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

3 lecture hours
0 lab hours
3 credits
3c-0l-3sh

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:*

Upon successful completion of this course, the students are expected to learn

a. The fundamentals of cryptography and encryption
b. Various cryptographic protocols and techniques
c. Cryptographic algorithms
d. Security of information systems

III. *Detailed Course Outline:*

1. Foundations and Principles of Cryptography (3 hours)
   a. history
   b. terminology
   c. confidentiality
   d. authentication
   e. integrity
   f. non-repudiation

2. Cryptographic Protocols (9 hours)
   a. protocol building blocks
   b. basic protocols
   c. intermediate protocols
   d. advanced protocols

3. Cryptographic Techniques (12 hours)
   a. key length
   b. key management
   c. algorithm types and modes
   d. using algorithms

4. Cryptographic Algorithms (12 hours)

a. mathematical background
b. data encryption standard (DES)
c. block ciphers- RC5
d. combining block ciphers- double & triple encryptions
e. stream ciphers and real random-sequence generators- RC4
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:
90-100% = A, 80-89% = B, 70-79% = C, 60-69% = D, and < 60% = F.

Attendance policy: The attendance policy will conform to the University wide attendance criteria.

V. *Required Textbook, Supplemental Books and Readings:*

Schneier, Bruce (1996) *Applied Cryptography*, Second Edition, John Wiley & Sons, ISBN# 0-471-11709-9 (paperback). The new edition is expected to be out soon.

VI. *Special Requirements:*

Visual programming environment. The students need to have access to the current version of Microsoft Visual C++ to work on their projects. All computer labs throughout the campus are being equipped with Visual C++ compiler. It is anticipated that while we use Microsoft Visual C++, as the industry standard changes, we will also make changes to our programming environment.

VII. *Bibliography:*

1. Kaufman, Charlie, Perlman, Radia, and Speciner, Mike (1995) *Cryptography and Security*, Prentice-Hall, ISBN# 0-13-061466-1.

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 graduate in the Information Assurance track. Students from interdisciplinary cybersecurity minor may also take this course. Students from other departments may take this course as an elective if they have taken the prerequisite course.

A2. **Does this course require changes in the content of existing courses or requirements for a program?**

The course does not require changes in the contents of any of our existing courses. It will serve as a controlled elective for Computer Science majors and a choice for the proposed interdisciplinary Cybersecurity minor.

A3. **Has this course ever been offered at IUP on a trial basis (e.g. as a special topic)? If so, explain the details of the offering.**

The course has not been previously offered at IUP.

A4. **Is this course to be a dual-level course? If so, what is the approval status at the graduate level?**

This course is not intended to be a dual level course.

A5. **If this course may be taken for variable credit, what criteria will be used to relate the credits to the learning experience of each student? Who will make this determination and by what procedures?**

The course may not be taken for variable credit.

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 into an existing course.**

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, explain the teaching plan and its rationale.**

The course is designed to be taught by one instructor.

B2. **What is the relationship between the content of this course and the content of courses offered by other departments? Summarize your discussions (with other departments) concerning the proposed changes and indicate how any conflicts have been resolved. Please attach relevant memoranda from these departments that clarify their attitudes toward the proposed change(s).**

This course does not overlap with any other course at this University.

B3. **Will seat in this course be made available to students in the School of Continuing Education?**

Students from the School of Continuing Education who meet the prerequisites are encouraged to take this course.

Section C: Implementation

C1. **Are faculty resources adequate? If you are not requesting or have not been authorized to hire additional faculty, demonstrate how this course will fit into the schedules of current faculty. What will be taught less frequently of in fewer sections to make this possible?**

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.

a. **Space:** Classroom space is adequate.

b. **Equipment:** The equipment needed for this course has been purchased with funds from the NSF Cybersecurity grant.

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

d. **Laboratory Supplies and other Consumable Goods:** The Computer Science department has licensed copies Visual C++ and some applications software for projects. However, periodic updates will be required to keep up with the technology.

e. **Travel Funds:** No travel funds are currently needed.

C3. **Are any of the resources for this course funded by a grant? If so, what provisions have been made to continue support for this course once the grant has expired? (Attach letters of support from Dean, Provost, etc.)**

The NSF cybersecurity grant helped purchase the equipment needed for the hands-on laboratory portion of this course. When the program progresses and the grant is no more, the Dean has committed to support the maintenance of the course (see attachment).

C4. **How frequently do you expect this course to be offered? Is this course particularly designated for or restricted to certain seasonal semesters?**

The course is expected to be offered every other academic semester. If demand increases, the frequency of offering will be increased accordingly.

C5. **How many sections of this course do you anticipate offering in any single semester?**

It is anticipated that one section of the course will be offered each time. Again, based on demand, this can be increased.

C6. **How many students do you plan to accommodate in a section of this course? Is this planned number limited by the availability of any resources? Explain.**

Twenty-four students will be accommodated in a section of the course. Available machines and space in the lab dictate this limitation. When additional space and machines became available enrolment can be increased.

C7. **Does any professional society recommend enrollment limits or parameters for a course of this nature? If they do, please quote from the appropriate documents.**

No professional society recommends enrollment limits or parameters for this course or for courses resembling this course. However, past experience with hands-on courses that are taught in computer labs has shown that twenty-four students per section can be accommodated.