CGS Agenda Item: 12-60
Effective: Spring 2014

Eastern Illinois University

NEW/REVISED COURSE PROPOSAL FORMAT

(Approved by CAA on 9/29/11 and CGS on 10/18/11, Effective Fall 2011)

This format is to be used for all courses submitted to the Council on Academic Affairs and/or the Council on Graduate Studies.

Please check one: ✓New course ___ Revised course

PART I: CATALOG DESCRIPTION

1. **Course prefix and number, *such as ART 1000*:** MAT 4873
2. **Title (*may not exceed 30 characters, including spaces*):** Introduction to Cryptography
3. **Long title, if any (*may not exceed 100 characters, including spaces*):**
4. **Class hours per week, lab hours per week, and credit [*e.g., (3-0-3)*]:** 3-0-3
5. **Term(s) to be offered:** ___ Fall ✓Spring ___ Summer ___ On demand
6. **Initial term of offering:** ___ Fall ✓Spring ___ Summer **Year:** 2014
7. **Course description:**

Classical monoalphabetic cryptosystems (e.g. shift, affine, substitution, and permutation ciphers), classical polyalphabetic cryptosystems (e.g. Hill and Vigenère ciphers), linear feedback shift registers, modern cryptosystems (public key, stream, and block ciphers). Other topics (with particular interest to topics relevant to current events) will be considered, such as: anonymity, identification schemes, secret sharing schemes, multicast security, copyright protection, bit commitment, signature schemes, one-way hash functions, pseudo-random numbers, and electronic cash.

8. **Registration restrictions:**
   a. **Equivalent Courses**

- **Identify any equivalent courses** (e.g., cross-listed course, non-honors version of an honors course).

  No such course

- Indicate whether coding should be added to Banner to restrict students from registering for the equivalent course(s) of this course. ___ Yes ✓No

   b. **Prerequisite(s)**

- **Identify the prerequisite(s),** including required test scores, courses, grades in courses, and technical skills. Indicate whether any prerequisite course(s) MAY be taken concurrently with the proposed/revised course.

  C or better in either MAT 2345 or MAT 2800, AND C or better in both MAT 2170 and MAT 2550

- Indicate whether coding should be added to Banner to prevent students from registering for this course if they haven't successfully completed the prerequisite course(s). ✓Yes ___ No

  If yes, identify the minimum grade requirement and any equivalent courses for each prerequisite course:

  C or better, No equivalent courses

Who can waive the prerequisite(s)?
___ No one ✓Chair ✓Instructor ___ Advisor ___ Other (Please specify)

d. Co-requisites (course(s) which MUST be taken concurrently with this one): n/a

e. Repeat status: ✓Course may not be repeated.

___ Course may be repeated once with credit.

Please also specify the limit (if any) on hours which may be applied to a major or minor.

f. Degree, college, major(s), level, or class to which registration in the course is restricted, if any:

n/a

g. Degree, college, major(s), level, or class to be excluded from the course, if any: n/a

9. Special course attributes [cultural diversity, general education (indicate component), honors, remedial, writing centered or writing intensive] n/a

10. Grading methods (check all that apply): ✓Standard letter ___ CR/NC ___ Audit ___ ABC/NC ("Standard letter"—i.e., ABCDF--is assumed to be the default grading method unless the course description indicates otherwise.)

Please check any special grading provision that applies to this course:

___ The grade for this course will not count in a student's grade point average.

___ The credit for this course will not count in hours towards graduation.

If the student already has credit for or is registered in an equivalent or mutually exclusive course, check any that apply:

___ The grade for this course will be removed from the student's grade point average if he/she already has credit for or is registered in _____ (insert course prefix and number).

___ Credit hours for this course will be removed from a student's hours towards graduation if he/she already has credit for or is registered in _____ (insert course prefix and number).

11. Instructional delivery method: (Check all that apply.)

✓lecture ___ lab ___ lecture/lab combined ___ independent study/research

___ internship ___ performance ___ practicum or clinical ___ study abroad

___ Internet ___ hybrid ___ other (Please specify)

PART II: ASSURANCE OF STUDENT LEARNING

1. **List the student learning objectives of this course:**

a. If this is a general education course, indicate which objectives are designed to help students achieve one or more of the following goals of general education and university-wide assessment:

- **EIU graduates will write and speak effectively.**
- **EIU graduates will think critically.**
- **EIU graduates will function as responsible citizens.**

b. If this is a graduate-level course, indicate which objectives are designed to help students achieve established goals for learning at the graduate level:

- **Depth of content knowledge**
- **Effective critical thinking and problem solving**
- **Effective oral and written communication**
- **Advanced scholarship through research or creative activity**

Students will learn to:

- classify the fundamental problems cryptography seeks to solve
- analyze the inherent design tradeoffs in cryptosystems
- encode text into a form that facilitates encryption
- build classical monoalphabetic cryptosystems (e.g. shift, affine, substitution, and permutation ciphers)
- build classical polyalphabetic cryptosystems (e.g. Hill and Vigenère ciphers)
- utilize statistical cryptanalysis methods (e.g. frequency analysis and index of coincidence)
- identify linear feedback shift registers and m-sequences
- compare modern cryptosystems (e.g. DES, AES, RSA, and ElGamal).
- analyze other topics with particular interest to topics relevant to current events, such as: anonymity, identification schemes, secret sharing schemes, multicast security, copyright protection, bit commitment, signature schemes, one-way hash functions, pseudo-random numbers, and electronic cash

	biweekly homework assignments	Examinations	Final exam	Grad students only: current cryptographic journal article.
classify the fundamental problems cryptography seeks to solve	XX	XX	XX	
analyze the inherent design tradeoffs in cryptosystems	XX	XX	XX	
encode text into a form that facilitates encryption	XX	XX	XX	
build classical polyalphabetic	XX	XX	XX	

cryptosystems (e.g. Hill and Vigenère ciphers) build classical monoalphabetic cryptosystems (e.g. shift, affine, substitution, and permutation ciphers)				
utilize statistical cryptanalysis methods (e.g. frequency analysis and index of coincidence)	XX	XX	XX	
identify linear feedback shift registers and m-sequences	XX	XX	XX	
compare modern cryptosystems (e.g. DES, AES, RSA, and ElGamal).	XX	XX	XX	XX
analyze other topics with particular interest to topics relevant to current events, such as: anonymity, identification schemes, secret sharing schemes, multicast security, copyright protection, bit commitment, signature	XX			XX

schemes, one-way hash functions, pseudo-random numbers, and electronic cash				
For graduate students: identify modern research methods in cryptography and be able to apply them.				XX

2. **Identify the assignments/activities the instructor will use to determine how well students attained the learning objectives:**

   The instructor will use biweekly homework assignments with a mixture of theoretical and practical problems, examinations, and a final exam to gauge performance.

3. **Explain how the instructor will determine students' grades for the course:**

   Instructors will determine grades from the weighted average of homework, examination, and final exam scores (e.g. 50% homework, 30% examinations, 20% final exam).

4. **For technology-delivered and other nontraditional-delivered courses/sections, address the following:**
   a. **Describe how the format/technology will be used to support and assess students' achievement of the specified learning objectives:**
   b. **Describe how the integrity of student work will be assured:**
   c. **Describe provisions for and requirements of instructor-student and student-student interaction, including the kinds of technologies that will be used to support the interaction (e.g., e-mail, web-based discussions, computer conferences, etc.):**

   n/a

5. **For courses numbered 4750-4999, specify additional or more stringent requirements for students enrolling for graduate credit. These include:**
   a. **course objectives;**
   b. **projects that require application and analysis of the course content; and**
   c. **separate methods of evaluation for undergraduate and graduate students.**

   For graduate students, the goal is to have students identify modern research methods in cryptography and be able to apply them. To this end, students taking this course for graduate credit will be required to read, present and answer questions on a current cryptographic journal article.

6. **If applicable, indicate whether this course is writing-active, writing-intensive, or writing-centered, and describe how the course satisfies the criteria for the type of writing course identified. (See Appendix *.)**

   n/a

PART III: OUTLINE OF THE COURSE

Provide a week-by-week outline of the course's content. Specify units of time (e.g., for a 3-0-3 course, 45 fifty-minute class periods over 15 weeks) for each major topic in the outline. Provide clear and sufficient details about content and procedures so that possible questions of overlap with other courses can be addressed. For technology-delivered or other nontraditional-delivered courses/sections, explain how the course content "units" are sufficiently equivalent to the traditional on-campus semester hour units of time described above.

Week 1 Introduction to the fundamental problems of cryptography and basic terminology
Text encoding
Shift cipher
Exhaustive key search
Involutory keys

Week 2 Affine cipher
Substitution cipher
Permutation ciphers
Frequency analysis

Week 3 Hill cipher
Vigenère cipher
Kasiski test
Index of coincidence
Homework 1 due

Week 4 Linear feedback shift registers
M-sequences
Elementary probability theory
Perfect secrecy

Week 5 Entropy
Spurious keys
Product cryptosystems
Homework 2 due

Week 6 Substitution permutation networks
Linear cryptanalysis
Differential cryptanalysis
Data Encryption Standard
Block cipher modes of operation
Exam 1

Week 7 Advanced Encryption Standard
Introduction to public key cryptography
Elementary number theory
Homework 3 due

Week 8 RSA cryptosystem
Primality testing
Factoring
Discrete logarithm problem

Week 9 ElGamal cryptosystem
Finite Fields
Elliptic curves over the reals and modulo a prime
Homework 4 due

Week 10 Security requirements for signature schemes
Signature schemes based on RSA and ElGamal

Week 11 Cryptographic hash functions
Message authentication codes
Homework 5 due

Week 12 Diffie-Hellman key exchange
Key distribution patterns
Session key distribution
Exam 2

Week 13 Pseudo-random number generation

Week 14 and 15 Other topics with particular interest to topics relevant to current events, such as: anonymity, identification schemes, secret sharing schemes, multicast security, copyright protection, bit commitment, and electronic cash
Homework 6 due
Review
Presentations from graduate students
Final exam

PART IV: PURPOSE AND NEED

1. **Explain the department's rationale for developing and proposing the course.**

   A deeper version of this course has run successfully three times as a graduate topics course. There has been consistent interest in the class. However, as a graduate class it is accessible only to a small portion of undergraduates. Adapting the course to be a high level undergraduate class serves both graduate and undergraduate students. It also allows students to be able to better plan their schedules around a course that is run on a fixed schedule (as opposed to a topics course) and adds a strong elective to the program. Cryptography is a significant and expanding area of modern computer science.

   a. **If this is a general education course, you also must indicate the segment of the general education program into which it will be placed, and describe how the course meets the requirements of that segment.**
   b. **If the course or some sections of the course may be technology delivered, explain why.**

2. **Justify the level of the course and any course prerequisites, co-requisites, or registration restrictions.**

   The proposed course requires maturity in two areas: mathematics and computer science. MAT 2170 provides the basic programing background needed. A background in Linear Algebra is required and provided by MAT 2550. Either MAT 2345 or MAT 2800 provides the background in mathematical proofs and logic needed to learn the methods used in most modern cryptosystems.

3. **If the course is similar to an existing course or courses, justify its development and offering.**

   a. **If the contents substantially duplicate those of an existing course, the new proposal should be discussed with the appropriate chairpersons, deans, or curriculum committees and their responses noted in the proposal.**
   b. **Cite course(s) to be deleted if the new course is approved. If no deletions are planned, note the exceptional need to be met or the curricular gap to be filled.**

   This course is not similar to any known existing course at Eastern Illinois University. A deeper version of this course has run successfully three times as a graduate topics course. There has been

consistent interest in the class. Cryptography is a significant and expanding area of modern computer science.

4. **Impact on Program(s):**

   a. For undergraduate programs, specify whether this course will be required for a major or minor or used as an approved elective.

   b. For graduate programs, specify whether this course will be a core requirement for all candidates in a degree or certificate program or an approved elective.

   If the proposed course changes a major, minor, or certificate program in or outside of the department, you must submit a separate proposal requesting that change along with the course proposal. Provide a copy of the existing program in the current catalog with the requested changes noted.

   This course will be accepted as an elective course for the Mathematics and Computer Science major. It may also be of interest to other Mathematics or MIS majors and graduate students in Mathematics or Technology, provided they have the appropriate prerequisites.

PART V: IMPLEMENTATION

1. **Faculty member(s) to whom the course may be assigned:**
   Andrews, Mertz, or other qualified faculty in the Department of Mathematics and Computer Science.

   If this is a graduate course and the department does not currently offer a graduate program, it must document that it employs faculty qualified to teach graduate courses.

   n/a

2. **Additional costs to students:**

   Include those for supplemental packets, hardware/software, or any other additional instructional, technical, or technological requirements. (Course fees must be approved by the President's Council.)

   None

3. **Text and supplementary materials to be used (Include publication dates):**
   Cryptography: Theory and Practice, Third Edition, Stinson, Chapman and Hall/CRC, 2005, 1584885084

   and/or

   Cryptography Engineering: Design Principles and Practical Applications, Ferguson, Schneier and Kohno, Wiley, 2010, 0470474246

PART VI: COMMUNITY COLLEGE TRANSFER

If the proposed course is a 1000- or 2000-level course, state either, "A community college course may be judged equivalent to this course" OR "A community college course will not be judged equivalent to this course." A community college course will not be judged equivalent to a 3000- or 4000-level course but may be accepted as a substitute; however, upper-division credit will not be awarded.

n/a

PART VII: APPROVALS

Date approved by the department or school: April 23, 2012

Date approved by the college curriculum committee: September 14, 2012

Date approved by the Honors Council *(if this is an honors course):*

Date approved by CAA: CGS:

*In **writing-active courses**, frequent, brief writing activities and assignments are required. Such activities -- some of which are to be graded – might include five-minute in-class writing assignments, journal keeping, lab reports, essay examinations, short papers, longer papers, or a variety of other writing-to-learn activities of the instructor's invention. Writing assignments and activities in writing-active courses are designed primarily to assist students in mastering course content, secondarily to strengthen students' writing skills. In **writing-intensive courses**, several writing assignments and writing activities are required. These assignments and activities, which are to be spread over the course of the semester, serve the dual purpose of strengthening writing skills and deepening understanding of course content. At least one writing assignment is to be revised by the student after it has been read and commented on by the instructor. In writing-intensive courses, students' writing should constitute no less than 35% of the final course grade. In **writing-centered courses** (English 1001G, English 1002G, and their honors equivalents), students learn the principles and the process of writing in all of its stages, from inception to completion. The quality of students' writing is the principal determinant of the course grade. The minimum writing requirement is 20 pages (5,000 words).

Student Success Center		Career Services	Disability Services
http://www.eiu.edu/~success/	http://www.eiu.edu/~counsctr/	http://www.eiu.edu/~careers/	http://www.eiu.edu/~disablty/
581-6696	**581-3413**	**581-2412**	**581-6583**