NEW COURSE FORM

1. General Information.

a.	Submitted by the College of:	Engineering		Today's Date:	3/10/2011
b.	Department/Division:	Computer Science			
c.	Contact person name:	Andrew Klapper	Email:	klapper@cs.uky.edu	Phone: 7-6743
d.	Requested Effective Date:	☒ Semester following approval	OR	☐ Specific Term/Year[1]:	____

2. Designation and Description of Proposed Course.

a.	Prefix and Number:	CS378
b.	Full Title:	Introduction to Cryptology
c.	Transcript Title (if full title is more than 40 characters):	____
d.	To be Cross-Listed[2] with (Prefix and Number):	____

e. Courses must be described by at least one of the meeting patterns below. Include number of actual contact hours[3] for each meeting pattern type.

3 Lecture	____ Laboratory[1]	____ Recitation	____ Discussion	____ Indep. Study
____ Clinical	____ Colloquium	____ Practicum	____ Research	____ Residency
____ Seminar	____ Studio	____ Other – Please explain:	____	

f.	Identify a grading system:	☒ Letter (A, B, C, etc.)	☐ Pass/Fail
g.	Number of credits:	3	
h.	Is this course repeatable for additional credit?	YES ☐	NO ☒
	If YES: Maximum number of credit hours:	____	
	If YES: Will this course allow multiple registrations during the same semester?	YES ☐	NO ☐
i.	Course Description for		

[1] Courses are typically made effective for the semester following approval. No course will be made effective until all approvals are received.

[2] The chair of the cross-listing department must sign off on the Signature Routing Log.

[3] In general, undergraduate courses are developed on the principle that one semester hour of credit represents one hour of classroom meeting per week for a semester, exclusive of any laboratory meeting. Laboratory meeting, generally, represents at least two hours per week for a semester for one credit hour. (from *SR 5.2.1*)

NEW COURSE FORM

	Bulletin:	The study of secrecy in digital systems. Methods of keeping information secure from classical systems dating from ancient times to modern systems based on modern mathematics. Basic methods of encryption using public key systems, block ciphers, and stream ciphers. The mathematical tools for the design and analysis of such systems. Topics will include classical cryptography, modern methods of public and private key encryption, authentication and digital signatures, hashing, and passwords. Number theory, abstract algebra, combinatorics, and complexity theory necessary for the design and analysis of cryptographic systems.
j.	Prerequisites, if any:	CS 315 and STA281, or instructor's consent
k.	Will this course also be offered through Distance Learning?	YES[4] ☐ NO ☒
l.	Supplementary teaching component, if any:	☐ Community-Based Experience ☐ Service Learning ☐ Both
3.	**Will this course be taught off campus?**	YES ☐ NO ☒
4.	**Frequency of Course Offering.**	
a.	Course will be offered (check all that apply):	☐ Fall ☒ Spring ☐ Summer
b.	Will the course be offered every year?	YES ☒ NO ☐
	If NO, explain:	____
5.	**Are facilities and personnel necessary for the proposed new course available?**	YES ☒ NO ☐
	If NO, explain:	____
6.	**What enrollment (per section per semester) may reasonably be expected?**	15
7.	**Anticipated Student Demand.**	
a.	Will this course serve students primarily within the degree program?	YES ☒ NO ☐
b.	Will it be of interest to a significant number of students outside the degree pgm?	YES ☒ NO ☐
	If YES, explain:	May be taken by students in ECE.

8. Check the category most applicable to this course:

☐ Traditional – Offered in Corresponding Departments at Universities Elsewhere

☐ Relatively New – Now Being Widely Established

☐ Not Yet Found in Many (or Any) Other Universities

9. Course Relationship to Program(s).

a. Is this course part of a proposed new program? YES ☐ NO ☒

[4] You must *also* submit the Distance Learning Form in order for the proposed course to be considered for DL delivery.

NEW COURSE FORM

	If YES, name the proposed new program:	____
b.	Will this course be a new requirement[5] for ANY program?	YES ☐ NO ☒
	If YES[5], list affected programs:	____

10. **Information to be Placed on Syllabus.**

a.	Is the course 400G or 500?	YES ☐ NO ☒

If YES, the *differentiation for undergraduate and graduate students must be included* in the information required in ***10.b***. You must include: (i) identification of additional assignments by the graduate students; and/or (ii) establishment of different grading criteria in the course for graduate students. (See *SR 3.1.4*.)

b.	☒	The syllabus, including course description, student learning outcomes, and grading policies (and 400G-/500-level grading differentiation if applicable, from ***10.a*** above) are attached.

[5] In order to change a program, a program change form must also be submitted.

NEW COURSE FORM

Signature Routing Log

General Information:

Course Prefix and Number: CS378

Proposal Contact Person Name: Andrew Klapper Phone: 7-6743 Email: klapper@cs.uky.edu

INSTRUCTIONS:
Identify the groups or individuals reviewing the proposal; note the date of approval; offer a contact person for each entry; and obtain signature of person authorized to report approval.

Internal College Approvals and Course Cross-listing Approvals:

Reviewing Group	Date Approved	Contact Person (name/phone/email)	Signature
CS Faculty	11/04/2011	Kenneth Calvert / calvert@cs.uky.edu / 7-3961	Kenneth Calvert
Engineering Faculty	11/28/11	Richard Sweigard / rsweigar@engr.uky.edu / 7-8827	
		/ /	
		/ /	
		/ /	

External-to-College Approvals:

Council	Date Approved	Signature	Approval of Revision[6]
Undergraduate Council	3/27/2012	Sharon Gill	
Graduate Council			
Health Care Colleges Council			
Senate Council Approval		University Senate Approval	

Comments:

[6] Councils use this space to indicate approval of revisions made subsequent to that council's approval, if deemed necessary by the revising council.

CS 378
Introduction to Cryptology

Instructor: Dr. Andrew Klapper
Office Address: 307 Marksbury Building
Email: klapper@cs.uky.edu
Office Phone: 257-6743

Office hours: Tuesday 11am-12pm
Thursday 10am-11am

Course Description:

The study of secrecy in digital systems. Methods of keeping information secure from classical systems dating from ancient times to modern systems based on modern mathematics. Basic methods of encryption using public key systems, block ciphers, and stream ciphers. The mathematical tools for the design and analysis of such systems. Topics will include classical cryptography, modern methods of public and private key encryption, authentication and digital signatures, hashing, and passwords. Number theory, abstract algebra, combinatorics, and complexity theory necessary for the design and analysis of cryptographic systems.

Prerequisites: CS 315 and STA281, or instructor's consent

Student Learning Outcomes: (Learning outcomes are a description of what a student will be able to do upon completion of the course. See appendix for an overview of Bloom's Taxonomy of Cognitive Learning for examples of active verbs associated with the various levels of cognition.)

Successful students will:
1. Learn basic issues of security in communication and computing.
2. Learn basic approaches to solving security problems.
3. Learn mathematical tools for analyzing cryptographic protocols, including basic number theory.
4. Become familiar with a variety of protocols for providing security in digital systems.
5. Have experience implementing security protocols.

Course goals or objectives: To develop skills needed to participate in the design and implementation of computer security mechanisms. To understand fundamental issues involved providing security in digital communications and computing. To learn the mathematics underlying cryptographic systems.

Required Materials:
Introduction to Cryptography with Coding Theory, second edition, by Wade Trappe, Lawrence Washington. Publisher: Prentice Hall. ISBN-13: 978-0131862395.

Description of Course Activities and Assignments
Course activities will consist of in class lecture, weekly or biweekly

homeworks,
a programming project implementing a major cryptosystem.

Course Assignments

10 homework assignments: 20% total
1 midterm exam: 20%
1 Programming project 10%
1 final exam: 40%
attendance: 10%

Summary Description of Course Assignments

Assignments and exam questions will include: proving mathematical properties of cryptosystems; determining the results of cryptographic protocols; analyzing the performance of protocols; cryptanalyzing protocols; developing skills with the mathematical tools for cryptography such as number theory and probability theory. There will be a major programming project involving the implementation of a cryptosystem such as RSA.

Grading scale for undergraduates:

80 – 100% = A
65-79% = B
50-64% = C
40-49% = D
0-39% = E

Final Exam Information

As determined by the registrar.

Mid-term Grade

Mid-term grades will be posted in myUK by the deadline established in the Academic Calendar (http://www.uky.edu/Registrar/AcademicCalendar.htm)

Course Policies:

Submission of Assignments:

Homework must be handed in on paper in class within 5 minutes of the start of class. Late homework is not accepted without a compelling

excuse. Programming assignment should be handed in electronically.

Attendance Policy.
Attendance in class is required and counts for 10% of the final grade.

Excused Absences
Students need to notify the professor of absences prior to class when possible. S.R. 5.2.4.2 defines the following as acceptable reasons for excused absences: (a) serious illness, (b) illness or death of family member, (c) University-related trips, (d) major religious holidays, and (e) other circumstances found to fit "reasonable cause for nonattendance" by the professor.

Students anticipating an absence for a major religious holiday are responsible for notifying the instructor in writing of anticipated absences due to their observance of such holidays no later than the last day in the semester to add a class. Information regarding dates of major religious holidays may be obtained through the religious liaison, Mr. Jake Karnes (859-257-2754).

Students are expected to withdraw from the class if more than 20% of the classes scheduled for the semester are missed (excused or unexcused) per university policy.

Verification of Absences
Students may be asked to verify their absences in order for them to be considered excused. Senate Rule 5.2.4.2 states that faculty have the right to request "appropriate verification" when students claim an excused absence because of illness or death in the family. Appropriate notification of absences due to university-related trips is required prior to the absence.

Academic Integrity
Per university policy, students shall not plagiarize, cheat, or falsify or misuse academic records. Students are expected to adhere to University policy on cheating and plagiarism in all courses. The minimum penalty for a first offense is a zero on the assignment on which the offense occurred. If the offense is considered severe or the student has other academic offenses on their record, more serious penalties, up to suspension from the university may be imposed.

Plagiarism and cheating are serious breaches of academic conduct. Each student is advised to become familiar with the various forms of academic dishonesty as explained in the Code of Student Rights and

Responsibilities. Complete information can be found at the following website: http://www.uky.edu/Ombud. A plea of ignorance is not acceptable as a defense against the charge of academic dishonesty. It is important that you review this information as all ideas borrowed from others need to be properly credited.

Part II of *Student Rights and Responsibilities* (available online http://www.uky.edu/StudentAffairs/Code/part2.html) states that all academic work, written or otherwise, submitted by students to their instructors or other academic supervisors, is expected to be the result of their own thought, research, or self-expression. In cases where students feel unsure about the question of plagiarism involving their own work, they are obliged to consult their instructors on the matter before submission.

When students submit work purporting to be their own, but which in any way borrows ideas, organization, wording or anything else from another source without appropriate acknowledgement of the fact, the students are guilty of plagiarism. Plagiarism includes reproducing someone else's work, whether it be a published article, chapter of a book, a paper from a friend or some file, or something similar to this. Plagiarism also includes the practice of employing or allowing another person to alter or revise the work which a student submits as his/her own, whoever that other person may be.

Students may discuss assignments among themselves or with an instructor or tutor, but when the actual work is done, it must be done by the student, and the student alone. When a student's assignment involves research in outside sources of information, the student must carefully acknowledge exactly what, where and how he/she employed them. If the words of someone else are used, the student must put quotation marks around the passage in question and add an appropriate indication of its origin. Making simple changes while leaving the organization, content and phraseology intact is plagiaristic. However, nothing in these Rules shall apply to those ideas which are so generally and freely circulated as to be a part of the public domain (Section 6.3.1).

Please note: Any assignment you turn in may be submitted to an electronic database to check for plagiarism.

Accommodations due to disability

If you have a documented disability that requires academic accommodations, please see me as soon as possible during scheduled office hours. In order to receive accommodations in this course, you must provide me with a Letter of Accommodation from the Disability

Resource Center (Room 2, Alumni Gym, 257-2754, email address: jkarnes@email.uky.edu) for coordination of campus disability services available to students with disabilities.

Tentative Course Schedule

1. Introduction to cryptography: classical approaches (7 hours)
2. Mathematical tools: basic number theory (8 hours)
3. Block ciphers - DES and Rijndael (6 hours)
4. Public key cryptography - RSA and discrete log systems (7 hours)
5. Hash functions (3 hours)
6. Authentication and signature schemes (2 hours)
7. Cryptographic protocols (4 hours)
8. Applications (3 hours)
9. Midterm, reviews (3 hours)