COSC 427 Introduction to Cryptography-CrsRvs-2019-03-30

- The workflow icon is no longer available. Please click on the Page Status after the orange circle icon near the page title. *

Form Information

The page you originally access is the global template version. To access the template document that progresses through the workflow, please complete the following steps:

First Step: **ONLY** change the text in the [brackets] so it looks like this: **CRIM 101 Intro to Criminology-CrsRvs-2015-08-10**

- ***If DUAL LISTED list BOTH courses in the page title***

Second Step: Click **"SAVE"** on bottom right

- ***DO NOT TYPE ANYTHING INTO THE FIRST PAGE OTHER THAN THE TEXT IN BRACKETS***
- ***Please be sure to remove the Brackets while renaming the page***

Third Step: Make sure the word ***DRAFT*** is in yellow at the top of the proposal

Fourth Step: Click on "**EDIT CONTENTS**" (*not EDIT*) and start completing the template. When exiting or when done, click **"SAVE"** (*not Save Draft*) on bottom right

When ready to submit click on the workflow icon and hit approve. It will then move to the chair as the next step in the workflow.

**Indicates a required field*

Proposer*	David T. Smith	**Proposer Email***	dtsmith@iup.edu
Contact Person*	David T. Smith	**Contact Email***	dtsmith@iup.edu
Proposing Department/Unit*	Mathematical and Computer Sciences	**Contact Phone***	7-4478

Course Level*	undergraduate-level

Course Revisions

(Check all that apply;fill out categories below as specified; i.e. if only changing a course title, only complete Category A)

Category A:	Category B:
mod_prereq	course_revision
	** Teacher Education: Please complete the Teacher Education section of this form (below)*
	** Liberal Studies: Please complete the Liberal Studies section of this form (below)*
	** Distance Education: Please complete the Distance Education section of this form (below) - Please check the APPROVED DE Course List - ON DOCUMENTS PAGE before completing this section If already approved - you DO NOT need to do a DE proposal*

Rationale for Proposed Changes (All Categories)

(A) Why is the course being revised/deleted: * *Please be specific - this should be have more detail than the Summary for the Senate.*	The prequisites are updated to list MATH 309 in place of MATH 122 or MATH 123. SLOs are reworded with active verbs and added assessments. Course outline is updated to be in line with current practice.

(B) University Senate Summary of Rationale*	*Please enter a single paragraph summary/rationale of changes or proposal for University Senate.* The prequisites are updated to list MATH 309 in place of MATH 122 or MATH 123. SLOs are reworded with active verbs and added assessments. Course outline is updated to be in line with current practice.
(C) Implications of the change on the program, other programs and the Students:*	None

Current Course Information*	
Category A	
(D) Current Prefix*	COSC
Proposed Prefix	
(E) Current Number*	427
Proposed Number	
(F) Current Course Title*	Introduction to Cryptography
Proposed Course Title	
(G) Prerequisite(s)	COSC 310, MATH 122 or 123
Proposed Prerequisite(s)	COSC 310 and MATH 309
(H) Current Catalog Description	Fundamental concepts of encoding and/or encrypting information, cryptographic protocols and techniques, various cryptographic algorithms, and security of information will be covered in depth.
Proposed Catalog Description	Covers fundamental concepts of encoding and/or encrypting information, cryptographic protocols and techniques, various cryptographic algorithms, and security of information in depth.
If changing Category A, no further action required.	
Category B (if no change, leave blank)	
(I)Repeatable Course This is for a course that can be repeated Multiple times e.g. Internship	If YES, please complete the following: Number of Credits that May be Repeated: Maximum Number of Credits Allowed to be Repeated:
Proposed Repeatable Course	If YES, please complete the following: Number of Credits that May be Repeated: Maximum Number of Credits Allowed to be Repeated:
(J) Number of Credits	Class Hours per week:3 Lab Hours:0 Credits:3
Proposed Number of Credits	Class Hours:Lab Hours:Credits:

(K) Current Course Student

Learning Outcomes (SLOs)

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

- The fundamentals of cryptography and encryption
- Various cryptographic protocols and techniques
- Cryptographic algorithms
- Security of information systems

(L) Proposed Course Student

Learning Outcomes (SLOs)

For each outcome, describe how

the outcome will be achieved

Note that the text box in the table expands

SLO #	Outcome	How outcome is assessed
1	Demonstrate the fundamentals of cryptography and encryption.	Exams
2	Apply various cryptographic protocols and techniques to encrypt and decrypt data.	Lab Assignments
3	Discuss cryptographic algorithms.	Exams and Research Papers
4	Evaluate the role of cryptography in security information systems.	Exams and Research Papers

(M) Previous Brief Course Outline

(It is acceptable to copy

from old syllabus)

As outlined by the federal definition of a "credit hour", the following should be a consideration

regarding student work - For every one hour of classroom or direct faculty instruction,

there should be a minimum of two hours of out of class student work.

1. Foundations and Principles of Cryptography 3 hrs
   a. history
   b. terminology
   c. confidentiality
   d. authentication
   e. integrity
   f. non-repudiation
2. Cryptographic Protocols 9 hrs
   a. protocol building blocks
   b. basic protocols
   c. intermediate protocols
   d. advanced protocols
3. Cryptographic Techniques 12 hrs
   a. key length
   b. key management
   c. algorithm types and modes
   d. using algorithms
4. Cryptographic Algorithms 12 hrs
   a. mathematical background
   b. data encryption standard (DES)
   c. block cyphers-RCS
   d. combining block ciphers- double & triple encryptions
   e. stream ciphers and real random-sequence generators - RC4
   f. on-way hash functions- MD5, SHA(secure hash algorithm)
5. Public-key algorithms 3 hrs
   a. RSA algorithms
   b. public-key digital signature algorithms- DSA
   c. secret-sharing algorithms

Two class tests 3 hrs

(N) Brief Course Outline *(Give sufficient detail to communicate the* *content to faculty across campus.* *It is not necessary to include specific* *readings, calendar or assignments)*	*As outlined by the federal definition of a "credit hour", the following should be a consideration* *regarding student work - For every one hour of classroom or direct faculty instruction,* *there should be a minimum of two hours of out of class student work.*

1	Overview of Cryptography and its Applications
2	Classical Cryptosystems
3	Basic Number Theory
4	Data Encryption Standards
5	Advanced Encryption Standard (AES)
6	RSA Algorithm
7	Protocols
8	Key and Key Management
9	Algorithm Types and Modes
10	Public-Key Algorithms
11	E-Commerce and Digital Cash (applications)
12	Quantum Cryptography

Distance Education Section

- Complete this section only if adding Distance Education to a New or Existing Course

If Completing this Section, **Check the Box to the Right:**	**NOTE: you must check this box if the Course has previously been approved for Distance Education**
Course Prefix/Number	
Course Title	
Type of Proposal	*See CBA, Art. 42.D.1 for Definition*
Brief Course Outline	*Give an outline of sufficient detail to communicate the course content to faculty across campus. It is not necessary to include specific readings, calendar or assignments* *As outlined by the federal definition of a "credit hour", the following should be a consideration regarding student work - For every one hour of classroom or* *direct faculty instruction, there should be a minimum of two hours of out of class student work.*
Rationale for Proposal (Required Questions from CBA)	
How is/are the instructor(s) qualified **in the Distance Education delivery** **method as well as the discipline?**	

For each outcome in the course, describe **how the outcome will be achieved using** **Distance Education technologies.**	
How will the instructor-student and **student-student interaction take place?** **(if applicable)**	
How will student achievement be evaluated?	
How will academic honesty for tests **and assignments be addressed?**	

Liberal Studies Section

- Complete this section only for a new Liberal Studies course or Liberal Studies course revision

If Completing this Section, **Check the Box to the Right:**	**NOTE: you must check this box if the Course/Program has previously been approved for Liberal Studies**

Liberal Studies Course Designations (Check all that apply)	
Learning Skills:	
Knowledge Area:	
Liberal Studies Elective	*Please mark the designation(s) that apply - must meet at least one*
Expected Undergraduate Student **Learning Outcomes** **(EUSLOs)** Map the Course Outcome to the **EUSLO's**	*Map each course outcome to the appropriate EUSLOs tha apply. Fill in the course outcome number* *See https://www.iup.edu/liberal/faculty-and-staff/euslos/ for additional information regarding mapping EUSLOs*

Informed Learners demonstrate:	**Course SLO #**
• the ways of modeling the natural, social and technical worlds	
• The aesthetic facets of human experience	
• the past and present from historical, philosophical and social perspectives	

• the human imagination, expression and traditions of many cultures	
• the interrelationships within and across cultures & global communities	
• the interrelationships within and across disciplines	
Empowered Learners demonstrate:	**Course SLO #**
• effective oral and written communication abilities	
• ease with textual, visual and electronically-mediated literacies	
• problem solving skills using a variety of methods and tools	
• information literacy skills including the ability to access, evaluate, interpret and use information from a variety of sources	
• the ability to transform information into knowledge and knowledge into judgement and action	
• the ability to work within complex systems and with diverse groups	
• critical thinking skills including analysis, application and evaluation	
• reflective thinking and the ability to synthesize information and ideas	
Responsible Learners demonstrate:	**Course SLO #**
• intellectual honesty	
• concern for social justice	
• civic engagement	
• an understanding of the ethical and behavioral consequences of decisions and actions on themselves, on society, and on the physical world	
• an understanding of themselves and a respect for the identities, histories and cultures of others	

How will each outcome be measured (note should mirror (L) Student Learning Outcomes* (SLO) from the course proposal	*Narrative on how the course will address the Selected Category Content* **Course SLO #** / **Assessment Tool to be used to measure the outcome** 1 2 3
All Liberal Studies courses are required to include perspectives on cultures and have a supplemental reading. Please answer the following questions.	
Liberal Studies courses must include the perspectives and contributions of ethnic and racial minorities and of women whenever appropriate to the subject matter. Please explain how this course will meet this criterion.	
Liberal Studies courses require the reading and use by students of at least one non-textbook work of fiction or non-fiction or a collection of related articles. Please describe how your course will meet this criterion.	

Teacher Education Section

- Complete this section only for a new Teacher Education course or Teacher Education course revision

If Completing this Section, Check the Box to the Right:	**NOTE: you must check this box if the Course/Program has previously been approved for Teacher Education related items**
Course Designations:	
Key Assessments	
	For both new and revised courses, please attach (see the program education coordinator): • The Overall Program Assessment Matrix • The Key Assessment Guidelines • The Key Assessment Rubric **File** **Modified** No files shared here yet. • Drag and drop to upload or browse for files
Narrative Description of the Required Content	*How the proposal relates to the Education Major*

Please scroll to the top and click the Page Status if you are ready to take action on the workflow.
Please submit an ihelp if you have any questions http://ihelp.iup.edu