

PROCESS A NON-GENERAL EDUCATION - CURRICULUM PROPOSAL

SCC #04-05- JK/O

LEAP: APPROVED FOR AM REGUL REC

Deadlines

October 8, 2004 to be implemented Fall 2005 - February 11, 2005 to be implemented Spring 2005

PROPOSAL TITLE: Computer Cryptography  
Sponsor: Seth P. Bergmann E-Mail: bergmann Ext: 3197  
DEPARTMENT: Computer Science  
COLLEGE: LAS

Liberal Arts & Sciences O-EDK:  History/Humanities  Math/Sciences  Social/Behavioral Sciences  
 UNDERGRADUATE  GRADUATE

THE ATTACHED NON-GEN-ED PROPOSAL IS BEST DESCRIBED BY THE ITEM(S) CHECKED:

New non-gen-ed course  Minor curricular changes (fewer than three) to  
 Short-term non-gen-ed course  Existing non-gen-ed course  
 Non-gen-ed degree requirements  
 Major  
 Minor, specialization, concentration, track,  
certificate program

THE FOLLOWING SIGNATURES REPRESENT APPROVAL

Department Chair: [Signature] Date: 2-3-05  
Department Curriculum Chair: [Signature] Date: Feb 8 2005  
Academic Dean: [Signature] Date: 2-9-05

COLLEGE CURRICULUM COMMITTEE

OPEN HEARING Date: 3/28/2005 Approved:  Not Approved:   
COLLEGE CURRICULUM CHAIR: [Signature]  
Senate Curriculum Chair Signature: [Signature] Date Senate Announcement: 4/12/05  
Comments: \_\_\_\_\_

EXECUTIVE VICE PRESIDENT/PROVOST Signature: [Signature] Date: 4/28/05  
 Approved  Not Approved

REGISTRAR  
Date: 5/3/05 Course Description Received & Approved - Reg's Taxonomy & Course #: 0707350  
Registrar Signature: [Signature]

NOTIFICATION FORWARD

SCC Chair  Academic Dean  Department Chair  Registrar  IR  CAP  
 VP Student Affairs  Others

DB 6-2-05  
Tom 5/25/05

# Course Proposal

## Computer Cryptography

### 1. Details:

- a. Course Title: Computer Cryptography
- b. Sponsor(s): Seth Bergmann, Computer Science Department
- c. Credit Hours: 3 cr.
- d. Course Level: Undergraduate (~~Junior/Senior level~~)
- e. Prerequisites: Foundations of Computer Science (0707.210)
- f. Time scale: This course is to be offered alternate years, beginning in Fall '06.
- g. Curricular Effect: This course will not be required for students in the CS major; it may be taken as a restricted elective.
- h. No additional resources will be needed.
- i. Recommended Library Resources: Additional books on cryptography have been ordered for the library.
- j. Short-term Evaluations: This course was offered as a 'Selected Topic in Computer Science', Fall '04. Informal feedback from students was very positive and encouraging. No formal survey was done.

### 2. Rationale:

Cryptography (the process of creating ciphers from plain text), as well as cryptanalysis (the process of retrieving plain text from a cipher), are becoming increasingly important in today's society. Secure communication in government, military, and financial operations are essential. Since most such communication is done via the internet, computers are used to encrypt and decrypt messages, authenticate messages, and ensure the integrity of messages.

### 3. Essence of the Course:

- a. Students who take this course will study the history of cryptology, which includes both cryptography and cryptanalysis. They will also learn how weak codes are broken, and they will study some of the popular encryption methods used today (single-key and public/private key). Students will gain an exposure to some of the by-products of cryptography, such as authentication and integrity. There will be brief discussions of the political and ethical aspects of cryptography.
- b. Topical Outline/Content
  - Essence of cryptography, cryptanalysis, authentication, integrity
  - History of cryptography
  - Classical techniques: Shift, affine, substitution, transposition, and polyalphabetic ciphers; cryptanalysis using statistical methods
  - Symmetric key cryptography
  - Public key cryptography

- Examples: DES, PGP, RSA
  - Java packages for cryptography
- c. Students will be evaluated on the basis of functional, correctly working programs, quizzes, and exams.
- d. Course Evaluation: This course will be evaluated through student surveys, as well as by the Computer Science Accreditation Commission when the computer science major is to be re-evaluated in 2006.
4. Consultations (responses are attached)
- a. Chris Simons, Mathematics
  - b. Shreekanth Mandayam, Electrical & Computer Engineering
  - c. Bob Fleming, Management & M.I.S.

6. Catalog Description:

0707.350 (Suggested hegis number)

3 s.h.

**Computer Cryptography**

(Prerequisite: 0707.210)

This course introduces students to the principles and practices which are required for secure communication: cryptography, cryptanalysis, authentication, integrity, and digital certificates. Mathematical tools and algorithms are used to build and analyze secure cryptographic systems with computers. Social, political, and ethical aspects of cryptography are also covered.

Rowan University  
CURRICULUM PROPOSAL  
LIBRARY RESOURCE FORM

The purpose of this form is to provide a channel of communication between the library and faculty changing and designing new courses/programs. The information will be used to assess the resources available in the library, and to identify resources the library should acquire to support the course program. The information will also provide rationale for institutional support for library acquisitions.

This form should be completed in a coordinated effort between the course sponsor(s) and the academic department liaison librarian. THIS FORM MUST BE COMPLETED FOR ALL CURRICULUM PROPOSALS.

- The sponsor(s) complete parts A & B. Lib assistance is required to complete parts A & B; please notify the liaison librarian.
- Forward this form to the librarian who will complete parts C, D & E.

*This form must be completed and attached to the original curriculum proposal before being approved by the Senate Curriculum Committee*

A. College LAS Department: Computer Science  
 Proposed by: Seth Bergmann Date: Oct. 10, 2004  
 Course Title: Computer Cryptography  
 Anticipated Date for Course/Program Offering: Fall '05

B. List specific resources that should be acquired to support this course.  
 Bruce Schneier Applied Cryptography (Wiley)  
 Jonathan Knudsen Java Cryptography (O'Reilly)  
 Scott Oaks Java Security (O'Reilly)  
 Journal - 'Communications of the ACM'

C. Describe the resources available in the library to support this course/program, including reference, monographic, electronic databases, audio-visual materials, etc. A summary statement is sufficient.

D. List key periodicals available in the library to support this course/program

E. Librarian comments and recommendations

*Library has the materials to support this class.*

Name: LIBRARIAN LIAISON John Mullens Librarian Signature: John Mullens



*Electrical and Computer Engineering*

October 11, 2004

Professor Seth Bergmann  
Computer Science Department  
Rowan University  
Glassboro, NJ 08028

Re: Computer Cryptography

Dear Professor Bergmann:

The Electrical & Computer Engineering department has received your course proposal entitled "Computer Cryptography." We have reviewed the rationale, curricular effect and proposed course content and are pleased to support this course offering.

Best wishes,

Shreekanth Mandayam, Ph.D.  
Associate Professor  
ECE Curriculum Committee Chair

Cc: Dr. Jennifer Kay, Chair, CS  
Dr. John Schmalzel, Chair, ECE

**From:** Christopher Smyth Simons  
**To:** Seth Bergmann  
**Date:** 9/21/04 10:20AM  
**Subject:** letter of consultation

Greetings,

Seth Bergman's proposal is excellent. This computer science oriented cryptography course fills an important need in the University's curriculum.

css

Christopher S. Simons, Ph.D.  
Mathematics Department, Rowan University, Glassboro NJ 08028  
Email: [simons@rowan.edu](mailto:simons@rowan.edu)

>>> Seth Bergmann 09/10/04 04:28PM >>>

To: Jooh Lee, Mgmt & MIS  
John Schmalzel, ECE  
Chris Simons, Math

I recently sent you a course proposal (Computer Cryptography) through the campus mail, and it now occurs to me that I forgot to enclose a cover letter. I am simply listing you as a 'consultant' on this proposal. If you care to respond, email or paper is fine. If you have any questions or concerns, don't hesitate to contact me.

Sincerely,

Seth D. Bergmann                      [bergmann@rowan.edu](mailto:bergmann@rowan.edu)  
Associate Professor                    tel: 856-256-4500 ext. 3197  
Computer Science Department        fax: 856-256-4741  
Rowan University                        [www.rowan.edu/~bergmann](http://www.rowan.edu/~bergmann)  
Glassboro, NJ 08028

Office: Robinson 3rd floor

>Subject: Course Proposal Consultation  
>Date: Tue, 5 Oct 2004 09:10:18 EDT  
>From: RSFHAZMAT@aol.com  
>To: kay@elvis.rowan.edu  
>CC: fleming@rowan.edu, RSFHAZMAT@aol.com  
>  
>Jennifer:  
>  
>Thank you for affording the Management/MIS Department the opportunity to  
>review and comment on your course proposal for /Computer Cryptography/.  
>  
>I have discussed the proposed course with our MIS faculty and we have no  
>reservations in supporting this course.  
>  
>Bob Fleming  
>Chairman  
>Management/MIS Department

Dear Seth,

We reviewed your proposal and identified no concerns. I hope you received a supporting consultation letter from Bob Fleming. If you have not receive it, please let me know.

Thanks, Dan.

Daniel J. McFarland, Ph.D.

Associate Professor, MIS

Rowan University

201 Mullica Hill Road

Glassboro, NJ 08028

Tel. 856.256.5426 Fax 856.256.4439

>>> "Seth Bergmann" <Bergmann@rowan.edu> 10/01/04 11:56 AM >>>

Sorry, Bob, the Rowan web site has Jooh Lee listed as department chair. I am attaching the proposal in case you didn't get the copy from Diane.

Thanks in advance,

Seth D. Bergmann

Associate Professor

Computer Science Department

Rowan University

bergmann@rowan.edu

tel: 856-256-4500 ext. 3197

fax: 856-256-4741

www.rowan.edu/~bergmann

Glassboro, NJ 08028

Office: Robinson 3rd floor

>>> <RSFHAZMAT@aol.com> 10/01/04 10:56AM >>>

Seth:

Sorry we have not responded but this is the first I have heard of this.

Providing a consultation in a timely manner should not be a problem.

Please send a copy of the proposal as an e-mail attachment to Diane and me

ASAP.

Thanks,

Bob Fleming