Chair: Tracy Christofero

GC#6: Course Addition

Request for Graduate Course Addition

1. Prepare one paper copy with all signatures and supporting material and forward to the Graduate Council Chair.
2. E-mail one identical PDF copy to the Graduate Council Chair. If attachments included, please merge into a single file.
3. ***The Graduate Council cannot process this application until it has received both the PDF copy and the signed hard copy.***

College: CITE Dept/Division: Computer Science Alpha Designator/Number: CYBR/625 ● Graded ○ CR/NC

Contact Person: Dr. Wook-Sung Yoo Phone: x5452

NEW COURSE DATA:

New Course Title: Cybersecurity Policies and Management

Alpha Designator/Number: C Y B R / 6 2 5

Title Abbreviation: A p p l i e d C r y p t o g r a p h y

(Limit of 25 characters and spaces)

Course Catalog Description: (Limit of 30 words) This course introduces fundamentals of cryptography, including classical ciphers, Shannon's perfect secrecy, DES, AES, public-key crypto (RSA), as well as advanced cryptographic schemes

Co-requisite(s): None First Term to be Offered: Spring 2020

Prerequisite(s): None Credit Hours: 3

Course(s) being deleted in place of this addition (*must submit course deletion form*): NA

Signatures: if disapproved at any level, do not sign. Return to previous signer with recommendation attached.

Dept. Chair/Division Head Yoo, wook Date 9/17/18

Registrar 110101 Date 9/21/18

College Curriculum Chair Date 9/26/18

Graduate Council Chair Date

Request for Graduate Course Addition - Page 2

College: CITE Department/Division: Computer Science Alpha Designator/Number: CYBR/625

Provide complete information regarding the new course addition for each topic listed below. Before routing this form, a complete syllabus also must be attached addressing the items listed on the first page of this form.

1. FACULTY: Identify by name the faculty in your department/division who may teach this course.

Paulus Wahjudi, Ph.D.
Wook-Sung Yoo, Ph.D.

2. DUPLICATION: If a question of possible duplication occurs, attach a copy of the correspondence sent to the appropriate department(s) describing the proposal. Enter "***Not Applicable***" if not applicable.

Not Applicable

3. REQUIRED COURSE: If this course will be required by another deparment(s), identify it/them by name. Enter "***Not Applicable***" if not applicable.

Not Applicable

4. AGREEMENTS: If there are any agreements required to provide clinical experiences, attach the details and the signed agreement. Enter "***Not Applicable***" if not applicable.

Not Applicable

5. ADDITIONAL RESOURCE REQUIREMENTS: If your department requires additional faculty, equipment, or specialized materials to teach this course, attach an estimate of the time and money required to secure these items. (Note: Approval of this form does not imply approval for additional resources.) Enter "***Not Applicable***" if not applicable.

Not Applicable

6. COURSE OBJECTIVES: (May be submitted as a separate document)

Please see attached document

Request for Graduate Course Addition - Page 3

7. COURSE OUTLINE (May be submitted as a separate document)

Please see attached document

8. SAMPLE TEXT(S) WITH AUTHOR(S) AND PUBLICATION DATES (May be submitted as a separate document)

Please see attached document

9. EXAMPLE OF INSTRUCTIONAL METHODS (Lecture, lab, internship)

Please see attached document

Request for Graduate Course Addition - Page 4

10. EXAMPLE EVALUATION METHODS (CHAPTER, MIDTERM, FINAL, PROJECTS, ETC.)

Exam, Homework Assignments and Projects

11. ADDITIONAL GRADUATE REQUIREMENTS IF LISTED AS AN UNDERGRADUATE/GRADUATE COURSE

Not applicable

12. PROVIDE COMPLETE BIBLIOGRAPHY (May be submitted as a separate document)

Please see attached document

Request for Graduate Course Addition - Page 5

Please insert in the text box below your course summary information for the Graduate Council agenda. Please enter the information exactly in this way (including headings):

Department:
Course Number and Title:
Catalog Description:
Prerequisites:
First Term Offered:
Credit Hours:

Department: Computer Science
Course Number and Title: CYBR 625 Applied Cryptography
Catalog Description: This course introduces fundamentals of cryptography, including classical ciphers, Shannon's perfect secrecy, DES, AES, public-key crypto (RSA), as well as advanced cryptographic schemes.
Prerequisites: None
First Term Offered: Spring 2020
Credit Hours: 3

BIBLIOGRAPHY

"Cryptography: Theory and Practice", 3rd Edition, by Douglas Stinson; Chapman and Hall/CRC; 3 edition (November 1, 2005), ISBN-10: 1584885084/ISBN-13: 978-1584885085

"Introduction to Modern Cryptography", 2nd Edition, by Jonathan Katz, Yehuda Lindell; Chapman and Hall/CRC, 2 editio; ISBN-13: 978-1466570269/ISBN-10: 1466570261

"Handbook of Applied Cryptography", 1st Edition, by Alfred Menezes, Paul van Oorschot, Scott Vanstone; CRC Press; 1 edition (October 16, 1996), ISBN-10: 0849385237/ISBN-13: 978-0849385230

CYBR 625 Applied Cryptography

Course Title/Number	Applied Cryptography/625
Semester/Year	Spring/2020
Days/Time	TBD
Location	TBD
Instructor	TBD
Office	TBD
Phone	TBD
E-Mail	TBD
Office Hours	TBD
University Policies	By enrolling in this course, you agree to the University Policies listed below. Please read the full text of each policy by going to www.marshall.edu/academic-affairs and clicking on "Marshall University Policies." Or, you can access the policies directly by going to www.marshall.edu/academic-affairs/policies/. Academic Dishonesty/Excused Absence Policy for Undergraduates/Computing Services Acceptable Use/Inclement Weather/Dead Week/Students with Disabilities/Academic Forgiveness/Academic Probation and Suspension/Academic Rights and Responsibilities of Students/Affirmative Action/Sexual Harassment

Course Description

This course introduces fundamentals of cryptography, including classical ciphers, Shannon's perfect secrecy, DES, AES, public-key crypto (RSA), as well as advanced cryptographic schemes.

Course Student Learning Outcomes

Course Student Learning Outcomes	How students will practice each outcome in this Course	How student achievement of each outcome will be assessed in this Course
An ability to understand modern cryptographic primitives	Homework assignments, In class examples, Group discussions	Graded exam problems Graded homework assignments
An ability to analyze the security strength of a given cryptographic scheme	Homework Assignments, In class examples Group discussions	Graded exam problems Graded homework assignments
An ability to apply cryptographic primitives in designing software, protocols	Homework, In class examples	Graded exam problems Graded homework assignments

Course Schedule

This is the list of topics. This could be adjusted as the semester progresses at the discretion of the instructor. Lecture slides will be posted to MUOnline.

Week	Schedule
1	Introduction to Course
2	Mathematical Background: Number Theory
3	Mathematical Background: Probability Theory and Complexity Theory
4	Perfect Secrecy
5	Secret Key Encryption: Stream Cipher, Block Cipher
6	Secret Key Encryption: Message Integrity and Authentication
7	Midterm Exam
8	Pseudo-random Number Generator
9	Key Establishment and Distribution
10	Public Key Infrastructure: RSA
11	Public Key Infrastructure: Digital Signatures
12	Security Protocols
13	Using Cryptographic Primitives
14	Advanced Cryptographic Schemes: Cryptocurrency
15	Advanced Cryptographic Schemes: Secret Sharing and Secure Computation

Required Texts, Additional Reading, and Other Materials

Required Text

Douglas Stinson, Cryptography: Theory and Practice, 3rd Edition, Chapman and Hall/CRC; 3 edition (November 1, 2005), ISBN-10: 1584885084/ISBN-13: 978-1584885085

Other Materials

Jonathan Katz, Yehuda Lindell, Introduction to Modern Cryptography, Chapman and Hall/CRC; 2 edition, ISBN-13: 978-1466570269/ISBN-10: 1466570261

Alfred Menezes, Paul van Oorschot, Scott Vanstone, Handbook of Applied Cryptography, CRC Press; 1 edition (October 16, 1996), ISBN-10: 0849385237/ISBN-13: 978-0849385230

Course Requirements / Due Dates

Midterm Examinations

Midterm exam is during regular class hours in Week 8.

Homework Assignments

Homework problems will be assigned bi-weekly (starting from week 2)

Attendance Policy

Missing more than 3 classes will result in a 10 points reduction from your final grade.

Grading Policy

Activity	Points
Attendance	10
Midterm Exam	30
Homework Assignments	30
Final Exam	30
Total	100

Course grades are awarded based on the following scheme:

Score	Letter Grade
>= 90	A
>= 80 & < 90	B
>= 70 & < 80	C
>= 60 & < 70	D
< 60	F