Washtenaw Community College Comprehensive Report

CSS 201 Introduction to Cryptography
Effective Term: Fall 2017

Course Cover

Division: Business and Computer Technologies
Department: Computer Instruction
Discipline: Computer Systems Security
Course Number: 201
Org Number: 13400
Full Course Title: Introduction to Cryptography
Transcript Title: Introduction to Cryptography
Is Consultation with other department(s) required: No
Publish in the Following: College Catalog , Time Schedule , Web Page
Reason for Submission: New Course
Change Information:
Rationale: This course is required for to our new Cybersecurity transfer degree and to satisfy "knowledge unit A-7 Intro to Cryptography" from National NSA/DHS Centers of Academic Excellence in Information Assurance/Cyber Defense.
Proposed Start Semester: Fall 2017
Course Description: In this course, students are introduced to the terminology, concepts, and application of cryptography in digital communications. Topics such as algorithms, encryption protocols, message integrity and authentication using hash functions will be discussed.

Course Credit Hours

Variable hours: No
Credits: 3
Lecture Hours: Instructor: 45 **Student:** 45
Lab: Instructor: 0 **Student:** 0
Clinical: Instructor: 0 **Student:** 0

Total Contact Hours: Instructor: 45 **Student:** 45
Repeatable for Credit: NO
Grading Methods: Letter Grades
Audit
Are lectures, labs, or clinicals offered as separate sections?: NO (same sections)

College-Level Reading and Writing

College-level Reading & Writing

College-Level Math

No Level Required

Requisites

Prerequisite
MTH 160
or Academic Math Level 3
and

Prerequisite
CSS 200 minimum grade "C"; may enroll concurrently
and
Prerequisite
CIS 161 minimum grade "C"

General Education

Request Course Transfer

Proposed For:
Eastern Michigan University

Student Learning Outcomes

1. Identify the elements of a cryptographic system.
   Assessment 1
   Assessment Tool: Laboratory report(s)
   Assessment Date: Fall 2019
   Assessment Cycle: Every Three Years
   Course section(s)/other population: A random sample of a minimum of two sections over the assessment period.
   Number students to be assessed: All students in the select sections.
   How the assessment will be scored: The lab report(s) are scored and evaluated with department-developed rubric.
   Standard of success to be used for this assessment: At least 75% of students must score 75% or better.
   Who will score and analyze the data: Department Faculty and external sources (if available)

2. Describe the differences between symmetric and asymmetric algorithms.
   Assessment 1
   Assessment Tool: Department-developed final exam.
   Assessment Date: Fall 2019
   Assessment Cycle: Every Three Years
   Course section(s)/other population: A random sample of a minimum of two sections over the assessment period.
   Number students to be assessed: All students in the select sections.
   How the assessment will be scored: Exams are scored and evaluated with department-developed rubric.
   Standard of success to be used for this assessment: At least 75% of students must score 75% or better.
   Who will score and analyze the data: Department Faculty and external sources (if available)

3. Describe which cryptographic protocols, tools, and techniques are appropriate for given scenarios.
   Assessment 1
   Assessment Tool: Department-developed final exam.
   Assessment Date: Fall 2019
   Assessment Cycle: Every Three Years
   Course section(s)/other population: A random sample of a minimum of two sections over the assessment period.
   Number students to be assessed: All students in the select sections.
   How the assessment will be scored: Exams are scored and evaluated with department-developed rubric.
   Standard of success to be used for this assessment: At least 75% of students must score 75% or better.

Who will score and analyze the data: Department Faculty and external sources (if available)

4. Describe the issues that have to be addressed in the implementation cryptography.

Assessment 1

Assessment Tool: Department-developed final exam.
Assessment Date: Fall 2019
Assessment Cycle: Every Three Years
Course section(s)/other population: A random sample of a minimum of two sections over the assessment period.
Number students to be assessed: All students in the select sections.
How the assessment will be scored: Exams are scored and evaluated with department-developed rubric.
Standard of success to be used for this assessment: At least 75% of students must score 75% or better.
Who will score and analyze the data: Department Faculty and external sources (if available)

Course Objectives

1. Describe the elements of a cryptographic system: confidentiality, integrity, and authentication.
2. Describe historical approaches used to implement cryptographic systems.
3. Describe the protocols and algorithms required to implement current cryptographic system.
4. Identify the elements necessary to implement symmetric encryption.
5. Identify the elements necessary to implement asymmetric encryption.
6. Describe benefits and shortcomings of both encryption algorithms.
7. Describe hashing algorithms and their use in cryptographic systems.
8. Describe how message authentication and message integrity is implemented using hashing functions.
9. Describe how public key cryptography is implemented.
10. Describe the implementation of digital signatures.
11. Describe the types of attacks against cryptographic systems.
12. Describe the key exchange problem inherent in symmetric encryption.
13. Describe public key cryptography is used for encryption and non-repudiation.

New Resources for Course

No additional resources are required.

Course Textbooks/Resources

Textbooks

William Stallings. *Cryptography and Network Security*, 6 ed. Pearson, 2013, ISBN: 978-013335469.
Fred Piper & Sean Murphy. *Cryptography: A Very Short Introduction*, ed. Oxford University Press, 2002

Manuals
Periodicals
Software

Equipment/Facilities

Level I classroom
Computer workstations/lab

Reviewer	Action	Date
Faculty Preparer:		
Michael Galea	*Faculty Preparer*	*Jan 14, 2017*
Department Chair/Area Director:		
Philip Geyer	*Recommend Approval*	*Feb 27, 2017*
Dean:		

Kimberly Hurns	*Recommend Approval*	*Feb 28, 2017*
Curriculum Committee Chair:		
David Wooten	*Recommend Approval*	*Mar 16, 2017*
Assessment Committee Chair:		
Ruth Walsh	*Recommend Approval*	*Mar 19, 2017*
Vice President for Instruction:		
Kimberly Hurns	*Approve*	*Mar 23, 2017*