Spring 2012-2013
CSC-650, Cryptography, Three Credit Hours
Syllabus

CLASS MEETINGS

Monday, 6 – 9 pm, Robinson Tech Center, Room 300

INSTRUCTOR

Dr. George Hsieh, Associate Professor, Department of Computer Science
Office Hours: Monday 4 – 6 pm, Tuesday 2 – 3 pm, Wednesday 11 am – noon
Room 320-M, Robinson Tech Center
(757) 823-8313, ghsieh@nsu.edu, hsiehgeo@yahoo.com
Computer Science Department: RTC Room 320, (757) 823-9454

DESCRIPTION

One course study of historical and modern cryptographic techniques and algorithms. Topics include symmetric and asymmetric key cryptography, one-way functions, secure hash functions, digital signatures, key exchange, authentication, key management, PKI, DES, AES (Rijndael), current topics.

PREREQUISITE: Instructor approval

COURSE RATIONALE

CSC-650 is one of the recommended courses for Information Assurance track of the MS in Computer Science degree. It covers one of the most critical technological foundation for information assurance: cryptography and the numerous applications of cryptography. The CSC-650 course is designed to explore the concepts and principles of cryptography, the different functional branches of cryptography, and the most common application domains for cryptography.

GOALS:

1. To introduce students to concepts, principles, functional building blocks, and applications of modern cryptography.
2. To enable students to gain knowledge, skill, and hands-on experience in working with industry standard cryptography software and practices.

By the end of the course, students will be able to

1. Describe the needs and benefits of cryptography.
2. Explain the different functional building blocks of cryptography.
3. Describe the concepts and principles for symmetric cryptography and the commonly used standard algorithms (such as DES, AES) in this category.
4. Describe the concepts and principles for asymmetric cryptography and the commonly used standard algorithms (such as RSA) in this category.
5. Explain the cryptography-based methods for integrity assurance such as hash functions.
6. Describe the cryptography-based methods for authentication such as secure hash functions and digital certificates.
7. Explain the key management requirements and solutions such as Public Key Infrastructure (PKI) and key agreement schemes.
8. Use Java Cryptographic Extension (JCE) and Java security service providers to implement security features in Java applications.

TEXTBOOKS

- ***Understanding Cryptography: A Textbook for Students and Practitioners*, by Christof Paar and Jan Pelzl, Springer, 2010, ISBN 978-3-642-04110-6. [Available online free of charge via NSU Library][Online Resource: http://wiki.crypto.rub.de/Buch/index.php]**

- ***Beginning Cryptography with Java,* by David Hook, Wrox/Wiley Publishing, 2005, ISBN 0-7645-9633-0.**

REFERENCES

- ***Cryptography: Theory and Practice*, Third Edition, by Douglas R. Stinson, Chapman & Hall/CRC, 2006, ISBN 1-58488-508-4.**

PRIMARY METHODS OF INSTRUCTION

Methods include lecture, reading, homework and programming assignments, term projects.

COURSE OUTLINE/CALENDAR

Date	Topic	Reading Assignment
WEEK 1	Introduction to Cryptography	Chapter 1
WEEK 2	Stream Ciphers	Chapter 2
WEEK 3	Data Encryption Standards (DES) and Alternatives	Chapter 3
WEEK 4	Advanced Encryption Standard (AES)	Chapter 4
WEEK 5	Block Ciphers and Modes of Operation	Chapter 5
WEEK 6	Labs and Projects	
WEEK 7	Introduction to Public Key Cryptography	Chapter 6
WEEK 8	RSA Cryptosystem	Chapter 7
WEEK 9	Diffie-Hellman Key Exchange	Chapter 8
WEEK 10	Elliptic Curve Cryptosystems	Chapter 9
WEEK 11	Labs and Projects	
WEEK 12	Digital Signatures	Chapter 10
WEEK 13	Hash Functions	Chapters 11
WEEK 14	Message Authentication Codes & Key Establishment	Chapters 12 & 13
WEEK 15	Labs and Projects	

* The schedule is subject to change at the discretion of the instructor or depending upon the progress of the class.

EVALUATION METHODS

- Homework and Lab Assignments…..…….…..…..... 50%
- Term Projects…..……...……... 40%
- Attendance & Class Participation……. 10%

ACADEMIC INTEGRITY STANDARDS

The Computer Science Department adheres to the University Policy on class attendance and University Standards on Honesty and Honor Code. The Department also requires students to adhere to the Association of Computing Machinery (ACM) Code of Conducts. In addition, students are required to follow classroom rules. Turn off cell phones. No side conversations, instant messaging, emailing, unauthorized web surfing, or other disruptive behaviors. On-time submission of assignments and tests is required; otherwise, penalty or forfeiture will be assessed.

AMERICANS WITH DISABILITIES ACT (ADA) STATEMENT

In accordance with Section 504 of the 1973 Rehabilitation Act and the Americans with Disabilities Act (ADA) of 1990, if you have a disability or think you have a disability, contact Supporting Students through Disabilities Services (SSDS) for information regarding programs and services to enhance student success.

Location: 2nd Floor/Lyman B. Brooks Library, Room 240
Contact Person: Marian E. Shepherd, Disability Services Coordinator
Telephone: 757-823-2014

UNIVERSITY ASSESSMENT

As part of NSU's commitment to provide the environment and resources needed for success, students may be required to participate in a number of university-wide assessment activities. The activities may include tests, surveys, focus groups, interviews, and portfolio reviews. The primary purpose of the assessment activities is to determine the extent to which the university's programs and services maintain a high level of quality and meet the needs of students. Students will not be identified in the analysis of results. Unless indicated otherwise by the instructor, results from University assessment activities will not be computed in student grades.

RELATED UNIVERSITY-WIDE AND COURSE-SPECIFIC REQUIREMENTS

This course emphasizes critical thinking and problem-solving.