MCS 597C-1 Cryptography

Instructor: Henry Brooks
E-Mail: brook057@cougars.csusm.edu

Online via Zoom
Monday 5:30 - 8:15pm
Wednesday 5:30 - 8:15pm

Session: 6/1/20 - 8/8/20
Final: Wednesday 8/8/20 @ 5:30pm

Course Description

Fundamentals of protecting confidentiality, integrity and availability of information in computer systems. This course covers the fundamentals of cryptographic concepts and methods. Several encryption/decryption algorithms will be discussed. The topics include an introduction to the mathematics behind cryptography; cryptographic algorithms including classical methods, symmetric key systems, public key systems,hash functions, digital signatures and certificates; cryptanalysis and attacks; and access control including authentication and authorization. Assignments include lab projects to apply public keys, dictionary attacks, digital signatures, and certificates.

Course Prerequisites

Graduate student status in the Master of Science in Cybersecurity,a Professional Science Master's program.

Course Objectives

- To provide the student with knowledge of the fundamental principles of cryptography
- Describe the uses of encryption in the field of cybersecurity
- Understand the use of encryption to address common cybersecurity threats and vulnerabilities
- Understand classic encryption techniques
- Understand common modern encryption standards
- Describe the application of encryption to common activities by use of public-key systems, cryptographic hash functions, digital signatures
- Understand the applied use of cryptography inaccess control, authentication, and network transportation

Required Text

Cryptography and Network Security: Principles and Practice, 7th Edition, Pearson, ISBN-13: 978-0134444284

Student Learning Outcomes

Upon successful completion of the course, students will be able to:

- Present an overview of the main concepts of symmetric cryptography.
- Understand the distinction between stream ciphers and block ciphers.
- Present an overview of Data Encryption Standard (DES).
- Summarize the principal block cipher design principles.
- Present an overview of the general structure of Advanced Encryption Standard (AES).
- Analyze the security of multiple encryption schemes.
- Present an overview of the basic principles of public-key cryptosystems.
- Present an overview of the RSA algorithm.
- Understand the man-in-the-middle attack.
- Summarize the applications of cryptographic hash functions.
- Present an overview of the digital signature process.
- Present an overview of public-key infrastructure concepts.

Assessment

Assignments	Points
Quizzes	250
HW Assignments	300
Lab Projects	200
In-class Activities	150
Final	100
Total points	1000

Quizzes (25% of the course grade)

There will generally be a “subject knowledge” quiz after each class.Each quiz may contain T/F, multiple choice, and/or short-answer questions. Most quiz questions will relate to the recent homework but may include anything we’ve studied or discussed in class. Quizzes are intended to demonstrate understanding of the assigned readings and class discussions. Unless otherwise noted, quizzes are open book, open notes. Use the web to help find answers to questions. Quizzes are untimed.

HW Assignments (30% of the course grade)

Students will complete six homework assignments to reinforce the understandings of cryptography concepts and principles. Typically, there will be one homework assignment per week.

Lab Projects (20% of the course grade)

There will be two lab projects that will help students gain a hands-on experience on encryption algorithms, encryption modes, and public key infrastructure. Students will be able to use tools to encrypt/decrypt messages, to understand how public key infrastructure works, how it is used to protect the Web, and how Man-in-the-middle attacks can be defeated by public key infrastructure. The lab projects will be done in a virtual machine environment and a lab report is expected for each lab project.

In-class Activities (15% of the course grade)

Interaction and participation are important elements of learning. Although lectures are recorded most of the time, you are expected to participate in online activities. We recognize that schedules and time-zones may impact an individual's ability to participate in every online session, but students must arrange to participate at minimum in 50% of the online sessions or, arrange an alternate participation strategy with the instructor. An alternate participate strategy may consist of recording voice or video commentary or questions, posting and answering discussion forum topic or similar activity. Examples of typical participation in the online activities consist of discussing the assignments and lecture topics, answering assigned questions, and general conduct as one would see in a classroom.

Final (10% of the course grade)

The final will be a written exam to demonstrate your overall understanding of the major topics covered in this class, your ability to analyze and solve different cryptographic problems

Grading

Grades will be assigned based on the cumulative score for all the coursework.

From	To	Grade
933	1000	A
900	932	-A
866	899	+B
833	865	B
800	832	-B
766	799	+C
733	765	C
700	732	-C
666	699	+D
633	665	D

Students with Disabilities Requiring Reasonable Accommodations

Students with disabilities who require reasonable accommodations must be approved for services by providing appropriate and recent documentation to the Office of Disable Student Services (DSS). This office is located in Craven Hall 4300, and can be contacted by phone at (760) 750-4905, or TTY (760) 750-4909. Students authorized by DSS to receive reasonable accommodations should contact me via email or phone in order to discuss the accommodations.

Grading Standard

All students must come to virtual class with reading and other assignments completed. The in-class activities will depend on students having completed the assignments prior to class. Missed quizzes may not be “made up” as we may be discussing quiz content in the session immediately following the quiz. All required work is expected to be on time. Unless prior instructor approval is secured, assignments will not be accepted after they are due. Exceptions will be handled on a case-by-case basis, as determined by the instructor and points will be deducted for these exceptions. HW assignments and lab projects will be graded on a rubric developed by the instructor based on the provided deliverables. It is important that all deliverables identified in the assignment and lab handout have been addressed.

CSUSM Academic Honesty Policy

> *Each student shall maintain academic honesty in the conduct of his or her studies and other learning activities at CSUSM. The integrity of this academic institution, and the quality of the education provided in its degree programs, are based on the principle of academic honesty.*
>
> *The maintenance of academic integrity and quality education is the responsibility of each student within this university and the California State University system. Cheating and plagiarism in connection with an academic program at a campus is listed in Section 41301, Title 5, California Code of Regulations, as an offense for which a student may be expelled, suspended, put on probation, or given a less severe disciplinary sanction.*

Incidents of Academic Dishonesty will be reported to the Dean of Students. Sanctions at the University level may include suspension or expulsion from the University.

CSUSM Academic Honesty Policy

Plagiarism

I expect each student will do his/her own work, and contribute equally to group-based discussion and/or processes. Plagiarism or cheating is unacceptable under any circumstances. If you are in doubt about whether your work is paraphrased or plagiarized see the Plagiarism Prevention for Students website http://library.csusm.edu/plagiarism/index.html. If there are questions about academic honesty, please consult the University catalog.

Communication

If you have a question about the assignments, materials, concepts and so on, please post that question to the forum. I will check the forum daily and respond to any question not adequately addressed by others in the class. Please note that you are encouraged to respond to each other's forum questions and posts. As mentioned above, online interactions may qualify as participation for that element of your grade.

If you need to contact me about a personal issue, please use email. It is my intention to respond to all email I receive on the day (it may be evening!) which I receive it. When someone asks a question or makes a comment via email that may be relevant to others, I will very likely post both the question and response in the forum in CougarCourses after removing the sender's identity information. No participation points will be assigned for relevant general questions sent to me via email instead of being posted. This is intended to encourage forum participation