MCS 597C-1 Cryptography

Instructor: Henry Brooks

E-Mail: hbrooks@csusm.edu

Online via Zoom

Monday 7 - 8:20pm

Wednesday 7 - 8:20pm

Session: 1/24/22 - 5/22/22

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 in access control, authentication, and network transportation

Required Text

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

Supplimental Text

Computer & Internet Security: A Hands-on Approach, 2nd Edition, Wenliang Du, ISBN-13: 978-1733003933

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 conc

Assessment

Assignments	Points
Quizzes	300
Assignments	500
In-class Activities	200
Total points	1000

Quizzes (30% of the course grade)

There will generally be a “subject knowledge” quiz every two weeks. Each quiz may contain T/F, multiple choice, short-answer and/or essay questions. Most quiz questions will relate to the recent content 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.

Assignments (50% of the course grade)

There will be briefings or other written assignments for the knowledge and analysis work. We will use these to analyze events, develop products and study current events and topics. These typically involve reading/research resulting in a 2-3 page analysis report or product such as policy/standard. The All-University Writing Requirement (850 words for a 1-unit course, 1700 words for a 2-unit course, and 2500 words for courses of 3 or more units) is satisfied in this course through classroom activities and the major assignments.

In-class Activities (20% of the course grade)

An important part of an information security professional's job is explaining and discussing concepts. In this class you will demonstrate this capability by answering the assigned questions when called upon in class. You will not be required to answer every question, every class – but you must be prepared to do so.

Attendance and Participation

This class uses CougarCourses along with Zoom. Some lectures may be recorded, but you are required to attend the live sessions in order to receive credit for the in-class 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.

Credit Hour Policy Statement

Per the University Credit Hour Policy: Students are expected to spend a minimum of two hours outside of the classroom each week for each unit of credit. This 3-unit class will require a minimum of six hours each week, in addition to recorded lectures and synchronous sessions.

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

From	To	Grade
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 Disability Support Services (DSS) Office. This office is located in Craven Hall 4300, and can be contacted by phone at (760) 750-4905, or TTY (760) 750-4909, and by email sent to dss@csusm.edu. Students authorized by DSS to receive reasonable accommodations should meet with me during my office hours in order to ensure confidentiality.

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

> *"Students will be expected to adhere to standards of academic honesty and integrity, as outlined in the Student Academic Honesty Policy. All written work and oral presentation assignments must be original work. All ideas/materials that are borrowed from other sources must have appropriate references to the original sources. Any quoted material should give credit to the source and be punctuated with quotation marks.*
>
> *Students are responsible for honest completion of their work including examinations. There will be no tolerance for infractions. If you believe there has been an infraction by someone in the class, please bring it to the instructor's attention. The instructor reserves the right to discipline any student for academic dishonesty in accordance with the general rules and regulations of the university. Disciplinary*

> *action may include the lowering of grades and/or the assignment of a failing grade for an exam, assignment, or the class as a whole."*

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 students 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 students 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 the grade.

If students 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.

Electronic messages (email, forum posts) need not be formal, but they must be professional. Gross disregard for grammar, spelling and the need for punctuation is not acceptable in a professional environment -so let's get used to it now. When we start talking about legal and ethical issues, there is a great deal of room for interpretation and disagreement. These discussions are encouraged, and being able to disagree with someone without offending them (or becoming offended) is an important skill. But all such communications needs to be thoughtful, respectful, impersonal and constructive.