CPSC 352 -- *Cryptography*

Spring 2024, Mikhail Gofman

Faculty Information

Instructor: Mikhail I. Gofman, Ph.D., Certified Information System Security Professional (CISSP)
Office: CS-104
Phone: (657) 278-7304
Email: mgofman@fullerton.edu
Office hours: Monday, Tuesday, Thursday 4:15 pm – 6:45 pm or by appointment (please email me)
Response time: I will strive to respond to email questions immediately (this includes weekends and holidays) and no later than within 24 hours.

Course Information

CPSC 352 – Cryptography (3 units)
Section 01
Canvas URL: https://csufullerton.instructure.com/courses/3427174
Modality: In-Person with no more than 20% of class offered remotely through Zoom
Meeting Days/Times: Mondays 7:00 pm – 9:45 pm
Place: CS-104
Zoom: https://fullerton.zoom.us/j/86013706284?pwd=UkYvZFJ6TkZMWjU4UnFlWWN6ODhMUT09
(password: 2Ji=cya`9v)

Course requisite(s): MATH 170B, CPSC 131, CPSC 253; Computer Science or Computer Engineering major or minor; or Computer Science or Computer Engineering graduate standing.
The course is not available for graduate credit. Also, **familiarity with basic Unix and C++ is assumed.**

Catalog description: Introduction to cryptography and steganography. Encryption, cryptographic hashing, certificates, and signatures. Classical, symmetric-key, and public-key ciphers. Block modes of operation. Cryptanalysis including exhaustive search, man-in-the-middle, and birthday attacks. Programing projects involving implementation of cryptographic systems.

Additional description: Cryptology is the art and science of making and breaking secret codes. It is essential for cybersecurity, as it allows us to safeguard our data from unauthorized use, change, or exposure. Cryptology has a long and fascinating history, from the ancient ciphers used by various cultures, to the modern ciphers that let us communicate, shop, and surf online securely. Cryptology also covers the study of steganography, which is the method of concealing messages in plain sight.

In this course, you will discover the basic concepts and methods of cryptology, as well as some of the advanced topics and applications. You will also acquire hands-on experience in encrypting, decrypting, examining, and applying real-world ciphers. This course will equip you for various cybersecurity roles that demand cryptological skills and knowledge, such as

Cryptographer, Cryptoanalyst, Cyber Defense Analyst, Cyber Defense Forensics Analyst, Cyber Defense Infrastructure Support Specialist, Cyber Operator, and Cybersecurity Researcher.

Topics include history of cryptology, classical ciphers, steganography fundamentals, symmetric key encryption, public key encryption, security protocols, and their applications. The course will give you hands-on experience in encrypting, decrypting, analyzing, and implementing real-world ciphers.

Course materials and equipment:

Required text(s): None

Recommended text(s): William Stallings, *Cryptography and Network Security Principles and Practice*, Seventh Edition. ISBN-13: 9780134444284 ISBN: 013444428.

Other course materials and equipment: All slides and supplemental materials will be posted on Canvas.

You will also use two platforms for your exercises. The first one is Tuffix, which is a Linux-based environment that the department provides for programming. Tuffix supports g++, Java, Python, with the possibility of installing other languages. It can be either used as a virtual machine or can be installed natively. Please see the Tuffix instructional page for details and to receive assistance.

The second platform is TryHackMe, which is an interactive platform for learning ethical hacking skills. Most of the hacking exercises will use TryHackMe. You will get a temporary license from the instructor.

Student Learning Outcomes (SLO)

1. **Define** cryptography and identify the components of a cryptography system such as plaintext, key, and ciphertext. This will be assessed by a written assignment and exam.

2. **Compare** and **Contrast** symmetric and public key cryptographic systems. This will be assessed by a written assignment and exam.

3. **Describe** the mathematical principles and algorithms underpinning cryptographic tools and protocols. This will be assessed by a written assignment and exam.

4. **Describe** the structure and function of AES, DES, RSA, Diffie-Hellman, Elliptical Curve, and other security protocols. This will be assessed by a written assignment, exam, and the final project.

5. **Discuss** common symmetric key exchange protocols. This will be assessed by a written assignment and exam.

6. **Explain** Public announcement, public key authority, and public key certificates. This will be assessed by a written assignment and exam.

7. **Select** proper cryptographic mechanisms and protocols for solving a particular security problem. This will be tested by the final project as well as by practical TryHackMe exercises.

8. **Describe** the strengths and weaknesses of various cryptographic mechanisms and protocols. This will be assessed by a written assignment and exam.

9. **Evaluate** a security system based on the cryptographic mechanisms and protocols it uses. This will be assessed by a written assignment and exam.

10. **Implement** cryptographic applications such as file encryptors and digital signers. This will be assessed by a programming assignment and the final project.

11. **Describe** the applications of cryptography in Virtual Private Networks, Blockchains, and securing at-rest and in-motion data. This will be assessed by a written assignment, an exam, and the final project.

12. **Identify** flaws in cryptographic protocols. This will be assessed by a written assignment and exam.

13. **Describe** and **utilize** cryptographic protocols such as Secure Sockets Layer (SSL)/Transport Layer Security (TLS), Virtual Private Networks (VPNs), and Tor.

Notes on the Curriculum

This course strives to align with the curriculum for National Centers of Academic Excellence (CAE) in Cyber Defense, which is jointly sponsored by the National Security Agency (NSA) and the Department of Homeland Security (DHS). The CAE program recognizes and grants designations to academic institutions that offer rigorous and relevant cybersecurity programs that meet the needs of the public and private sectors.

This course also strives to align with the Workforce Framework for Cybersecurity (NICE Framework), which is developed by the National Institute of Standards and Technology (NIST) as part of the National Initiative for Cybersecurity Education (NICE). The NICE Framework provides a common language and structure to describe cybersecurity work and workers across various sectors and domains. It categorizes and defines the knowledge, skills, and abilities (KSAs) that are required for different cybersecurity work roles. Most importantly, both CAE-CD and NICE prioritize hands-on instruction.

By completing this course, you will learn the fundamental concepts and techniques of cryptology, as well as some of the advanced topics and applications. You will also gain hands-on experience in encrypting, decrypting, analyzing, and implementing real-world ciphers. Through platforms such as TryHackMe, you will learn applications of cryptography by setting up, configuring, attacking, and defining real-world systems and applications that rely on cryptography.

This course will prepare you for various cybersecurity roles that require cryptological skills and knowledge, such as Cryptographer, Cryptoanalyst, Cyber Defense Analyst, Cyber Defense Forensics Analyst, Cyber Defense Infrastructure Support Specialist, Cyber Operator, and Cybersecurity Researcher.

Grading Policy

a. **Attendance and participation policy:** You must attend every class and your attendance will be recorded at the beginning of each class. However, we will not take attendance for the first three weeks because new students may join the class during that period. You can miss one class without affecting your attendance grade. We urge you to participate actively in the class discussions and ask questions. Also, the hands-on exercises we do in class may be part of the assignments and exams. Therefore, it is very important that you attend every class.

b. **Absence Policy:** For an absence to be considered "excused," you must be able to document a valid reason for missing class, preferably in advance but always within 24 hours following the class and upon the instructor's request. Examples include medical documentation, a supervisor's note explaining a one-time necessity to be at work or somewhere else, and so on. The instructor determines the validity of the reason for being absent.

c. **Examinations:** All examinations are closed book and cumulative unless specified otherwise. Missed exams shall be dealt with according to University policies on incompletes and withdrawals (please see below). The tentative schedule for the examinations is given below

   Exam 1: 3/18/2024 in class

   Final Exam: 5/13/2024 7:00 pm – 8:50 pm in class (please also check with the Final Exam Schedule posted online)

d. **Handouts:** Handouts are designed to help you learn and apply the concepts and techniques of cryptology. They contain questions that will guide you through the lectures, review the material, prepare for examinations, and enhance your skills for interviews, certification exams, and real-world problems. Handouts are for your own benefit and will not be collected or graded. However, we strongly recommend that you complete them. Experience shows that students who complete handouts tend to perform better in the course.

e. **Make-up and late submission policy.** Consistent with UPS 300.005, no make-up assignments, including the exam or substitute essays, are given except "for reasons of illness, verified emergency, or other serious and compelling reasons approved by the instructor. The instructor must approve any make-up work.

f. **Assignments:** You will find all the assignments for this course on CANVAS. They will include both written, hands-on problem solving, and programming questions. You should work on them by yourself, unless the instructions say otherwise.

   You should use Tuffix for all the assignments, unless the instructions say otherwise. For programing assignments, you can choose from C, C++, Java, Python, or C# for the coding questions, unless the instructions say otherwise. On some assignments the language will be assigned.

You will use TryHackMe for all the ethical hacking exercises. TryHackMe is a platform that lets you learn ethical hacking skills in a fun and interactive way. You will get links to the TryHackMe rooms that you need through Canvas.

The due dates for all the assignments will be posted on Canvas throughout the semester. Assignments submitted less than 24 hours late shall be penalized with a 10% deduction. No assignments more than 24 hours late shall be accepted.

g. **Quizzes and Lab Exercises:** These are designed to help you practice and apply the concepts you learn in class. You can think of lab exercises as take-home quizzes. Your quiz and lab grades will be averaged together, and the lowest grade will be dropped. Some of the hands-on exercises will be administered through the TryHackMe platform that will allow you to practice hands-on cryptographic challenges.

   All in-class quizzes will be closed book. The questions will test your understanding of the material covered in class. If you miss an in-class quiz, you will get a zero grade, unless you have a valid excuse (such as a doctor's note) in writing. The instructor reserves the right to decide whether there will be in-class quizzes and may choose to replace them with lab exercises.

   Lab exercises will challenge you to think critically (and creatively!) and solve real-world problems using cryptology. You should submit your lab exercises on time, as late submissions will be penalized by 10%. No lab exercises will be accepted after 24 hours from the deadline.

h. **Final Project:** The final project is the culminating experience of the course. It challenges students to creatively apply their knowledge of cryptography to solve real-world security problems. The instructions for completing the project and the list of topics have been posted on Canvas. The topics are based on the real-world secure application development and system security problems students are likely encounter in the workplace. Successful completion of the project can help strengthen students' resume and to prepare students for security certification exams. **It is due at the end of the semester. Students are advised to start early and not wait until the end.**

i. **Grade breakdown.** Your course grade shall be calculated as follows:

Table 2: Grade Breakdown

Item	*Points = %*
Assignments (around 4)	25
Quizzes and Lab Exercises (around 3; may drop the lowest)	15
Attendance and Participation (may drop one absence)	3
Exam 1	20
Final Exam	22
Final Project	15
Total	**100**

The grade for each category (e.g., assignments, quizzes, etc) shall be an average of its constituents. The course grade shall be computed as weighted mean of all categories. A curve will then be applied in the form of additional points added to the overall average. The amount of curving shall be determined by the performance of the entire class as observed by the instructor.

j. **Grading Scale:** The course will be graded according to the following scale

Table 1: Grading Scale

Grade	*% or Points*
A+ = 4.0	98-100
A = 4.0	93-97
A- = 3.7	90-92
B+ = 3.3	87-89
B = 3.0	83-86
B- = 2.7	80-82
C+ = 2.3	77-79
C = 2.0	73-76
C- = 1.7	70-72
D+ = 1.3	67-69
D = 3.0	63-66
D- = 2.7	60-62
F = 0.0	0-59

k. **Authentication of student work:** We will use plagiarism tools and manual checks to verify the originality of your work. Your work will be compared with Google and other sources, as well as with other students' work. Moreover, the instructor may ask you to explain your work and make a decision if the instructor thinks that you copied or used ChatGPT or similar tools without citation.

l. **Penalty for academic dishonesty:** Students must be familiar with the policy on academic integrity, found at the student information website and in UPS 300.021. The penalty in this course for academic dishonesty is a failing grade, and the incident is reported to the Office of Student Conduct. Please note: repeated cheating offenses can lead to suspension from the university!

m. **Extra credit**: Any extra credit, if given, will be offered on an equal basis to all students. The final project and some assignments, exams, and quizzes may include bonus sections. No other forms of extra credit shall be granted.

Technical Problems

If you encounter any technical difficulties, contact the instructor immediately to document the problem. Then, contact for help:

For technical difficulties: student IT help desk, email, phone = 657-278-8888, walk-in student genius center, online chat - log into portal; click "Online IT Help"; click "Live Chat."

For issues with Canvas: Canvas Support Hotline = 855-302-7528, student support chat, faculty support chat.

In the event a technical problem prevents students from submitting work, the instructor will communicate with students through CSUF email. The instructor may grant an extension until the problem is resolved, or the instructor may have students submit assignments by email, or the instructor may have a different solution. In the case email does not work, students should call the department office for further direction.

Technical Competencies

The website with student information for course syllabi describes the student information technology (IT) services and competencies. In brief, students should have access to a fairly current and reliable computer or tablet (Windows or Mac) and internet connectivity. Students are also expected to have basic computer skills. Visit the student information website above for more details and how you can receive technology assistance, if needed.

In this class students should be comfortable with Linux/UNIX command line and programming in C++. Students are also expected to have the ability to learn Python and other programming languages as needed during class.

Student Resources Website

It is the student's responsibility to read and understand the required and important student information for course syllabi. Included is information about:

- University learning goals
- General Education learning outcomes
- Netiquette
- Students' rights to accommodations
- Campus student support resources
- Academic integrity
- Emergency preparedness
- Library services
- Student IT services and competencies
- Software privacy and accessibility
- Accessibility statement
- Diversity statement
- Land acknowledgement
- Final exam schedule
- Semester calendar

Classroom Management

Cell phones: Out of courtesy and respect for others, you should turn off your cell phones during class. You may check your cell phones during breaks.

Recording: Any requests to record class meetings will be decided on a case-by-case basis by the instructor. If permitted, any approved recordings are for private study and "shall not be made publicly

accessible without the written consent of the instructor and any students recorded in the class" (UPS 330.230). Any approved recordings must be deleted at the end of the semester.

Technology: If you need any assistance with technology, including checking out a laptop computer for the semester, obtaining ancillaries (e.g., webcam, microphone), accessing Wi-Fi, downloading free software for class or personal use, or other help, you can find what you need at the student technology services website. Another useful website is IT essential resources.

Calendar of Topics / Schedule of Classes

NOTE: The class topics and schedule below are subject to change based on the instructor's discretion and the class progress.

Week 1 (01/22)
Topic(s): Class Logistics, Introduction, Confidentiality, Integrity, Availability, Authentication, Non-Repudiation, Government and Public Sector Data Classification, OSI model, (OSI) ITU-T X.800, FIPS-140 series.
Reading(s): Course Syllabus, Stallings 1

Week 2 (01/29)
Topic(s): Overview of Symmetric and Public Key Cryptography, Hashing and MACs, Basics of Confidentiality and Authentication, Bruteforce and Cryptoanalytic Attacks; and Known and Chosen plaintext attacks, Basics of Identity-Based Cryptography.
Reading(s): Stallings 3

Week 3 (02/05)
Topic(s): Authentication Protocols, Key Management, Key Distribution, Public Key Infrastructure, Diffie-Hellman, SSL/TLS, Kerberos, Replay and Man-in-the-Middle Attacks.
Reading(s): Stallings 15
Lab: TryHackMe Room

Week 4 (02/12)
Topic(s): Authentication Protocols, Key Management, Key Distribution, Public Key Infrastructure, Diffie-Hellman, SSL/TLS, Kerberos, Replay and Man-in-the-Middle Attacks.
Reading(s): Stallings 15
Lab: TryHackMe Room

Week 5 (02/19): President's Day –Campus Closed

Week 6 (02/26)
Topic(s): Classical Ciphers
Reading(s): Stallings 3

Week 7 (03/04)

Topic(s): Block Cipher principles, Confusion and Diffusion, Data Encryption Standard (DES), TwoFish, Differential and Linear Cryptoanalysis
Reading(s): Stallings 4
Labs: TryHackMe room

Week 8 (03/11)
Topic(s): Block Cipher Principles, Confusion and Diffusion, Data Encryption Standard (DES), TwoFish, Differential and Linear Cryptoanalysis (Cont.), and Advanced Encryption Standard (AES)
Reading(s): Stallings 6

Week 9 (03/18)
Topic(s): Block Cipher Modes of Operation
Reading(s): Stallings 5

Week 10 (03/25): Exam 1

Week 11 (04/01): Spring Recess (no classes)

Week 12 (04/08)
Topic(s): Operation of hashing algorithms
Reading(s): Stallings 2 and 9
Labs: TryHackMe room

Week 13 (04/15)
Topic(s): Principles of Public Key Cryptography, Number Theory, RSA, and Elliptical Curve
Reading(s): Stallings 2 and 9
Labs: TryHackMe room

Week 14 (04/22)
Topic(s): Principles of Public Key Cryptography, Number Theory, RSA, and Elliptical Curve (Contd)
Reading(s): Stallings 9 and 10

Week 15 (04/29)
Topic(s): Onion routing, Blockchain, VPNs, and Quantum Cryptography
Reading(s):
https://skerritt.blog/how-does-tor-really-work/
https://www.youtube.com/watch?v=bBC-nXj3Ng4
https://skerritt.blog/how-does-tor-really-work/
Lab: TryHackMe room

Week 16 (05/06)
Topic(s): Onion routing, Blockchain, VPNs, and Quantum Cryptography (Contd)
Reading(s):
https://skerritt.blog/how-does-tor-really-work/
https://www.youtube.com/watch?v=bBC-nXj3Ng4
https://skerritt.blog/how-does-tor-really-work/

Lab: TryHackMe room

Week 16 (05/13)
Final Exam