ECE 471/571: Fundamentals of Information and Network Security

Spring 2024

General Course Information:

Instructor	Ming Li, Associate Professor lim@arizona.edu *(preferred method of contact)* Phone: 621-6191 ECE Room 404
Course Websites	https://piazza.com/arizona/spring2024/ece471571/ (Course logistics, and Q&A) https://d2l.arizona.edu (Lecture notes, video, homework/lab submissions, grades) https://app.tophat.com/e/477234 (for on-campus students only, including ECE 471, and ECE 571-001) (To use Tophat, there is a registration fee of $26) (Slides, class exercises, and attendance/participation)
Lecture Times/Modality	In person (and will be recorded via zoom, link will be posted in D2L), Location: Chavez Bldg, Room 400; M, W, F, 1:00PM - 1:50PM;
Instructor Office Hours	M, F, 2:00PM - 3:00PM (online via zoom, link will be posted in D2L). All other times are by appointment only (schedule a zoom meeting via email)
Grader	Yousuf Choudhary ychoudhary@arizona.edu

Course Description:

Spring (3 Units) Introduction to Information and Network Security: Introduction to security concepts and basic cryptographic building blocks. Implementation of fundamental security properties such as message and user authentication, confidentiality, privacy, anonymity, authorization, certification, non-repudiation, and revocation. Application of basic cryptographic primitives on building secure protocols and systems. Network security protocols.

This course adopts a principle of combining theory and practice. Students will learn the basic attacks and defenses by performing them via lab assignments. They will be introduced to a number of security tools to understand how they work and what security guarantee they provide. The experiments will be conducted in the virtual machine environments. Students are expected to know basic C programming and Linux/Unix.

Prerequisite(s)

Required: ECE 275 (Computer Programming for Engineering Applications II), ECE 310 (Applications of Engineering Mathematics) or equivalent

Recommended (but not required): ECE 478/578 (Fundamentals of Computer Networking) or equivalent

Textbook

Required

- *Cryptography and Network Security: Principles and Practice*, 8th Edition, W. Stallings, Pearson, 2020 (can get the digital version via UA bookstore's Inclusive Access program: https://shop.arizona.edu/textbooks/Inclusive.asp)

Recommended (and reference)

- *Network Security (private communication in a public world),* C. Kaufman, R. Perlman, M. Speciner, Prentice Hall, 3rd Edition. (more suitable for undergraduate students)
- *Cryptography: Theory and Practice*, Douglas Stinson, 4th Edition, Prentice Hall (more suitable for graduate students)
- *Computer & Internet Security: A Hands-on Approach*, Second Edition, May 2019, by Wenliang (Kevin) Du, ISBN: 978-1733003926 (hardcover) and 978-1733003933 (paperback) https://www.handsonsecurity.net/ (reference book for the labs)

Course Objectives:

Upon the completion of this course, students should have achieved the following objectives:

- Have a fundamental understanding of the objectives of cryptography and network security.
- Become familiar with the cryptographic techniques that provide information and network security.
- Be able to apply suitable cryptographic primitives to achieve specific security goals for communication systems and networks
- Be able to evaluate the security of communication systems, networks and protocols based on a multitude of security metrics.

Expected Learning Outcomes

By the end of this course, the student will be able to:

1. Identify the basic notions of information and network security
2. Grasp the basic concept and approaches of cryptanalysis
3. Describe and apply cryptographic primitives for achieving confidentiality in both private key and public key settings
4. Describe and apply cryptographic mechanisms for achieving information integrity
5. Evaluate the security/computation/communication tradeoffs between public key and private key cryptography.
6. Describe methods and cryptographic primitives for achieving user authentication.
7. Apply private key or public key cryptographic primitives for building mutual authentication protocols, and be able to identify and avoid common pitfalls in protocol design
8. Outline key agreement and key distribution protocols and analyze their overhead
9. Explain the application of cryptographic primitives and protocols in the context of wireless and network security

Additional Learning Outcomes for 571:

10. Describe and apply cryptanalysis methods to crack early and modern ciphers.
11. Describe and apply formal security definitions and proof mechanisms to reason about the security of a cryptosystem or security protocol

Relationship to Student Outcomes:

ECE 471 contributes directly to the following specific Electrical and Computer Engineering Student Outcomes of the ECE Department:

a) an ability to apply knowledge of mathematics, science, and engineering (High).
e) an ability to identify, formulate, and solve engineering problems (High).

f) an understanding of professional and ethical responsibility (Medium).
g) an ability to communicate effectively (Medium).
h) the broad education necessary to understand the impact of engineering solutions in a global and societal context (High).
j) a knowledge of contemporary issues (Medium)
k) an ability to use the techniques, skills, and modern engineering tools necessary for engineering practice (High).

Course Topics

Introduction to Information Security (~1 week)

- Information security objectives
- Schematic of a secure communication system
- Formal definition of a cryptosystem and adversary models

Classical Encryption Techniques (~1.5 weeks)

- Number theory basics
- Early cryptosystems: substitution and transposition
- Cryptanalysis of early cryptosystems

Measures of Security and Ideal Cryptosystems (~1 week)

- Measures of security
- Perfect secrecy
- Entropy and secrecy
- Ideal cryptosystems & one-time pad

Symmetric Key Cryptography (~2 weeks)

- The notions of symmetric key cryptography, and computational security
- Block cipher, product cipher, and substitution-permutation networks
- The Data Encryption Standard (DES)
- The Advanced Encryption Standard (AES)
- Modes of operation
- Pseudorandom numbers and stream ciphers

Public Key Cryptography (~1.5 weeks)

- Principles of Public-key Cryptography (PKC)
- More number theory basics
- Common public key cryptosystems: RSA
- Diffie-Hellman key exchange and ElGamal

Message Integrity and Authentication (~1.5 weeks)

- Definition of hash functions and security properties
- Examples of hash functions: MD series, and Secure Hash Algorithm (SHA)
- Message Authentication Codes (MAC), HMAC
- More hash applications, including commitment protocols
- Common digital signatures schemes: RSA, ElGamal, Schnorr, and DSA

Key Management and Distribution (~1 week)

- Symmetric key distribution schemes, Key Distribution Centers (KDC), session keys
- Public key distribution and Certificate Authorities (CA)
- Public Key Infrastructure (PKI)

User Authentication (~1.5 weeks)

- User authentication principles
- Password authentication protocols
- Challenge-response protocols and common pitfalls
- Kerberos

Network Security (~2 weeks)

- TCP/IP Threats
- IP security: the IPSec protocol
- Transport-level security: SSL and TLS protocols
- Electronic mail security, S/MIME, PGP

System Security (~1 week)

- Malware, Worms, DDoS attacks, SBGP
- Firewalls and Virtual Private Networks (VPNs)
- Intrusion detection

Important Dates

- Undergraduate Students: http://registrar.arizona.edu/dates-and-deadlines/view-dates?field_display_term_value=181
- Graduate Students: http://registrar.arizona.edu/dates-and-deadlines/view-dates-grad-students?field_display_term_value=181
- No class dates: 1/16/2022 (Monday), Spring recess (March 6-12, 2022), 5/4/2023: reading day (no classes).

Course Assignments and Exams:

There will be weekly homework assignment on the topics covered in class, with an approximate 5 homework assignments and 5 lab assignments. There will also be a midterm exam and a final exam. All homework and lab assignments should be submitted electronically through D2L. Details will be posted later during the semester. All exams will be held online via D2L (in the form of timed quiz). The length of the exams will be two hours and there will be a one day window to finish them.

The grading distribution for course assignments and exams is as follows:

- Homework Assignments: 30%
- Lab Assignments: 25%
- Midterm Exam (TBD, around mid-March): 20%
- Final Exam: 20%
- Class participation (Tophat, on-campus students only): 5%
- Quizzes (ECE571 online students only): 5%

Note that, we will use Tophat to record class participation/attendance (for on-campus students), which consists of participation and the correctness of answers to in-class questions & exercises. Thus, it is highly recommended that you preview the corresponding reading materials (e.g., book chapters) prior to each class. For online students, we will use quizzes in D2L to evaluate course participation.

ECE 571 and ECE 471 may have slightly different problem sets for homework and exams. The difference in difficulty and scope reflect the additional expectations in ECE 571 learning outcomes.

Course Grading Policies:

Your course letter grade will be assigned based on your final numerical grade as follows:

A	=	90 – 100 points
B	=	80 – 89 points
C	=	70 – 79 points
D	=	60 – 69 points
E	=	0 – 59 points

Homework is due at the time that it is specified in the homework handout (all homework handouts will be posted on the class website). **NO late** assignment will be accepted in general (except in extraordinary scenarios).

Make-up exams: A make-up exam may only be given under extraordinary circumstances. The student requesting a make-up exam should contact the instructor well in advance and provide *written* documentation for the reason that he/she will not be able to attend the regularly scheduled exam. It is up to the discretion of the Instructor to accept the justification provided by the student.

Requests for incompletes (I) and withdrawal (W) must be made in accordance with University policies which are available at http://catalog.arizona.edu/2015-16/policies/grade.htm#I and http://catalog.arizona.edu/2015-16/policies/grade.htm#W respectively.

Dispute of Grade Policy: You can dispute any grade that you receive within two weeks that the grade has been awarded.

Equipment and software requirements
For this class you will need access to the following hardware: desktop/laptop or web-enabled device with webcam and microphone; regular access to reliable internet signal; ability to download and run the following software: web browser, Adobe Acrobat, Word processer such as MS word, Zoom, etc.

Class Recordings
For lecture recordings, which are used at the discretion of the instructor, students must access content in D2L only. Recorded zoom lectures will be available in D2L shortly after each lecture. Students may not modify content or re-use content for any purpose other than personal educational reasons. All recordings are subject to government and university regulations. Therefore, students accessing unauthorized recordings or using them in a manner inconsistent with UArizona values and educational policies are subject to suspension or civil action.

Lab Assignments
The lab assignments will be based on the SEED labs (https://seedsecuritylabs.org/index.html). They are take home assignments (since we don't have lab sessions), which can all be done on your own computers. You need to first install VirtualBox and the Ubuntu VM image (version 20.04). A written report needs to be submitted after the lab, before the designated due dates. Expected outcomes of your submission will be specified in the end of each lab description. For each lab assignment, students' grade will generally be based on two parts: correctness of the results and your understanding, and writing quality of the report (e.g., clarity, enough details to demonstrate evidence of actually carrying out of the tasks). All labs are individual labs, you are encouraged to discuss with others, but each student must independently carry out the tasks in the labs. You cannot copy code/results/writings from other students.

Class attendance policies
Participating in course and attending lectures and other course events are vital to the learning process. As such, attendance is required at all lectures and discussion section meetings. In general, students who miss class due to illness or emergency are required to bring documentation from their healthcare provider or other relevant, professional third parties. The UA's policy concerning Class Attendance, Participation, and Administrative Drops is available at: http://catalog.arizona.edu/2015-16/policies/classatten.htm

The UA policy regarding absences for any sincerely held religious belief, observance or practice will be accommodated where reasonable, http://policy.arizona.edu/human-resources/religious-accommodation-policy

Absences pre-approved by the UA Dean of Students (or Dean Designee) will be honored. See: http://uhap.web.arizona.edu/policy/appointed-personnel/7.04.02

Special note this year:

- If you feel sick, or if you need to isolate or quarantine based on University protocols, stay home. Except for seeking medical care, avoid contact with others and do not travel.
- Notify your instructor(s) if you will be missing a course meeting or an assignment deadline.
- Non-attendance for any reason does **not** guarantee an automatic extension of due date or rescheduling of examinations/assessments.
  - Please communicate and coordinate any request directly with your instructor.
- If you must miss the equivalent of more than one week of class, please contact the Dean of Students Office DOS-deanofstudents@email.arizona.edu to share documentation about the challenges you are facing.
- Voluntary, free, and convenient COVID-19 testing is available for students on Main Campus.
- If you test positive for COVID-19 and you are participating in on-campus activities, you must report your results to Campus Health. To learn more about the process for reporting a positive test, visit the Case Notification Protocol.
- The COVID-19 vaccine and booster is available for all students at Campus Health.
- Visit the UArizona COVID-19 page for the most up-to-date information.

Academic advising: If you have questions about your academic progress this semester, or your chosen degree program, please note that advisors at the Advising Resource Center can guide you toward university resources to help you succeed.

Life challenges: If you are experiencing unexpected barriers to your success in your courses, please note the Dean of Students Office is a central support resource for all students and may be helpful. The Dean of Students Office can be reached at 520-621-2057 or DOS-deanofstudents@email.arizona.edu.

Physical and mental-health challenges: If you are facing physical or mental health challenges this semester, please note that Campus Health provides quality medical and mental health care. For medical appointments, call (520-621-9202. For After Hours care, call (520) 570-7898. For the Counseling & Psych Services (CAPS) 24/7 hotline, call (520) 621-3334.

Accessibility and Accommodations

Our goal is that learning experiences be as accessible as possible. If you anticipate or experience physical or academic barriers based on disability, please let me know immediately so that we can discuss options. You are also welcome to contact Disability Resources (520-621-3268) to establish reasonable accommodations. For additional information on Disability Resources and reasonable accommodations, please visit http://drc.arizona.edu/.

If you have reasonable accommodations, please plan to meet with me by appointment or during office hours to discuss accommodations and how my course requirements and activities may impact your ability to fully participate.

Code of Academic Integrity

Students are encouraged to share intellectual views and discuss freely the principles and applications of course materials. However, graded work/exercises must be the product of independent effort unless otherwise instructed. Students are expected to adhere to the UA Code of Academic Integrity as described in the UA General Catalog. See: http://deanofstudents.arizona.edu/academic-integrity/students/academic-integrity.

The University Libraries have some excellent tips for avoiding plagiarism available at: http://www.library.arizona.edu/help/tutorials/plagiarism/index.html.

Selling class notes and/or other course materials to other students or to a third party for resale is not permitted without the instructor's express written consent. Violations to this and other course rules are subject to the Code of Academic Integrity and may result in course sanctions. Additionally, students who use D2L or UA email to sell or buy these copyrighted materials are subject to Code of Conduct Violations for misuse of student email addresses. This conduct may also constitute copyright infringement.

UA Nondiscrimination and Anti-harassment Policy
The University is committed to creating and maintaining an environment free of discrimination, http://policy.arizona.edu/human-resources/nondiscrimination-and-anti-harassment-policy

Our classroom is a place where everyone is encouraged to express well-formed opinions and their reasons for those opinions. We also want to create a tolerant and open environment where such opinions can be expressed without resorting to bullying or discrimination of others.

Additional Resources for Students (recommended links)
UA Academic policies and procedures are available at:
http://catalog.arizona.edu/2015-16/policies/aaindex.html
Student Assistance and Advocacy information is available at:
http://deanofstudents.arizona.edu/student-assistance/students/student-assistance

Disruptive Student Behavior and Student Accountability, from the Dean of Student's Office (http://deanofstudents.arizona.edu/accountability/disruptive-student-behavior)

Confidentiality of Student Records
http://www.registrar.arizona.edu/ferpa/default.htm

Subject to Change Statement
Information contained in the course syllabus, other than the grade and absence policy, may be subject to change with advance notice, as deemed appropriate by the instructor.