Course Number: EE P 595

Title: Network Security and Cryptography

Quarter and Year: Summer 2025

Credits: 4

Instructor: Dinuka Sahabandu

Course Goals:

To develop an understanding of the fundamental principles of cryptography and its application to network and communication security. This course will serve as an introduction to the fundamental tools in cryptography and the protocols that enable its application to network and communication security. We will cover topics including encryption (secret-key and public-key), digital signatures, secure authentication, key management, cryptographic hashing, public key infrastructure, and ethics and challenges associated with the use of computer security in a vulnerable world.

Learning Objectives:

At the end of this course, students will be able to:

1. Describe the basic cryptographic primitives, authentication protocols and why they work, and the common design errors.
2. Design, implement and analyze algorithms covered in class using Python.
3. Design algorithms using block ciphers and relate it to the modern symmetric key encryption standards.
4. Design and analyze Hash functions for checking message integrity under transmission.
5. Design and analyze Message Authentication Codes (MAC).
6. Analyze the strength of a given cryptosystem using classical/modern cryptanalysis tools.
7. Describe and analyze authenticated session establishment protocols used in internet communication.
8. Describe the ethical issues related to the misuse of computer security.

Textbook:

D. Stinson, Cryptography Theory and Practice, 4th edition, Chapman & Hall/CRC, 2019.

Reference Texts:

1. C. Kaufman, R. Perlman, M. Speciner, Network Security (Private Communication in a Public World), Prentice Hall, 2002.
2. A. Menezes, P. Van Oorschot, S. Vanstone, Handbook of Applied Cryptography, CRC Press, 2001.

Prerequisites:

Working knowledge of Python, calculus and matrix algebra, and probability and statistics.

Topics:

1. Week 1: Introduction to classical cryptography and cryptanalysis (Stinson Chapter
2. Week 2: Block Ciphers and the Advanced Encryption Standard (Stinson Chapter 3)
3. Week 3-4: Public key encryption based on RSA and Integer Factorization (Stinson Chapter 5)
4. Week 4-5: Public key encryption based on El-Gamal and Discrete Logarithm Problem (Stinson Chapter 6)
5. Week 5-6: Hash Functions for Message Integrity Verification (Stinson Chapter 4)
6. Week 6-7: Digital signatures (RSA, El-Gamal, DSA) (Stinson Chapter 7)
7. Week 8: Key Management Schemes, Authenticated Key Agreement Schemes (Stinson Chapter 10)
8. Week 9: Public Key Infrastructure and the PKI Standard
9. Week 10: Technology, Ethical Challenges, IEEE Code of Ethics related to Security Engineering in a vulnerable world
10. Week 11: Final Group Project Presentations

Computer Resources:

The course uses Python for homework exercises and course projects. Students are expected to use their personal laptops, but they may use the ECE department computers if available.

Grading:

Homework: 40% (four at 10% each)

Quiz: 10%

Project: 50%

- Proposal: 10%
- Final presentation: 15%
- Final report: 25%

COURSE POLICIES

- Please complete the homework by yourself and do not copy code from others or the internet. Any answer from Chat-GPT needs to be identified as such. Suppose your homework is identical to others or any sample code snippets online. In that case, you will receive zero scores, and UW mandates us to report it to the College of Engineering.
- You are encouraged to discuss lab and homework content with your classmates offline and on the discussion board. However, please limit your discussion to ideas and not discuss the code. Specifically, do not copy-paste any homework answers into the discussion board.
- Students must submit homework and project materials online by the posted due date. Throughout the quarter, we will provide you with six late-day credits for the three homework assignments, which you can use to submit one or more homework without a penalty. However, if you have used all six days, each additional late day will result in a 20% penalty in the corresponding homework.
- Students need to submit project reports and presentations on time. The project does not have any credit days. Any overdue project materials will receive a zero score.

RELIGIOUS ACCOMMODATIONS

Washington state law requires that UW develop a policy for accommodation of student absences or significant hardship due to reasons of faith or conscience, or for organized religious activities. The UW's policy, including more information about how to request an accommodation, is available at Religious Accommodations Policy (https://registrar.washington.edu/staffandfaculty/religious-accommodations-policy/). Accommodations must be requested within the first two weeks of this course using the Religious Accommodations Request form (https://registrar.washington.edu/students/religious-accommodations-request/).

ACCOMMODATIONS AND ACCESS

If you have already established accommodations with Disability Resources for Students (DRS), please communicate your approved accommodations to me at your earliest convenience so we can discuss your needs in this course. If you have not yet established services through DRS, but have a temporary health condition or permanent disability that requires accommodations (conditions include but not limited to; mental health, attention-related, learning, vision, hearing, physical or health impacts), you are welcome to contact DRS at 206-543-8924 or uwdrs@uw.edu or disability.uw.edu. DRS offers resources and coordinates reasonable accommodations for students with disabilities and/or temporary health conditions. Reasonable accommodations are established through an interactive process between the student, instructor, and DRS. It is the policy and practice of the University of Washington to create inclusive and accessible learning environments consistent with federal and state law.

ACADEMIC INTEGRITY

Engineering is a profession demanding a high level of personal honesty, integrity and responsibility. Therefore, it is essential that engineering students, in fulfillment of their academic requirements and in preparation to enter the engineering profession, adhere to the College of Engineering Statement of Principles. Any student in this course suspected of academic misconduct (e.g., cheating, plagiarism, or falsification) will be reported to the College of Engineering Dean's Office and the University's Office of Community Standards and Student Conduct to initiate the student conduct process.

TITLE IX

"UW, through numerous policies, prohibits sex- and gender-based violence and harassment, and we expect students, faculty, and staff to act professionally and respectfully in all work, learning, and research environments. For support, resources, and reporting options related to sex- and gender-based violence or harassment, visit UW Title IX's webpage (https://www.washington.edu/titleix/), specifically the Know Your Rights & Resources guide (https://www.washington.edu/titleix/files/2020/08/KYRR-guide-8-10-2020-LINKED.pdf).

If you choose to disclose information to me about sex- or gender-based violence or harassment, I will connect you (or the person who experienced the conduct) with resources and individuals who can best provide support and options. You can also access those resources directly:

- Confidential: Confidential advocates (https://www.washington.edu/sexualassault/support/advocacy/) will not share information with others unless given express permission by the person who has experienced the harm or when required by law.
- Private and/or anonymous: SafeCampus (https://www.washington.edu/safecampus/) provides consultation and support and can connect you with additional resources if you want them. You can contact SafeCampus anonymously or share limited information when you call

Please note that some senior leaders and other specified employees have been identified as “Officials Required to Report.” (https://www.washington.edu/titleix/title-ix-officials-required-to-report/) If an Official Required to Report learns of possible sex- or gender-based violence or harassment, they are required to call SafeCampus and report all the details they have in order to ensure that the person who experienced harm is offered support and reporting options (https://www.washington.edu/titleix/resources/).”