ECE 443 – Introduction to Computer Cyber Security
ECE 518 – Computer Cyber Security
Fall 2025

Instructor: Professor Jia Wang
E-Mail: jwang34@illinoistech.edu (Please start your email subject line with [ECE443] or [ECE518].)

Prerequisites: Computer programming; digital logic and computer organization; probability.

Class Time and Location: Mon./Wed. 11:25 AM – 12:40 PM, IIT Tower 16E4-1

Class Home Page: `https://wngjia.github.io/ece443-web/`

Required Textbook:
- [UC] "Understanding Cryptography: A Textbook for Students and Practitioners" C. Paar and J. Pelzl, Springer, 2010. ISBN-13: 978-3642446498. Download at `https://link-springer-com.ezproxy.gl.iit.edu/book/10.1007/978-3-642-04101-3`

Recommended Textbook:
- [ICS] "Introduction to Computer Security" M. Bishop, Addison-Wesley, 2005. ISBN: 0321247442

Computer Requirement:
- A computer supporting development in Go
- Internet access to common code and package repositories like GitHub

Course Descriptions:

ECE 443: This course introduces students to computer and cyber security by identifying threats and defense mechanisms. Key topics covered include ciphers, hash functions, public-key cryptography, authenticated encryption, system security, digital forensics, software and hardware security, and side-channel attacks. Course projects will survey trending topics and provide hand-on experiences on languages, libraries, and tools supporting state-of-the-art cryptography systems.

ECE 518: This course gives students a clear understanding of computer and cyber security as threats and defense mechanisms backed by mathematical and algorithmic guarantees. Key topics covered include introductory number theory and complexity theory, cryptography and applications, system security, digital forensics, software and hardware security, and side-channel attacks. Course projects will survey trending topics and provide hand-on experiences on languages, libraries, and tools supporting state-of-the-art cryptography systems and advanced applications.

Grading:
- 4 Homeworks: 5 points each for a total of 20 points.
- 6 Projects: 15 points each for a total of 90 points.
- Midterm Exam: 30 points.
- ECE 443: A $\geq$ 90 / B $\geq$ 80 / C $\geq$ 60 / D (undergraduate only) $\geq$ 55.
- ECE 518: A $\geq$ 115 / B $\geq$ 100 / C $\geq$ 80.

Homework and Project Policy: Late homeworks and project reports will not be graded. Discussions on homeworks and projects are encouraged, but copying will call for disciplinary action.

Exam Policy: Close book, close note, cheat sheet allowed. Makeup exams will NOT be given.

Lecture Schedule (tentative):

No.	Date	Topic	Chapters	HW Out	Project Due
1, 2	8/18, 8/20	Introduction	ICS 1, UC 1		
3, 4	8/25, 8/27	Stream and Block Ciphers	UC 2–5	HW #1	
5, 6	~~9/1~~, 9/3, 9/5	Go, Cryptographic Hash Function	UC 11		
7, 8	9/8, 9/10	Authenticated Encryption, Number Theory	UC 12		PRJ #1
9,10	9/15, 9/17	RSA, Diffie-Hellman	UC 6, 7, 8	HW #2	
11,12	9/22, 9/24	Digital Signatures	UC 10		PRJ #2
13,14	9/27,10/1	Key Establishment	UC 13		
15,16	10/6, 10/8	OpenSSL, **Midterm Exam**			
17	~~10/13~~,10/15	Secure Collaborations			
18,19	10/20,10/22	Consensus and Cryptocurrency			
20,21	10/27,10/29	Smart Contract, Bitcoin Security			PRJ #3
22,23	11/3, 11/5	Secure Multi-Party Computation	ICS 2–7, 14	HW #3	
24,25	11/10,11/12	Access Control			
26,27	11/17,11/19	Digital Forensics	ICS 19	HW #4	
28	11/24,~~11/26~~	Malware			PRJ #4
29,30	12/1, 12/3	Hardware Security, Side-Channel Attacks			PRJ #5
	12/8–12/12	**No Final Exam**			PRJ #6

ECE 443 Course Objectives (ABET)
After completing this course, you should be able to:

1. Describe computer cyber security as threats and defense mechanisms.
2. Understand stream ciphers, block ciphers, cryptographic hash functions, and public-key cryptography.
3. Explain authenticated encryption, man-in-the-middle attack, perfect forward secrecy, and their impact on secure communication protocol designs.
4. Understand system security concepts including security policies and access control.
5. Describe vulnerabilities in software and hardware systems.
6. Explain digital forensics processes.

ADA Statement: Reasonable accommodations will be made for students with documented disabilities. In order to receive accommodations, students must obtain a letter of accommodation from the Center for Disability Resources and make an appointment to speak with me as soon as possible. The Center for Disability Resources is located in the Life Sciences Building, room 218, 312-567-5744 or `disabilities@iit.edu`.

Sexual Harassment and Discrimination Information: Illinois Tech prohibits all sexual harassment, sexual misconduct, and gender discrimination by any member of our community. This includes harassment among students, staff, or faculty. Sexual harassment of a student by a faculty member or sexual harassment of an employee by a supervisor is particularly serious. Such conduct may easily create an intimidating, hostile, or offensive environment. Illinois Tech encourages anyone experiencing sexual harassment or sexual misconduct to speak with the Office of Title IX Compliance for information on support options and the resolution process. You can report sexual harassment electronically at iit.edu/incidentreport, which may be completed anonymously. You may additionally report by contacting the Title IX Coordinator, Virginia Foster at `foster@iit.edu` or the Deputy Title IX Coordinator at `eespeland@iit.edu`. For confidential support, you may reach Illinois Tech's Confidential Advisor at (773) 907-1062. You can also contact a licensed practitioner in Illinois Tech's Student Health and Wellness Center at `student.health@iit.edu` or (312)567-7550 For a comprehensive list of resources regarding counseling services, medical assistance, legal assistance and visa and immigration services, you can visit the Office of Title IX Compliance website at `https://www.iit.edu/title-ix/resources`.