ECE 443 – Introduction to Computer Cyber Security
ECE 518 – Computer Cyber Security
Fall 2023

Instructor: Professor Jia Wang
E-Mail: jwang34@iit.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, Stuart Building 111

Class Home Page: `http://www.ece.iit.edu/~jwang/ece443-2023f/`

Required Textbook:
- [UC] "Understanding Cryptography: A Textbook for Students and Practitioners"
  C. Paar and J. Pelzl, Springer, 2010. ISBN-13: 978-3642446498
  Available at `https://i-share.carli.illinois.edu/vf-iit/Record/IITdb.809772`

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

Computer Requirement: A computer desktop or laptop that is able to run VirtualBox is required for this course. Computers with solid-state drives, at least 16GB of memory, and at least 4 physical processor cores are recommended.

Course Descriptions: 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 provide hand-on experiences on languages, libraries, and tools supporting state-of-the-art cryptography applications. Students registering for ECE 518 are required to complete additional projects in advanced areas.

Grading:
- Homeworks: 5 points each for a total of 20 points.
- 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 $\geq$ 110 / B $\geq$ 90 / C $\geq$ 75.

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, except for extraordinary reasons.

Lecture Schedule (tentative):

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