ECE 443 – Introduction to Computer Cyber Security
ECE 518 – Computer Cyber Security
Fall 2021

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. 11:15 AM – 12:30 PM, John T. Rettaliata Engg Center 104

Class Home Page: `http://www.ece.iit.edu/~jwang/ece443-2021f/`

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

Course Summary: This course gives students a clear understanding of computer and cyber security as threats and defense mechanisms. Students will learn to approach security from a formal perspective and to gain hand-on experiences on practical systems and applications.

Topics Covered:
- Cryptography, cryptographic protocols, and their applications.
- System security, hardware security, and side-channel attacks.
- Digital forensics.

ECE 443 Grading: Homeworks 10% / Projects 20% (Extra) / Midterm Exam: 45% / Final Exam: 45%. A: $\geq$ 90% / B: $\geq$ 80% / C: $\geq$ 60% / D (undergraduate only): $\geq$ 55%.

ECE 518 Grading: Homeworks 10% / Projects 20% / Midterm Exam: 35% / Final Exam: 35%. A: $\geq$ 90% / B: $\geq$ 80% / C: $\geq$ 60%.

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/Project Out
1, 2	8/23, 8/25	Introduction	ICS 1, UE 1	HW #1
3, 4	8/30, 9/1	Stream and Block Ciphers	UE 2–5	HW #2
5	~~9/6~~, 9/8	Cryptographic Hash Function	UE 11	
6, 7	9/13, 9/15	MAC, Authenticated Encryption	UE 12	PRJ #1
8, 9	9/20, 9/22	RSA	UE 6, 7	
10,11	9/27, 9/29	Diffie-Hellman, Digital Signatures	UE 8, 9	HW #3
12,13	10/4, 10/6	Authentication and Key Establishment	UE 13	PRJ #2
	~~10/11~~, 10/13	**Midterm Exam**		
14,15	10/18,10/20	Cryptocurrency		PRJ #3
16,17	10/25,10/27	Secure Multi-Party Computation		
18,19	11/1, 11/3	Access Control	ICS 2–7, 14	HW #4
20,21	11/8, 11/10	Secure Storage and Digital Forensics		PRJ #4
22,23	11/15,11/17	Bugs, Worms, and Viruses	ICS 19	HW #5
24	11/22,~~11/24~~	Hardware Security		
25,26	11/29, 12/1	Side-Channel Attacks		
	12/6–12/10	**Final Exam**		

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`.

Campus Reopening: Please refer to `https://www.iit.edu/reopening` for the most recent information regarding campus reopening.

Currently, as recently announced, the university is requiring all students, faculty, and staff to receive a COVID-19 vaccination. Full details may be found in Vaccine Requirement and Reopening Policy at `https://web.iit.edu/sites/web/files/departments/general-counsel/policies/procedure_c7_COVID-19_Vaccination_Requirement_and_Reopening_Policy_Policy-C.7.pdf`

Moreover, consistent with Centers for Disease Control and Prevention and Chicago Department of Public Health recommendations, all students, faculty, staff, and campus visitors must now wear face coverings in all shared indoor settings, regardless of vaccination status.