ECE 443 – Introduction to Computer Cyber Security
ECE 518 – Computer Cyber Security
Fall 2018

Instructor: Professor Jia Wang
Office: 317 Siegel Hall
Phone: 312-567-3696
E-Mail: jwang@ece.iit.edu (Please start your email subject line with [ECE443] or [ECE518].)

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

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`.

Class Time and Location: Mon./Wed.: 11:25 AM – 12:40 PM, Wishnick Hall 115

Class Home Page: `http://www.ece.iit.edu/~jwang/ece443-2018f/`

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`
- [ICS] "Introduction to Computer Security" M. Bishop, Addison-Wesley, 2005. ISBN: 0321247442
- Plus additional notes.

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 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
1	8/20, 8/22	Introduction	ICS 1, UE 1	HW #1
2	8/27, 8/29	Stream and Block Ciphers	UE 2, 3, 4	HW #2
3	~~9/3~~, 9/5	Modes of Operation	UE 5	
4	9/10, 9/12	Cryptographic Hash Function and MACs	UE 11, 12	PRJ #1
5	9/17, 9/19	RSA	UE 6, 7	
6	9/24, 9/26	Diffie-Hellman, Digital Signatures	UE 8, 9	HW #3
7	10/1, 10/3	Key Establishment and Authentication	UE 13	PRJ #2
8	~~10/8~~, 10/10	**Midterm Exam**		
9	10/15, 10/17	Cryptocurrency		PRJ #3
10	10/22, 10/24	Topics in Advanced Cryptography		
11	10/29, 10/31	Security Policies	ICS 4, 5, 6, 7	HW #4
12	11/5, 11/7	Access Control, Digital Forensics	ICS 2, 14	PRJ #4
13	11/12, 11/14	Bugs, Worms, and Viruses	ICS 19	HW #5
14	11/19, ~~11/21~~	Topics in Hardware Security		
15	11/26, 11/28	Side-Channel Attacks		
16	12/3 – 12/7	**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.