# ECE 443 – Introduction to Computer Cyber Security
# ECE 518 – Computer Cyber Security
# Fall 2020

**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.

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:** Lectures will be recorded and published online. Additional office hours may be streamed Mon./Wed. 11:15 AM – 12:30 PM.

**Class Home Page:** `http://www.ece.iit.edu/~jwang/ece443-2020f/`

**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:** Online in Blackboard using Respondus (lockdown browser). Close book, close note, cheat sheet allowed. Makeup exams will NOT be given, except for extraordinary reasons.

**Lecture Schedule (tentative):**

| No. | Week | Topic | Chapters | HW/Project |
|---|---|---|---|---|
| 1, 2 | 8/24 | Introduction | ICS 1, UE 1 | HW #1 |
| 3, 4 | 8/31 | Stream and Block Ciphers | UE 2–5 | HW #2 |
| 5 | 9/7 | Cryptographic Hash Function | UE 11 | |
| 6, 7 | 9/14 | MAC, Authenticated Encryption | UE 12 | PRJ #1 |
| 8, 9 | 9/21 | RSA | UE 6, 7 | |
| 10,11 | 9/28 | Diffie-Hellman, Digital Signatures | UE 8, 9 | HW #3 |
| 12,13 | 10/5 | Authentication and Key Establishment | UE 13 | PRJ #2 |
| | 10/12 | **Midterm Exam** | | |
| 14,15 | 10/19 | Cryptocurrency | | PRJ #3 |
| 16,17 | 10/26 | Secure Multi-Party Computation | | |
| 18,19 | 11/2 | Access Control | ICS 2–7, 14 | HW #4 |
| 20,21 | 11/9 | Secure Storage and Digital Forensics | | PRJ #4 |
| 22,23 | 11/16 | Bugs, Worms, and Viruses | ICS 19 | HW #5 |
| 24 | 11/23 | Hardware Security | | |
| 25,26 | 11/30 | Side-Channel Attacks | | |
| | 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.

While we do not expect to utilize traditional classrooms for lectures and exams for this online course, please refer to the next page for **COVID-19 Precautions and Face Coverings in Class**.

**COVID-19 Precautions and Face Coverings in Class**

Illinois Tech students are required to wear face masks at all times and maintain social distancing (6 feet between individuals) in traditional classrooms, instructional laboratories, and similar settings. In general, individuals should spend as little time as practicable in closer proximity when doing so is necessary to achieve learning objectives. Students who are feeling ill or experiencing symptoms such as sneezing, coughing, or a higher than normal temperature will be excused from class and are expected to stay at home.

Instructors have the right to ask those who are not complying with these requirements to leave class in the interest of everyone's health and safety. In the event that a student refuses to comply with instructor directions regarding face masks and/or social distancing, the instructor has the right to ask the student to leave, and/or cancel class. A student who refuses to comply with these requirements will be referred to the Office of the Dean of Students for possible disciplinary action under the Student Code of Conduct.

Additionally, as a reminder, following other simple practices such as frequent and thorough hand washing, wiping down desks and seats with disinfectant wipes when possible, not sharing personal items such as pens and cell phones, and avoiding crowded hallways and other enclosed spaces will promote good health in and out of the classroom.

Visit `iit.edu/COVID-19` for details on Illinois Tech's response to coronavirus (COVID-19). For information from government authorities, please see the Centers for Disease Control and Prevention website at `cdc.gov`.