ECE 443 – Introduction to Computer Cyber Security

Credits: 3, **Contact Hours:** Two 75 minute lecture session per week.

Coordinator: J. Wang, Associate Professor of ECE

Textbook: C. Paar and J. Pelzl, *Understanding Cryptography: A Textbook for Students and Practitioners*, Springer, 2010

2019 Catalog Data: ECE 443: Introduction to Computer Cyber Security. Credit 3.
Computer security as threats and defense mechanisms. Introductory cryptography and key management. Authentication and authorization. System security. Network security. Cloud and web security. Hardware security. Digital Forensics. Advanced cryptography topics. (3-0-3) **(P)**

Prerequisites or co-requisites by topic:

Enrollment: Elective course for EE majors; computer systems/software elective course for CPE majors.

Specific outcomes of instruction:
After completing this course, the student should be able to do the following:

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.

Relationship of ECE 443 specific outcomes of instruction to student outcomes:

	Student Outcomes	**Course Goals**
1	An ability to identify, formulate, and solve complex engineering problems by applying principles of engineering, science, and mathematics	1,2,3,4,5,6
2	An ability to apply engineering design to produce solutions that meet specified needs with consideration of public health, safety, and welfare, as well as global, cultural, social, environmental, and economic factors	1,2,3,4,5,6
3	An ability to communicate effectively with a range of audiences	
4	An ability to recognize ethical and professional responsibilities in engineering situations and make informed judgments, which must consider the impact of engineering solutions in global, economic, environmental, and societal contexts	
5	An ability to function effectively on a team whose members together provide leadership, create a collaborative and inclusive environment, establish goals, plan tasks, and meet objectives	
6	An ability to develop and conduct appropriate experimentation, analyze and interpret data, and use engineering judgment to draw conclusions	2,4
7	An ability to acquire and apply new knowledge as needed, using appropriate learning strategies	

Topics:

- Introduction to computer cyber security (1 week)
- Stream and block ciphers (1 week)
- Cryptographic hash function and MAC (1.5 week)
- Authenticated encryption (0.5 weeks)
- RSA, DH, digital signatures (2 week)
- Authentication and key establishment (1 week)
- Cryptocurrency (1 week)
- Secure multi-party computation (1 week)
- Access control (1 week)
- Secure storage and digital forensics (2 weeks)
- Bugs, worms, and viruses (1 week)
- Hardware security (1 week)
- Side-channel attacks (1 week)

Laboratory topics: **None**

Prepared by: J. Wang **Date:** February 28, 2020