University of South Carolina – Aiken Department of Mathematical Sciences
CSCI A285 Introduction to Cryptography– SRESFS Summer 2024 (4.10.24)

Instructor: Barry Hudson
Office: ADM
Phone: 803-292-6055
Email: Barry.Hudson@usca.edu

Classroom: USCA In Person
Class Time: MWF 10AM – 1PM
Office Hours: TBA

Textbook: Niels Ferguson, Bruce Schneier, Tadayoshi Kohno (2010) *Cryptography Engineering: Design Principles and Practical Applications,* Wiley Publishing. (PDF file provided)
Additional text: William Stallings (2010) *Cryptography and Network Security Principles and Practice (6th Edition*) (PDF file provided). Supplemental books by Lisa Bock and Jean-Phillipe Aumasson (PDFs provided)
Catalog Description: 3 Credit Hours, Pre-req: Approval from Instructor. This course introduces fundamental topics in cryptography, including symmetric cryptography, historical ciphers, the data encryption standard, DES, the advanced encryption standard, and asymmetric, especially PKI. Special focus for DOE interns will include Federal Standards.

Goals and Objectives: Each student who successfully completes this course should be able to:

1. Obtain a firm grasp of cryptography concepts and become confident contributor to Cybersecurity community
2. Describe the purpose of cryptography and list ways it is used in data communications.
3. Define the following terms: cipher, cryptanalysis, cryptographic algorithm, and cryptology, and describe the two basic methods (ciphers) for transforming plain text in cipher text.
4. Explain how public key infrastructure supports digital signing and encryption.
5. Summarize security definitions related to attacks on cryptographic primitives, attacker capabilities and goals.
6. Develop critical thinking and research skills, and a collaborative mindset.
7. Learn how to used PowerShell to write small security-based programs for Windows systems.
8. Expand overall thought process - thinking outside the box!!

Note: In addition to scheduled class meeting, there will be some required scheduled activities, field trips and assignments outside of classroom hours and an expectation of about 1.5 hours of daily homework and class prep.

Date (Slides File #)	Topic
June Week 5.3 (0,1)	Chapter 1. (Ferguson) The Context of Cryptography
July Week 1.1 (2)	Chapter 2. (Stallings) Classical Encryption Techniques
July Week 1.2 (3)	Chapter 2. (Ferguson) Introduction to Cryptography (CISA Speaker)
July Week 1.3	Insurance company Audit Report Prep. Finish Poster 1, Draft Poster 2. Independent study.
July Week 2.1 (4) Poster 2 Finalization	Chapters 3-4. (Ferguson) Block Ciphers, Block Cipher Modes, Stream Ciphers Chapters 5-6. (Ferguson, Hudson) Hash Functions, Message Authentication Codes
July Week 2.2 (5)	Chapter 21. (Ferguson) Storing Secrets (SRNS IT/Cyber Speaker)
July Week 2.2 (6)	Chapter 8-9. (Ferguson) Implementation Issues, Generating Randomness Chapter 7. (Stallings) Chapter 10 (Ferguson), Chapter 8 (Stallings) Primes
July Week 2.3 (7)	Chapter 8. (Bock) PKI (In Depth) Insurance company Audit Report Draft
July Week 3.1 (8)	Chapter 7. (Ferguson) Secure Channel Chapter 17 (Stallings) TLS and VPN (Hudson)
July Week 3.2 (9)	Lesson 9. (Stallings) Chapters 18.1-18.2 and 19.1-19.2 Wireless, Mobile, Email Security
July Week 3.3 (10)	Lesson 10. (Hudson) Additional Topics and Protections (SRNL Tour?)
July Week 4.1 (11)	Lesson 11. (Hudson) Adhering to Standards… Putting it all together into a Summary Table SRNL Speaker2.
July Week 4.2	Practice Poster Presentations and Student Presentations. Review, Interviews, Final Assessments… Possible Cyber Conference in Augusta.

Course Assignments & Grading:

- Because each 3 hour lecture/discussion session is the equivalent of a week in a normal semester, we will only have time for a few in-class graded exercises. Similarly, attendance is mandatory, as missing one class results in missing 10% of the course. Remember, you are on a working/paid internship. **Please consider this to be your job.** Absences could reduce your grade even if test and homework scores are good.

University of South Carolina – Aiken Department of Mathematical Sciences
CSCI A285 Introduction to Cryptography– SRESFS Summer 2024 (4.10.24)

- I will emphasize the most important concepts in each chapter and we will discuss their application in real-world scenarios through brief case studies and labs. I will also cover topics that are not in the book, and there will be outside reading assignments and projects as well. Currently plan on 1.5 hours per class in homework assignments.

- I hate classes that require memorization of acronyms, what they mean, and who invented them. Unfortunately, there is the need to become conversant in about 30 acronyms in this course, but it will come naturally. I will focus on understanding concepts and applications of cryptography rather than the rigorous mathematical basis for the technology. At least 50% of the grade will come from homework assignments and projects. I will also conduct a 30-40 minute face to face interview with each student that will factor in my decision of final grades. My goal is to help you improve your communication skills along with your technical knowledge.

- Because of the rapid pace of the course, you should read the assignments before coming to class. It is OK if you only understand about 50% of the content. That is a good thing, because I will expect you to ask questions about what you didn't grasp so we can all learn together.

Grading Policies:

- *Late Work:* All assignments must be submitted by the due time (typically before the next class), no later than Friday 11PM EST of the week. Late assignments (on projects only) will only be accepted with 24 hour advance permission, if granted.
- *Make-Ups:* My goal is for you to learn, so we will work together to allow you to submit any incomplete work for consideration on your final grade.
- *Contesting:* Because I believe there is always more than one "right" answer, I encourage you to challenge my assessment if you disagree. But come prepared with facts, a quick wit, and collaborative attitude.

Grading scale: I believe all of you are A and B students and will satisfactorily complete all the assignments and quizzes. However, you can affect your grades by exhibiting the following behaviors.

F < 60% Bad attitude, slack attendance	D 60-70 Frequent absence, missing assignments	C 71-80 Attending and listening, but not contributing	B 81-90 Attending, listening, and contributing	A > 90 Attending, listening, and contributing and proposing alternative ideas. Completion of (ISC)2 Certified in Cybersecurity and passing the practice exam.

Students with Disabilities: Any student who desires accommodations for special needs should discuss this with the course instructor by the second class.
Academic Misconduct: We really do not expect it, so please do not disappoint us! However, any form of cheating will be penalized and may result in failing the course or eviction from the university.
Face-covering and Hygiene Requirements: Any student who has health and safety of our students should immediately notify the instructor or Internship coordinator.

- If a student becomes sick or feels he or she is becoming ill, that student should not come to campus. The student should immediately notify the course instructor and seek medical assistance/advice from the USC Aiken Student Health Center by calling 803-641-2840.

Computer and Communication Requirements:
• Each student must have regular access to a computer with a video camera and microphone; these may be required daily or only on occasion depending on the mode of instruction or the health status of the student or faculty. All students must be able to access and use Blackboard.
• Students must check their university email and Blackboard announcements each day.
• Each student must have internet access to receive notifications about the class and to complete assignments, if required by the instructor.