CS582: Applied Cryptography, Fall 2018
Weisberg Division of Computer Science
Marshall University

Course Information:

- Instructor: Dr. Cong Pu (Ph.D., Assistant Professor)
- Office: Weisberg Applied Engineering Complex (WAEC) 3109
- Phone: (304) 696-6204
- Email: puc@marshall.edu
- Course meetings: Tue/Thu, 11:00 a.m. – 12:15 p.m., WAEC 1103
- Tentative office hours: Mon, 2:00 p.m. – 4:00 p.m.
  Tue, 1:00 p.m. – 5:00 p.m.
  Thu, 1:00 p.m. – 5:00 p.m.
  Or by appointment.
- Course web page: (MUOnline) http://www.marshall.edu/muonline/. It is important to visit MUOnline regularly for up-to-date course information.

Course Description:

- This course introduces the basic aspects of modern cryptography, including block ciphers, pseudorandom functions, symmetric encryption, hash functions, message authentication, number-theoretic primitives, public-key encryption, digital signatures, as well as advanced cryptographic schemes.

Prerequisites:

- None

Course Student Learning Outcomes: The table below shows the following relationships: How each student learning outcomes will be practiced and accessed in the course.

Course Student Learning Outcomes	How students will practice each outcome in this course	How student achievement of each outcome will be assessed in this course
An ability to understand modern cryptographic primitives	Lecture Example In-class exercise Discussion	Assignment Review Quiz Exam Project
An ability to analyze the security strength of a given cryptographic scheme	Lecture Example In-class exercise Discussion	Assignment Review Quiz Exam Project
An ability to apply cryptographic primitives in designing software, protocols	Lecture Example In-class exercise Discussion	Assignment Review Quiz Exam Project

Preferred Communication Method and Expected Response Time:

- You can always see me during office hours. No appointment is required.
- You can generally expect an email response within 12 hours. If you don't get a response within 12 hours, please forward your previous email to me to remind me.
- You can generally expect the feedback on assignment, review quiz, and exam in one week after submission. If you don't receive the feedback in two weeks, please send an email to me.

Required Textbooks, Additional Reading, and Other Materials:

- A list of reference books will be used. For more information, please refer to the following resources:
    - William Stallings. Cryptography and Network Security: Principles and Practice. Pearson. 7th Edition. ISBN-10: 0134444280. ISBN-13: 978-0134444284.
    - Jonathan Katz, Yehuda Lindell. Introduction to Modern Cryptography. Chapman and Hall/CRC. 2nd Edition. ISBN-10: 1466570261. ISBN-13: 978-1466570269.
    - Bruce Schneier. Applied Cryptography: Protocols, Algorithms and Source Code. Wiley. ISBN-10: 1119096723. ISBN-13: 978-1119096726.
- Important concepts/materials will be included in the lecture notes from various sources, and posted on MUOnline.

Course Requirements and Grading Policy:

- **1st Midterm Exam: 15%, Oct 02 (Tuesday), 11:00 a.m. - 12:15 p.m., WAEC 1103**
- **2nd Midterm Exam: 15%, Nov 01 (Thursday), 11:00 a.m. - 12:15 p.m., WAEC 1103**
- **Final Exam: 15%, Dec 13 (Thursday), 10:15 a.m. – 12:15 p.m., WAEC 1103**
    - Closed book and closed notes. You are required to bring your student ID for the exams.
    - There will be **NO** make-up for missing exam. Only university excused absences with appropriate **DOCUMENTATION** will be accepted for make-up exam.
    - If you want to take a conflict exam, you must talk to instructor and provide a valid document at least two weeks before the scheduled exam. The conflict exam must be taken within two days after the scheduled exam.
- **Review Quiz: 15%**
    - Review quiz will **NOT** be announced in advance, so attendance is highly required.
    - There will be **NO** make-up for missing review quiz. Only university excused absences with appropriate **DOCUMENTATION** will be accepted for make-up review quiz.
- **Homework: 25%**
    - Homework should be **SUBMITTED** on **Blackboard** before deadline. Other submission methods will **NOT** be accepted.
    - **LATE** submission will **NOT** be accepted on Blackboard, since the submission link will be closed automatically.
- **Team Project: 15%**
    - Team project should be **SUBMITTED** on **Blackboard** before deadline. Other submission methods will **NOT** be accepted.
    - **LATE** submission will **NOT** be accepted on Blackboard, since the submission link will be closed automatically.
    - Each team can have a maximum of two members.

    - Instructor expect and encourage **Equal** contribution and participation to team project. However, all the contribution related issues will be solved by team members only, without instructor involvement.
- Plagiarism Detection:
    - Plagiarism or cheating will not be tolerated and will result in immediate dismissal (F grade).
- Grade Scale:
    - A (100 - 90), B (89 - 80), C (79 - 70), D (69 - 60), and F (59 - 0)

Attendance and Classroom Policy:

- Students are expected to attend punctually all class meetings, from the beginning of the semester until the end of the semester. **After THREE unexcused absences, your grade will be decreased by ONE letter grade and for every two absences afterwards.**
- If a student misses a class without university excused absence, the student should not expect individualized instruction what was missed. This will be effective from the beginning of semester.
- Students are expected to assist in maintaining a classroom environment that is conducive to learning. In order to assure that all students have the opportunity to gain from time spent in class, unless otherwise approved by the instructor, students are prohibited from engaging in any other form of distraction. Inappropriate behavior in the classroom shall result, minimally, in a request to leave class.
- Inappropriate behaviors include but not limited to:
    - Late for class
    - Sleeping during class
    - Leaving without proper excuse
    - Web surfing, chatting, or gaming on electric devices

Marshall University Policy: By enrolling in this course, you agree to the University Policies. Please read the full text of each policy (listed below) by going to Academic Affairs: Marshall University Policies. (URL: http://www.marshall.edu/academic-affairs/policies/)

- Academic Dishonesty Policy
- Academic Dismissal Policy
- Academic Forgiveness Policy
- Academic Probation and Suspension Policy
- Affirmative Action Policy
- Dead Week Policy
- D/F Repeat Rule
- Excused Absence Policy for Undergraduates
- Inclement Weather Policy
- Sexual Harassment Policy
- Students with Disabilities (Policies and Procedures)
- University Computing Services Acceptable Use Policy

Course Schedule: Topics and/or dates may be changed during the semester at the instructor's discretion because of scheduling issues, developments in the discipline, or other contingencies.

- Aug 21: Welcome & Computer and Network Security Concepts
- Aug 23: Computer and Network Security Concepts
- Aug 28: Introduction to Number Theory
- Aug 30: Introduction to Number Theory
- Sep 04: Classical Encryption Techniques
- Sep 06: Classical Encryption Techniques
- Sep 11: Block Ciphers and Data Encryption Standard
- Sep 13: Block Ciphers and Data Encryption Standard
- Sep 18: Block Ciphers and Data Encryption Standard
- Sep 20: Advanced Encryption Standard
- Sep 25: Advanced Encryption Standard
- Sep 27: Advanced Encryption Standard
- **Oct 02: 1st Midterm Exam, 11:00 a.m. - 12:15 p.m., WAEC 1103**
- Oct 04: Block Cipher Operation
- Oct 09: Block Cipher Operation
- Oct 11: Block Cipher Operation & Random Bit Generation and Stream Ciphers
- Oct 16: Random Bit Generation and Stream Ciphers
- Oct 18: Random Bit Generation and Stream Ciphers
- Oct 23: Public Key Cryptography and RSA
- Oct 25: Public Key Cryptography and RSA
- Oct 30: Public Key Cryptography and RSA
- **Nov 01: 2nd Midterm Exam, 11:00 a.m. - 12:15 p.m., WAEC 1103**
- Nov 06: Cryptographic Hash Functions
- Nov 08: Cryptographic Hash Functions
- Nov 13: Message Authentication Codes
- Nov 15: Message Authentication Codes
- **Nov 20: Thanksgiving Break – University Closed**
- **Nov 22: Thanksgiving Break – University Closed**
- Nov 27: Digital Signatures
- Nov 29: Digital Signatures
- Dec 04: "Dead week"
- Dec 06: "Dead week"
- **Dec 13: Final Exam, 10:15 a.m. – 12:15 p.m., WAEC 1103**