CYBR625: Applied Cryptography, Fall 2019
Weisberg Division of Computer Science
Marshall University

Course Information:

- Instructor: Dr. Cong Pu (Ph.D., Assistant Professor)
- Office: Weisberg Applied Engineering Complex (WAEC) 3109
- Office Phone: (304) 696-6204
- Email: puc@marshall.edu
- Website: http://mupfc.marshall.edu/~puc/
- Course meetings: Tue/Thu, 11:00 a.m. – 12:15 p.m., WAEC 2241
- Tentative office hours: Tue, 8:00 a.m. – 11:00 a.m., 2:00 p.m. – 4:00 p.m.
  Thu, 8:00 a.m. – 11:00 a.m., 2:00 p.m. – 4:00 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
Students will be able to understand modern cryptographic primitives	Lecture Example discussion In-class exercise	Assignment Review Quiz Exam
Students will be able to analyze the security strength of a given cryptographic scheme	Lecture Example discussion In-class exercise	Assignment Review Quiz Exam
Students will be able to apply cryptographic primitives in designing software, protocols	Lecture Example discussion In-class exercise	Assignment Review Quiz Exam

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 Exam: 15%, Oct 03 (Thursday), 11:00 a.m. - 12:15 p.m., WAEC 2241**
- **2nd Exam: 15%, Oct 31 (Thursday), 11:00 a.m. - 12:15 p.m., WAEC 2241**
- **3rd Exam: 15%, Dec 12 (Thursday), 10:15 a.m. – 12:15 p.m., WAEC 2241**
    - All three exams are **computer-based exam**. You have to bring your own device or use the computer in the classroom.
    - Closed book and closed notes, no Internet resources allowed.
    - 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 due to absence, lateness, etc.. Only university excused absences with appropriate and official **DOCUMENTATION** will be accepted for make-up review quiz. The make-up review quiz must be taken within two days after the scheduled quiz.
- **Assignment: 40%**
    - Assignment should be **SUBMITTED on Blackboard before Due Date**. *Other submission methods will NOT be accepted.*
    - **LATE Submission will NOT Be Accepted on Blackboard**, since the submission link will be closed automatically after due date.
- Plagiarism:
    - Plagiarism or cheating will not be tolerated in the class.
        - 1st plagiarism will result in zero point in the suspected work.
        - 2nd plagiarism will result in immediate dismissal (F grade).
- All grades will be posted on Blackboard:
    - Mid-term grade will be posted before October 7 (Monday)

        - October 25 (Friday), last day to drop an individual course. Fall semester 2019 calendar: https://www.marshall.edu/academic-calendar/fall-2019-semester/
- Grade Scale:
    - Actual points received in each category should be converted into category percentage.
    - A (100 - 90), B (89 - 80), C (79 - 70), D (69 - 60), and F (59 - 0)
- Bonus Points & Extra Credits:
    - Throughout the semester, the instructor will create certain **voluntary** work for **all** students to get bonus points. However, the instructor will only reward the students who complete the **voluntary** work.

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.
- 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 27: Welcome
- Aug 29: Computer and Network Security Concepts
- Sep 03: Introduction to Number Theory
- Sep 05: Classical Encryption Techniques
- Sep 10: Classical Encryption Techniques
- Sep 12: Block Ciphers and Data Encryption Standard
- Sep 17: Block Ciphers and Data Encryption Standard
- Sep 19: Block Ciphers and Data Encryption Standard
- Sep 24: Advanced Encryption Standard
- Sep 26: Advanced Encryption Standard
- Oct 01: Advanced Encryption Standard
- **Oct 03: 1st Exam. Thursday, 11:00 a.m. - 12:15 p.m., WAEC 2241**
- Oct 08**:** Block Cipher Operation
- Oct 10: Block Cipher Operation
- Oct 15: Block Cipher Operation & Random Bit Generation and Stream Ciphers
- Oct 17: Random Bit Generation and Stream Ciphers
- Oct 22: Random Bit Generation and Stream Ciphers & Public Key Cryptography and RSA
- Oct 24: Public Key Cryptography and RSA
- Oct 29: Public Key Cryptography and RSA
- **Oct 31: 2nd Exam. Thursday, 11:00 a.m. - 12:15 p.m., WAEC 2241**
- Nov 05: Cryptographic Hash Functions
- Nov 07**:** Cryptographic Hash Functions
- Nov 12: Message Authentication Codes
- Nov 14: Message Authentication Codes
- Nov 19: Digital Signatures
- Nov 21: Digital Signatures
- **Nov 26: Thanksgiving Break – University Closed**
- **Nov 28: Thanksgiving Break – University Closed**
- Dec 03: "Dead week"
- Dec 05: "Dead week"
- **Dec 12**: **3rd Exam. Thursday, 10:15 a.m. – 12:15 p.m., WAEC 2241**