CMSC 415: Introduction to Cryptography (Fall 2022)

Instructor: Dr. Hong-Sheng Zhou, http://www.people.vcu.edu/~hszhou
Office hours: Tuesdays & Thursdays, 12:30 – 1:30 pm, East Hall E4240, by appointment; additional office hours may be offered upon requests.
Class hours: Tuesdays & Thursdays, 2:00pm -- 3:15pm, West Hall 106

Semester course; 3 lecture hours. 3 credits.

1. Course Description

Cryptography has a very long and exciting history; more importantly, it has widely been used in real world computer and communication systems. This course offers an introduction to this fascinating and important subject.

Over decades, cryptography has been transformed from an "art" to a "science" and we will follow a rigorous approach to modern cryptography. We set out the formal definitions to be able to investigate perfectly-secret and computationally secure encryption, pseudorandomness, message authentication codes and hash functions. We then turn to another important aspect, public-key cryptography, and investigate key exchange protocols, public-key encryption and digital signatures. Through these important topics, we will learn basic tools, techniques, and methods for designing and analyzing cryptographic schemes.

2. Learning Outcomes

- ✓ Develop an understanding of modern cryptography theory.
- ✓ Provide an introduction to important aspects of private-key and public-key cryptography.
- ✓ Learn basic tools for designing cryptographic schemes
- ✓ Learn reasoning techniques for analyzing/proving the security of concrete constructions.
- ✓ Develop the skill to model the security concerns in real world information systems.

3. ABET Criteria Addressed:

1. Analyze a complex computing problem and to apply principles of computing and other relevant disciplines to identify solutions.

5. Function effectively as a member or leader of a team engaged in activities appropriate to the program's discipline.

4. Prerequisites CMSC 401 with a grade of C or better

The course is designed as an advanced undergraduate course. Students are expected to have attained "mathematical maturity" by completing the standard sequence of math courses in the undergraduate level.

5. Textbooks

We suggest students to have the textbook "Introduction to Modern Cryptography" by Jonathan Katz and Yehuda Lindell, 3rd Edition. (Earlier editions of the textbook also work.) Most of course material will be covered by the textbook.

6. Tentative Topics and Schedule

- Classical vs. modern cryptography; principles of modern cryptography; perfectly secret encryption;
- Computational security; Symmetric-key encryption; pseudorandomness;
- Message authentication and hash functions;
- Number theory; cryptographic hardness assumptions and their applications;
- The public-key revolution; Diffie-Hellman key exchange;
- Public-key encryption;
- Digital signatures;
- Additional topics

6. Course Evaluation

ACTIVITIES	PERCENTAGES
Homework	**50%**
Attendance	**5%**
Midterm Exam	**20%**
Final Exam	**25%**

Final grade: A (90% - 100%), B (80% - 89%), C(70% - 79%), D(60%-69%), F(0% - 59%)

Homework: There will be 6 homework assignments.

Midterm Exam: There will be 1 midterm exam.

Final Exam: There will be 1 final exam.

Late submission: At most 10 late submission days will be allowed for the first 5 homework assignments in total. No late submission is allowed for the last homework assignment.

Attendance and class participation: You will be expected to attend class regularly in the classroom.

7. Statements for Syllabi and Blackboard Pages

The topics are:

1. VCU Email Policy
2. VCU Honor System: Upholding Academic Integrity
3. Student Conduct in the Classroom
4. Students with Disabilities
5. Statement on Military Short-Term Training or Deployment
6. Excused Absences for Students Representing the University
7. Campus Emergency Information
8. Important Dates
9. VCU Mobile
10. Class registration required for attendance

Email Policy

Electronic mail or "email" is considered an official method for communication at VCU because it delivers information in a convenient, timely, cost effective and environmentally aware manner. Students are expected to check their official VCU e-mail on a frequent and consistent basis in order to remain informed of university-related communications. The University recommends checking e-mail daily. Students are responsible for the consequences of not reading, in a timely fashion, university-related communications sent to their official VCU student e-mail account. This policy ensures that all students have access to this important form of communication. It ensures students can be reached through a standardized channel by faculty and other staff of the university as needed. Mail sent to the VCU email address may include notification of university-related actions, including disciplinary action. Please read the policy in its entirety: http://www.ts.vcu.edu/kb/3407.html

VCU Honor System: Upholding Academic Integrity

The VCU honor system policy describes the responsibilities of students, faculty and administration in upholding academic integrity, while at the same time respecting the rights of individuals to the due process offered by administrative hearings and appeals. According to this policy, "members of the academic community are required to conduct themselves in accordance with the highest standards of academic honesty and integrity." In addition, "All members of the VCU community are presumed to have an understanding of the VCU Honor System and are required to:

- Agree to be bound by the Honor System policy and its procedures;
- Report suspicion or knowledge of possible violations of the Honor System;
- Support an environment that reflects a commitment to academic integrity;
- Answer truthfully when called upon to do so regarding Honor System cases, and,
- Maintain confidentiality regarding specific information in Honor System cases."

The Honor System in its entirety can be reviewed on the Web at http://www.provost.vcu.edu/pdfs/Honor_system_policy.pdf or it can be found in the current issue of the VCU Insider at http://www.students.vcu.edu/insider.html

Student Conduct in the Classroom

According to the *Faculty Guide to Student Conduct in Instructional Settings* (http://www.assurance.vcu.edu/Policy%20Library/Faculty%20Guide%20to%20Student%20Conduct%20in%

20Instructional%20Settings.pdf), "The university is a community of learners. Students, as well as faculty, have a responsibility for creating and maintaining an environment that supports effective instruction. In order for faculty members (including graduate teaching assistants) to provide and students to receive effective instruction in classrooms, laboratories, studios, online courses, and other learning areas, the university expects students to conduct themselves in an orderly and cooperative manner." Among other things, cell phones and beepers should be turned off while in the classroom. Also, the university Rules and Procedures prohibit anyone from having "in his possession any firearm, other weapon, or explosive, regardless of whether a license to possess the same has been issued, without the written authorization of the President of the university..." For more information, visit the VCU Insider online at http://www.students.vcu.edu/insider.html

Students with Disabilities

SECTION 504 of the Rehabilitation Act of 1973 and the Americans with Disabilities Act of 1990 as amended, require that VCU provides "academic adjustments " or "reasonable accommodations" to any student who has a physical or mental impairment that substantially limits a major life activity. To receive accommodations, students must request them by contacting the Disability Support Services Office on the Monroe Park Campus (828-2253) or the Division for Academic Success on the MCV campus (828-9782). More information is available at the Disability Support Services webpage: http://www.students.vcu.edu/dss/ ; or the Division for Academic Success webpage at www.specialservices.vcu.edu/disabilityss.

If you have a disability that requires an academic accommodation, please schedule a meeting with me at your earliest convenience. Additionally, if your coursework requires you to work in a lab environment, you should advise your instructor or a department chairperson of any concerns you may have regarding safety issues related to your disability. This statement applies not only to this course but also to every other course in this university.

Statement on Military Short-Term Training or Deployment

If military students receive orders for short-term training or deployment, they should inform and present their orders to Military Student Services and to their professor(s). For further information on policies and procedures contact Military Services at 828-5993 or access the corresponding policies at http://www.pubapps.vcu.edu/bulletins/about/?Default.aspx?uid=10096&iid=30704 and http://www.pubapps.vcu.edu/BULLETINS/undergraduate/?uid=10096&iid=30773.

Excused Absences for Students Representing the University

Students who represent the university (athletes and others) do not choose their schedules. Student athletes are required to attend games and/or meets. All student athletes should provide their schedule to the instructor at the beginning of the semester. The Intercollegiate Athletic Council (IAC) strongly encourages faculty to treat missed classes or exams (because of a scheduling conflict) as excused absences and urges faculty to work with the students to make up the work or exam.

Campus Emergency information

What to Know and Do To Be Prepared for Emergencies at VCU:

- Sign up to receive VCU text messaging alerts (http://www.vcu.edu/alert/notify). Keep your information up-to-date. Within the classroom, the professor will keep his or her phone on to receive any emergency transmissions.

- Know the safe evacuation route from each of your classrooms. Emergency evacuation routes are posted in on-campus classrooms.
- Listen for and follow instructions from VCU or other designated authorities. Within the classroom, follow your professor's instructions.
- Know where to go for additional emergency information (http://www.vcu.edu/alert).
- Know the emergency phone number for the VCU Police (828-1234). Report suspicious activities and objects.

Important Dates

Important dates for the Fall 2016 semester are available at:

http://academiccalendars.vcu.edu/ac_fullViewAll.asp?term=Fall+2016

VCU Mobile

The VCU Mobile application is a valuable tool to get the latest VCU information on the go. The application contains helpful information including the VCU directory, events, course schedules, campus maps, athletics and general VCU news, emergency information, library resources, Blackboard and more. To download the application on your smart phone or for more information, please visit http://m.vcu.edu.

Class Registration Required for Attendance

Please remember that students may only attend those classes for which they have registered. Faculty may not add students to class rosters. Therefore, if students are attending a class for which they have not registered, they must stop attending.