ECE 646, Applied Cryptography
Fall 2021

Instructor

Dr. Kris Gaj
The Nguyen Engineering Building, room 3225
E-mail: kgaj@gmu.edu
Office hours: By appointment.
Using Zoom. Please send an e-mail request or private Piazza request, including your availability in the form of a list of days and time slots suitable for you. I will select one particular day and starting time of the meeting, and I will send you the corresponding Zoom link.
During the conference call, please make sure to have your camera on and an ability to share your screen.

Teaching Assistant

Sreenitha Kasarapu
E-mail: skasarap@gmu.edu

Lecture

Thursdays 7:20-10:00 PM, Engineering Building, room 1107

Web Page

https://people-ece.vse.gmu.edu/~kgaj →
click on ECE 646 Applied Cryptography

Communication

Please use Piazza instead of e-mail for asking questions and holding discussions related to this class. Please submit all your homework and project reports using Blackboard by going to https://mymason.gmu.edu.

Course description

Topics include need for security services in computer networks and digital devices, basic concepts of cryptology, modern symmetric ciphers, public key cryptography (RSA, elliptic curve cryptosystems, post-quantum cryptography), data integrity and authentication, digital signature schemes, key exchange and key management, standard protocols for secure mail, the web and electronic payments, security aspects of mobile communications, efficient software and hardware implementations of cryptographic primitives, attacks against implementations and relevant defenses, requirements for implementation and validation of cryptographic modules, and security engineering with cryptography.

Recommended Prerequisite

ECE 542 or CS 555 or CYSE 610 or INFS 612 or permission of instructor

Tentative Schedule (subject to possible modifications)

No.	Subject	Date
1.	Organization of the course. Proposed project topics.	08/26/2021
2.	Basic concepts of cryptography. Types of cryptosystems.	09/02/2021
3.	Implementation of security services using cryptographic primitives.	09/09/2021
4.	Key management.	09/16/2021
5.	Public-key certificates and public-key infrastructure. Mathematical background and its applications – Part 1	09/23/2021
6.	Mathematical background and its applications – Part 2.	09/30/2021
	Historical ciphers. Enigma. One-time pad. DES.	10/07/2021
7.	Modern secret-key cryptography. Cryptographic competitions & standards. AES.	10/14/2021
8.	Hash functions and Message Authentication Codes. Authenticated ciphers.	10/21/2021
9.	**Midterm Exam**	**10/28/2021**
10.	Public-key cryptography algorithms. RSA. DSA.	11/04/2021
11.	Elliptic Curve Cryptosystems.	11/11/2021
12.	Post-Quantum Cryptography. Public-key encryption, digital signature and key encapsulation mechanism schemes.	11/18/2021
13.	Applications of Cryptography: TLS. Secure implementations. Validation and use of cryptographic modules.	12/02/2021
15.	**Final Exam**	**12/09/2021**

Homework

Homework assignments will be posted on the course web page at least 7 days before a given assignment is due.

Each student can have an automatic 72-hour extension on one assignment, no questions asked, as long as the student informs the instructor in writing.
Any additional late assignments will earn a flat 20% grade deduction as long as they are completed within 7 days of the deadline.

Exams

All exams will be take-home, open-book, open-notes. They may involve using educational cryptographic software. You must not communicate with anybody by any means during the exam! You must not submit any document or code you have not created entirely by yourself without citing its source!

Lab

Lab assignments will involve getting familiar with selected implementations of cryptographic algorithms and protocols. Students will be asked to solve a set of problems involving the use of educational software, web and smartphone applications, or open source-cryptographic libraries. Students will then prepare a short report including answers to questions included in the corresponding instructions. All lab assignments can be done at home, at student's own speed.

Project

Project can be done in a team of 1-3 students. Students can choose a project topic from a list of topics suggested by the instructor, posted on the course website. They can also suggest a project topic by themselves. Projects can be of different types: software, hardware, analytical, and mixed. All types of projects are expected to involve some experiments and literature search. Students will be asked to write a project specification, deliver bi-weekly project reports, give a project presentation, and develop a comprehensive project report.

Grading

Homework	10%
Laboratory	10%
Project	35%
Midterms Exam	20%
Final Exam	25%
Class & Piazza Activity:	up to 5% bonus

Literature

Required Textbooks

William Stallings, *Cryptography and Network Security: Principles and Practice*, 8th ed. Pearson, 2020 or 7th ed. Prentice Hall, 2017.

Supplementary Textbooks

- Alfred J. Menezes, Paul C. van Oorschot, and Scott A. Vanstone, *Handbook of Applied Cryptography*, CRC Press, Inc. (available online at http://cacr.uwaterloo.ca/hac).
- Christof Paar and Jan Pelzl, *Understanding Cryptography: A Textbook for Students and Practitioners*, 1st ed., Springer, 2010.

Basic Course Technology Requirements

Activities and assignments in this course will regularly use the Blackboard learning system, available at https://mymason.gmu.edu. Students are required to have regular, reliable access to a computer with an updated operating system (recommended: Windows 10 or Mac OSX 10.13 or higher) and a stable broadband Internet connection (cable modem, DSL, satellite broadband, etc., with a consistent 1.5 Mbps [megabits per second] download speed or higher.

Activities and assignments in this course will regularly use web-conferencing software:

- Zoom for office hours and project meetings.

In addition to the requirements above, students are required to have a device with a functional camera and microphone. In an emergency, students can connect through a telephone call, but video connection is the expected norm.

Academic Integrity

The integrity of the University community is affected by the individual choices made by each of us. Mason has an Honor Code with clear guidelines regarding academic integrity. Three fundamental and rather simple principles to follow at all times are that: (1) all work submitted be your own; (2) when using the work or ideas of others, including fellow students, give full credit through accurate citations; and (3) if you are uncertain about the ground rules on a particular assignment, ask for clarification. No grade is important enough to justify academic misconduct. Plagiarism is the equivalent of intellectual robbery and cannot be tolerated in the academic setting. If you have any doubts about what constitutes plagiarism, please see me.

For more information about the Mason Honor Code and about the Honor Committee, please visit the website for the Office of Academic Integrity (http://oai.gmu.edu).

Safe Return to Campus

All students taking courses with a face-to-face component are required to follow the university's public health and safety precautions and procedures outlined on the university Safe Return to Campus webpage (https://www2.gmu.edu/safe-return-campus). Similarly, all students in face-to-face and hybrid courses must also complete the Mason COVID Health Check daily, seven days a week. The COVID Health Check system uses a color code system and students will receive either a Green, Yellow, or Red email response. Only students who receive a "green" notification are permitted to attend courses with a face-to-face component. If you suspect that you are sick or have been directed to self-isolate, please quarantine or get testing. Faculty are allowed to ask you to show them that you have received a Green email and are thereby permitted to be in class.

Students are required to follow Mason's current policy about facemask-wearing. As of August 11, 2021, all community members are required to wear a facemask in all indoor settings, including classrooms. An appropriate facemask must cover your nose and mouth at all times in our classroom. If this policy changes, you will be informed; however, students who prefer to wear masks either temporarily or consistently will always be welcome in the classroom.