**ECE 646, Applied Cryptography**
**Fall 2020**

## Instructor

Dr. Kris Gaj
E-mail: kgaj@gmu.edu
Office hours: Monday 5:00-6:00 PM, Wednesday 8:30-9:30 PM,
Thursday 5:00-6:00 PM, and by appointment
*Using Zoom. Please send an e-mail request or a private Piazza request, including the day and time slot suitable for you.*

## Lecture

Wednesday 4:30-7:10 PM
*Online, in synchronous mode, using Blackboard Collaborate Ultra.*
*In order to join, please go to myMason (https://mymason.gmu.edu), log in to Blackboard (Mason Bb Login), choose the course ECE-646-001 (Fall 2020), and click on Collaborate Ultra in the left menu.*

## Web Page

https://people-ece.vse.gmu.edu/~kgaj → click on ECE 646 Applied Cryptography, *or*
https://people-ece.vse.gmu.edu/coursewebpages/ECE/ECE646/F20/

## 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. Basic concepts of cryptography. | 08/26/2020 |
| 2. | Types of cryptosystems. Implementation of security services using cryptographic primitives. | 09/02/2020 |
| 3. | Key management. Public-key certificates and public-key infrastructure. | 09/09/2020 |
| 4. | Applications of cryptography. | 09/16/2020 |
| 5. | Mathematical background and its applications. | 09/23/2020 |
| 6. | Historical ciphers. Enigma. One-time pad. DES. | 09/30/2020 |
| 7. | Modern secret-key cryptography. Cryptographic competitions & standards. AES. | 10/07/2020 |
| 8. | Hash functions and Message Authentication Codes. Authenticated ciphers. | 10/14/2020 |
| **9.** | **Midterm Exam** | **10/21/2020** |
| 10. | Public-key cryptography algorithms. RSA. DSA. | 10/28/2020 |
| 11. | Elliptic Curve Cryptosystems. | 11/04/2020 |
| 12. | Post-Quantum Cryptography. Public-key encryption, digital signature and key encapsulation mechanism schemes. | 11/11/2020 |
| 13. | Implementing major operations of secret-key and public-key ciphers in software and hardware. Generation and storage of keys. | 11/18/2020 |
| 14. | Side-channel attacks and countermeasures against these attacks. Secure high-speed and lightweight implementations. Validation and use of cryptographic modules. | 12/02/2020 |
| **15.** | **Final Exam** | **12/09/2020** |

**Homework**

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

*Considering the circumstances, the following late-submission options are available regarding homework assignments.*

- *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:

- Blackboard Collaborate Ultra for lectures
- 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.

**Online Learning Etiquette**

Students are required to mute themselves on joining an online session, and at all times while not actively communicating. The use of video is encouraged when asking questions or communicating with others.

**Course Materials and Student Privacy**

All of the lectures will be recorded to provide necessary information for students in this class. Recordings will be available by logging in to Blackboard Collaborate Ultra and will only be accessible to students taking this course during this semester.

All course materials posted to Blackboard Collaborate Ultra are private to this class; by federal law, any materials that identify specific students (via their name, voice, or image) must not be shared with anyone not enrolled in this class.
Videorecordings — whether made by instructors or students — of class meetings that include audio, visual, or textual information from other students are private and must not be shared outside the class.
Live video conference meetings (e.g., using Blackboard Collaborate Ultra or Zoom) that include audio, textual, or visual information from other students must be viewed privately and not shared with others in your household or recorded and shared outside the class.

**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).