## Course Information:

Course: CSCI 4331 / 6331 – Cryptography
Semester: Fall, 2020
Synchronous meeting time: Tuesdays, 12:45 – 3:15
Course webpage: https://www2.seas.gwu.edu/~arkady/teaching/crypto/f20/

**Instructor:**

Name: Arkady Yerukhimovich
Email: arkady@gwu.edu
Office hours: TBD

**Course description**

This course will introduce students to modern cryptography with a focus on formal definitions and provably-secure constructions of cryptographic protocols. Topics covered will include secret-key and public-key encryption, message-authentication codes, digital signatures, and advanced topics.

**Course prerequisites**

The main prerequisite for this course is a basic level of mathematical maturity. Students should feel comfortable with mathematical notation and be able to follow and apply mathematical reasoning. Basic familiarity with asymptotic notation, mathematical logic, and probability are recommended.

Suggested prerequisites to cover this material include:

For CSCI 4331:
CSCI 2312, CSCI 3212, CSCI 3313

For CSCI 6331:
CSCI 6212

**Learning outcomes**

As a result of completing this course, students will be able to:

1. Understand and differentiate between cryptographic definitions
2. Choose appropriate security definitions for given applications
3. Prove security of basic cryptographic constructions
4. Demonstrate familiarity with core building blocks of modern cryptography

**Average expected effort**

There will be approximately 1.5 hours of recorded lectures for students to watch each week. Additionally, students are expected to participate in the synchronous discussion to review the material, go over the homework, and for quizzes. In addition to watching the lectures and attending synchronous sessions, students are expected to spend approximately 5-10 hours per week on understanding the material and completing homework assignments.

**Textbooks**

Jonathan Katz, Yehuda Lindell: “Introduction to Modern Cryptography. Second Edition.” CRC Press 2014.

While this book is not strictly required, it is strongly recommended. The material covered will follow the book, and the book provides background and discussion that will not be covered in lectures.

## Technology for online instruction

This will be an entirely online class for the Fall 2020 semester. The material will be accessible as follows:

**Lectures**

All lectures will be pre-recorded and shared via Blackboard. Videos of the lectures along with a lecture outline, and the corresponding slides will be available immediately after the preceding synchronous class (i.e., lectures for week 2 material will be available after the synchronous session on week 1). Students are expected to watch all lectures prior to the synchronous session for the week.

**Synchronous sessions:**

The synchronous sessions will be held at 12:45PM on Tuesdays via Blackboard Collaborate Ultra (accessible under Tools in Blackboard). These sessions will be used to review material from the video lectures, review homework, and for quizzes. The synchronous sessions will be recorded and shared via Blackboard.

**Discussion Boards:**

The asynchronous discussion for the course will use Blackboard discussion boards (accessible under Discussions). These will be used to ask and answer questions about the video lectures.

**Homework:**

All homework will be posted, collected, and graded via Blackboard.

**Office Hours:**

Office hours will be held via Zoom.

## Grading

The grades for this course will be determined as follows:

| | |
|---|---|
| Exam | 25% |
| Research project | 25% |
| Homework | 40% |
| Class participation | 10% |

**Homework policy**

Homeworks will be assigned approximately every two weeks. Homeworks are due before class (by 12:45PM) on the due date. They must be submitted via Blackboard (https://blackboard.gwu.edu/) by this time to receive credit. Homeworks can be typed using your favorite tool (I am happy to help

anybody interested in learning LaTex) or handwritten and scanned. But, make sure that what you submit is legible as it is what will be graded. No late homeworks will be accepted!

Students are welcome to work together on homeworks, however each student must write up and submit their own solutions. If you work on the homework with someone else, you MUST acknowledge them on your submitted homework. Additionally, you may use outside resources (e.g., web search, other text books, lecture notes) to help with the homework. However, if you use any such resource, you MUST cite them appropriately. Moreover, the solutions you submit MUST be your own. Make sure to write-up your own answers and that you understand them, copying and pasting solutions is not acceptable. Submitted homeworks violating these guidelines will be considered in breach of the academic integrity code and will be prosecuted accordingly.

The final homework grade will be the average of all homework assignments with the lowest homework score dropped.

**Class Participation**

While the class will be entirely online, there is still an expectation of class participation. Students should make an effort to attend the synchronous sessions. However, the main avenue for participation will be via the discussion boards. The expectation is that students will use these boards to ask an answer questions about the week's lectures. Each week, each student should post at least one question and answer at least one other question on the bulletin board. Additionally, students may vote for questions to be discussed at the next synchronous session. These votes must be in by the Friday before.

**Exam**

There will be one take-home exam in this course.

**Research Project**

The students will complete a research project due at the end of the semester.

## Lecture schedule

The following is a tentative agenda for the course:

| Lecture | Topic(s): |
|---|---|
| Sep. 1 | Introductions, Syllabus review |
| Sep. 8 | Modern cryptography, probability review, perfectly secure encryption, one-time pad |
| Sep. 15 | Computationally-secure encryption, proofs by reduction, pseudorandom generators |
| Sep. 22 | PRG+OTP secure encryption, CPA security, pseudorandom functions, |
| Sep. 29 | Construction of CPA-secure encryption |
| Oct. 6 | CCA-secure encryption, modes of operation, padding oracle attack |
| Oct. 13 | Message authentication codes definitions and constructions, authenticated encryption, hash function definitions and applications |
| Oct. 20 | Practical constructions of symmetric-key primitives, DES, 3DES, AES, Feistel networks |
| Oct. 27 | Number theory, group theory |
| Nov. 3 | Cryptographic assumptions, Key exchange, Public-key encryption, Diffie-Hellman |
| Nov. 10 | El Gamal, RSA, Paillier, CCA security |

| | |
|---|---|
| Nov. 17 | Digital Signatures |
| Nov. 24 | Student project presentations |
| Dec. 1 | Advanced Topics, review for exam |

## University Policies

### Use of Electronic Course Materials and Class Recordings

Students are encouraged to use electronic course materials, including recorded class sessions, for private personal use in connection with their academic program of study. Electronic course materials and recorded class sessions should not be shared or used for non-course related purposes unless express permission has been granted by the instructor. Students who impermissibly share any electronic course materials are subject to discipline under the Student Code of Conduct. Please contact the instructor if you have questions regarding what constitutes permissible or impermissible use of electronic course materials and/or recorded class sessions. Please contact Disability Support Services if you have questions or need assistance in accessing electronic course materials.

### Academic Integrity Code

Academic Integrity is an integral part of the educational process, and GW takes these matters very seriously. Violations of academic integrity occur when students fail to cite research sources properly, engage in unauthorized collaboration, falsify data, and in other ways outlined in the Code of Academic Integrity. Students accused of academic integrity violations should contact the Office of Academic Integrity to learn more about their rights and options in the process. Outcomes can range from failure of assignment to expulsion from the University, including a transcript notation. The Office of Academic Integrity maintains a permanent record of the violation.

More information is available from the Office of Academic Integrity at studentconduct.gwu.edu/academic-integrity. The University's "Guide of Academic Integrity in Online Learning Environments" is available at studentconduct.gwu.edu/guide-academic-integrity-online-learning-environments. Contact information: rights@gwu.edu or 202-994-6757.

### University policy on observance of religious holidays

In accordance with University policy, students should notify faculty during the first week of the semester of their intention to be absent from class on their day(s) of religious observance. For details and policy, see "Religious Holidays" at provost.gwu.edu/policies-procedures-and-guidelines

### Support for students outside the classroom

### Virtual academic support

A full range of academic support is offered virtually in fall 2020. See coronavirus.gwu.edu/top-faqs for updates.

Tutoring and course review sessions are offered through Academic Commons in an online format. See academiccommons.gwu.edu/tutoring

Writing and research consultations are available online. See academiccommons.gwu.edu/writing-research-help

Coaching, offered through the Office of Student Success, is available in a virtual format. See studentsuccess.gwu.edu/academic-program-support

Academic Commons offers several short videos addressing different virtual learning strategies for the unique circumstances of the fall 2020 semester. See academiccommons.gwu.edu/study-skills. They also offer a variety of live virtual workshops to equip students with the tools they need to succeed in a virtual environment. See tinyurl.com/gw-virtual-learning

**Writing Center**

GW's Writing Center cultivates confident writers in the University community by facilitating collaborative, critical, and inclusive conversations at all stages of the writing process. Working alongside peer mentors, writers develop strategies to write independently in academic and public settings. Appointments can be booked online. See gwu.mywconline.

**Academic Commons**

Academic Commons provides tutoring and other academic support resources to students in many courses. Students can schedule virtual one-on-one appointments or attend virtual drop-in sessions. Students may schedule an appointment, review the tutoring schedule, access other academic support resources, or obtain assistance at academiccommons.gwu.edu.

**Disability Support Services (DSS)** 202-994-8250

Any student who may need an accommodation based on the potential impact of a disability should contact Disability Support Services to establish eligibility and to coordinate reasonable accommodations. disabilitysupport.gwu.edu

**Counseling and Psychological Services** 202-994-5300

GW's Colonial Health Center offers counseling and psychological services, supporting mental health and personal development by collaborating directly with students to overcome challenges and difficulties that may interfere with academic, emotional, and personal success. healthcenter.gwu.edu/counseling-and-psychological-services

**Safety and Security**

- In an emergency: call GWPD 202-994-6111 or 911
- For situation-specific actions: review the Emergency Response Handbook at safety.gwu.edu/emergency-response-handbook
- In an active violence situation: Get Out, Hide Out, or Take Out. See go.gwu.edu/shooterpret
- Stay informed: safety.gwu.edu/stay-informed