## Course Information

Course: CSCI 4331 / 6331 – Cryptography
Semester: Fall, 2021
Meeting time: Tuesdays, 12:45 – 3:15
Location: Duques Hall 251
Course webpage: https://www2.seas.gwu.edu/~arkady/teaching/crypto/f21/

### Instructor

Name: Arkady Yerukhimovich
Email: arkady@gwu.edu
Office: SEH 4570
Phone: (202)-994-1057
Office hours: M 10:00 – 11:00, W 2:00 – 3:00

### 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. Students will also learn how to read and understand academic papers in cryptography and how to give a technical presentation.

### 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:
Any of 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

In addition to 2.5 hours / week of lecture, 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.

The material of the course will largely follow the presentation in this book.

**Grading**

The grades for this course will be determined as follows:

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

The class will have one exam which will contribute 25% to your grade. Additionally, there will be a semester-long research project which will also count for 25% of your grade. The remaining 50% of the grade are for homework and class participation.

**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. 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.

**Laptop policy**

I ask that students not use laptops or other electronic devices in class. I will make sure to lecture at a pace that allows for hand-written notes. If you need to use an electronic device for taking notes, please come talk to me.

**Lecture schedule**

The following is a tentative agenda for the course:

| Lecture | Topic(s): |
|---|---|
| Aug. 31 | Introductions, Syllabus review, Private-Key encryption, Probability review |
| Sep. 7 | Perfectly secure encryption, one-time pad |
| Sep. 14 | Computationally-secure encryption, proofs by reduction, pseudorandom generators |

| | |
|---|---|
| Sep. 21 | PRG+OTP secure encryption, CPA security, pseudorandom functions |
| Sep. 28 | Construction of CPA-secure encryption |
| Oct. 5 | modes of operation, CCA-secure encryption, padding oracle attack |
| Oct. 12 | Message authentication codes definitions and constructions, authenticated encryption, hash functions |
| Oct. 19 | Practical constructions of symmetric-key primitives, DES, 3DES, AES, Feistel networks |
| Oct. 26 | Number theory, group theory, Cryptographic assumptions |
| Nov. 2 | Key exchange, Public-key encryption, Diffie-Hellman |
| Nov. 9 | Digital signatures |
| Nov. 16 | Advanced topics |
| Nov. 23 | Student project presentations |
| Nov. 30 | Advanced topics, Exam review |

## 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 at disabilitysupport.gwu.edu if you have questions or need assistance in accessing electronic course materials.

### University policy on observance of religious holidays

Students must notify faculty during the first week of the semester in which they are enrolled in the course, or as early as possible, but no later than three weeks prior to the absence, of their intention to be absent from class on their day(s) of religious observance. If the holiday falls within the first three weeks of class, the student must inform faculty in the first week of the semester. For details and policy, see “Religious Holidays” at provost.gwu.edu/policies-procedures-and-guidelines.

### 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.

## Academic support

### 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 at 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.

## Support for students outside the classroom

### 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 at disabilitysupport.gwu.edu to establish eligibility and to coordinate reasonable accommodations.

### 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