Course Information

Course: CSCI 3907-83 / 6907-82 – Advanced Cryptography
Semester: Spring, 2019
Meeting time: Wednesdays, 12:45 – 3:15
Location: District House B205
Course webpage: https://www2.seas.gwu.edu/~arkady/teaching/advanced_crypto/s19/

Instructor

Name: Arkady Yerukhimovich
Email: arkady@gwu.edu
Office: SEH 4570
Phone: (202)-994-1057
Office hours: TBD

Course description

This course will introduce students to modern research in cryptography. This is a seminar-style course with students reading and leading discussion on recent academic papers in the field. The course will teach students how to read, understand, and analyze academic papers and how to identify open problems for further research. There will also be a semester-long research project for students to apply the skills they have learned.

The course will cover two different active research topics in cryptography. The first is differential privacy, or how can we perform statistical analyses on large data sets while maintaining the privacy of the individuals whose data is contained in the datasets. The second topic will study the cryptography underlying blockchain technology. We will focus on the low-level protocols and algorithms to understand the properties that blockchain does and does not provide.

Course prerequisites

The main prerequisites for this course is mathematical maturity. Students should be able to follow rigorous mathematical concepts and proofs. Some background in algorithms and cryptography is recommended, but is not required. In particular, the intro cryptography course (CS 4331/6331) is NOT required.

Suggested prerequisites to cover this material include:

For CSCI 3907:
CSCI 2312, CSCI 3212, CSCI 3313

For CSCI 6907:
CSCI 6212

Learning outcomes

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

1. Read, understand, and analyze modern crypto research papers

2. Identify strengths and weaknesses of cryptographic constructions
3. Identify open questions based on recent crypto literature
4. Carry out independent research projects on topics in 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 reading papers and the research project.

Textbooks

None

Grading

The grades for this course will be determined as follows:

Participation in class discussions	30%
Paper presentations	30%
Research project	40%

University Policies

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: students.gwu.edu/accommodations-religious-holidays.

Academic integrity code

Academic dishonesty is defined as cheating of any kind, including misrepresenting one's own work, taking credit for the work of others without crediting them and without appropriate authorization, and the fabrication of information. For details and complete code, see: studentconduct.gwu.edu/code-academic-integrity

Support for students outside the classroom

Disability Support Services (DSS)

Any student who may need an accommodation based on the potential impact of a disability should contact the Disability Support Services office at 202-994-8250 in the Rome Hall, Suite 102, to establish eligibility and to coordinate reasonable accommodations. For additional information see: disabilitysupport.gwu.edu/

Mental Health Services 202-994-5300

The University's Mental Health Services offers 24/7 assistance and referral to address students' personal, social, career, and study skills problems. Services for students include: crisis and emergency mental health consultations confidential assessment, counseling services (individual and small group), and referrals. For additional information see: counselingcenter.gwu.edu/

Safety and security

In the case of an emergency, if at all possible, the class should shelter in place. If the building that the class is in is affected, follow the evacuation procedures for the building. After evacuation, seek shelter at a predetermined rendezvous location.