Course Information

Course: CSCI 4331 / 6331 – Cryptography
Semester: Fall, 2018
Meeting time: Mondays, 12:45 – 3:15
Location: Monroe Hall 113
Course webpage: https://www2.seas.gwu.edu/~arkady/teaching/crypto_fall18.html

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 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. 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.

We will use this textbook extensively. The material will follow the book, and homeworks will include problems from the book.

Grading

The grades for this course will be determined as follows:

Midterm exam	25%
Final exam	25%
Homework	40%
Class participation / quizzes	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 are welcome to use outside resources (e.g., web search, other text books, lecture notes) to help with the homework. However, if you use any such resources, you MUST cite them appropriately in your submitted work. Submitted homeworks violating these guidelines will be considered in breach of the academic integrity code.

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.

Lecture schedule

The following is a tentative agenda for the course:

Lecture	Topic(s):
Aug. 27	Probability and asymptotics review, principles of modern cryptography, perfect secrecy and the one-time pad
Sep. 3	Labor day – no class
Sep. 10	Computationally-secure encryption, proofs by reduction, pseudorandom generators and security of PRG+OTP encryption
Sep. 17	CPA security, pseudorandom functions, construction of CPA-secure encryption, modes of operation, CCA-security and padding oracle attacks

Sep. 24	Message authentication codes definitions and constructions, CBC-MAC, authenticated encryption
Oct. 1	Hash functions, Merkle-Damgard transform, HMAC, attacks on hash functions, applications of hash functions, random oracle model
Oct. 8	Fall break – no class
Oct. 15	Practical constructions of symmetric-key primitives, DES, 3DES, AES, Feistel networks
Oct. 22	Exam (in class)
Oct. 29	Linear and differential cryptanalysis
Nov. 5	Number theory, group theory, cryptographic assumptions, key exchange
Nov. 12	Public-key encryption, El Gamal, RSA, key-encapsulation mechanisms
Nov. 19	CCA security, RSA-OAEP, CCA security in the ROM
Nov. 16	Digital signatures, Hash-and-sign, Fiat-Shamir transform and Schnorr signatures, DSA
Dec. 3	Advanced topic I
Dec. 10	Advanced topic II
TBD	Final Exam

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.