Syllabus and More

CS 608 – Cryptography and Security Syllabus

Fall 2023

Instructor: Fuad Hamidli

Email: fuad.hamidli@njit.edu

Course website (on CANVAS): https://njit.instructure.com/courses/29056

Office hours: Tuesday 2:00-3:00 pm (Newark GITC 4202
or https://njit.webex.com/meet/fh224 Links to an external site.)

Also, by appointment via email.

Suggested Textbooks:

William Stallings, "Cryptography and Network Security: Principles and Practice", 7th Ed., 2017 (not mandatory).

Jonathan Katz; Yehuda Lindell, "Introduction to Modern Cryptography"

Dan Boneh, Victor Shoup, "A Graduate Course in Applied Cryptography"

Lecture material will be posted in Canvas. However, students are suggested to take notes, as there may be examples that do not appear in the slides.

Course in a nutshell: The goal is to study main modern symmetric-key and public-key cryptography algorithms with focus on their efficient implementation. Practical aspects of the algorithms, such as the bits of-security work factor and specific applications, are examined. The course covers algorithms based on discrete logarithm, RSA, elliptic curve discrete logarithm, and learning with errors problems. Advanced public-key cryptography protocols, such as attribute-based encryption and fully homomorphic encryption, are introduced.

Learning Outcomes

By the end of the course, students will be able to:

● SLO1. Understand the differences between the symmetric key and public key cryptography approaches.

● SLO2. Select appropriate symmetric and/or public key cryptography protocols for a given application.

● SLO3. Develop an efficient implementation of a cryptographic protocol based on a Discrete Logarithm Problem, RSA (Factoring) Problem, Elliptic Curve Discrete Logarithm Problem, or Learning with Errors Problem.

● SLO4. Perform correctness analysis of a given number-theory cryptographic algorithm.

● SLO5. Perform vulnerability assessment/penetration testing of perimeter security.

● SLO6. Give a presentation/talk on an advanced topic in cryptography/security based on critical analysis of scholarly papers or your own experiments.

Course Schedule

Class meetings: Students will be required to participate weekly (on Thursdays at 6:00 pm) in the course in the Newark campus.

Topic Assignment Due Dates

	Topic	**Assignment**	**Due Dates**
Week 1	Introduction to cryptography and security ● Security concepts ● Security problems ● Symmetric key & public key cryptography Basic symmetric key cryptography algorithms ● Substitution ciphers ● Columnar transposition cipher ● Permutation cipher ● Playfair cipher	→ Introduction Discussion: Introduce yourselves to your classmates. → Discussion topic: Explain when to choose symmetric key vs. public key cryptography and why.	9/10/23
	More complex/modern symmetric key cryptography algorithms	→ Discussion topic: Which variant of AES (AES-128, AES-192, or AES-256) should be chosen for a	

Week 2	● Work factor ● Data Encryption Standard (DES), Triple-DES ● Advanced Encryption Standard (AES) Block cipher modes of operation ● Electronic Codebook mode ● Cipher Block Chaining mode ● Feedback modes ● Counter mode	real application and why? Provide an example.	9/17/23
Week 3	Principles of public-key cryptography ● Public key encryption ● Digital signatures ● Ciphertext indistinguishability Number Theory ● Introduction to modular arithmetic ● Little Fermat Theorem ● Euler's Theorem	→ Discussion topic: Which block cipher mode is most secure/efficient for AES?	9/24/23
Week 4	Number Theory (Continued) ● Square-and-multiply exponentiation ● Multiplicative modular inverse/modular linear equation	→ Discussion topic: Why is ciphertext indistinguishability important for practical systems?	10/1/23

Week 5	Assignment		10/8/23

Week 6	Hard mathematical problems ● Discrete logarithm ● RSA/integer factoring Numerical representation of plaintext Diffie-Hellman key exchange	→ Discussion topic: Why are “difficult” m important for public key cryptography?
Week 7	Public key encryption schemes ● ElGamal public cryptosystem ● RSA public-key encryption Digital signature schemes ● ElGamal’s digital signature ● RSA digital signature	→ Discussion topic: Which cryptosyste RSA? Explain why.
Week 8	MIDTERM	
Week 9	Elliptic curve cryptography ● Introduction ● Elliptic curves over real numbers ● Elliptic curves over integers ● Modular square root	→ Discussion topic: What are the adva cryptography over DLP/RSAbased prot

Week 10	Elliptic curve cryptography algorithms ● Diffie-Hellman key exchange ● Menezes-Vanstone EC cryptosystem Access sharing protocols	→ Discussion topic: Discuss an applica
Week 11	Zero-knowledge proof ● Introduction ● Proof of identity (Quadratic residue authentication)	→ Discussion topic: Discuss the zero-k
Week 12	Security Definitions, Probability Theory, Perfect security, Stream Ciphers	→ Discussion topic: Discuss perfect se

Week 13	Pseudo-random Generators, Perfect Security	→ Discussion topic: What is semantic s application of semantic security in pract
Week 14	Pseudo-random Functions, Semantic Security, CCA Indistinguishability	→ Discussion topic: Can we construct I vice versa?
Week 15	FINAL EXAM	Will be announced

General Information

Netiquette

Throughout this course, students are expected to be courteous of classmates by being a polite, active participant. Students should respond to discussion forum assignments in a timely manner so classmates have adequate time to respond to your post. Respect opinions, even those that differ from your own and avoid using profanity or offensive language.

Grading

The conversion of numerical to letter grades is as follows:

[90,100)=A; [80,89.9)=B+; [70, 79.9)=B; [60, 69.9)=C+; [50; 59.9)=C; [0, 50)=F.

Final Grade Calculation:

Assignment	**20%**
Participation	**10%**
Midterm Exam	**35%**
Final Exam	**35%**

Course Work

Assignment: (20% of grade) The assignment will include 4 problems on symmetric-key cryptography and basic number theory algorithms. The input conditions will be different for each student. No programming is needed for this test.

Class participation: (10% of grade) Each week with lectures will have a discussion topic assignment. An initial response will be due by 11:59 PM on Sunday of the same week, a response to the comments of 2 peers will be due by 11:59 PM of the following Wednesday.

Midterm Exam: (35% of grade) The midterm test will have 5 problems on public-key cryptography algorithms. The input conditions will be different for each student. Along with the exam paper, every student will need to submit her own source code for (1) square-and-multiply modular exponentiation, (2) multiplicative modular inverse operation, (3) finding generators, and (4) finding greatest common divisor. The source code has to be written by each student independently and cannot be a group project.

Final Exam: (35% of grade)

1st part (Take home 10%) The final exam will have 4 problems on elliptic curve public-key cryptography, secret sharing schemes, and zero-knowledge proof. The input conditions will be different for each student. Along with the exam paper, every student will need to submit her own source code for (1) modular square root operation, (2) finding the order/all points on an elliptic curve, (3) scalar "multiplication" over elliptic curve, and (4) finding the generator point for an elliptic curve. The source code has to be written by each student independently and cannot be a group project.

2nd part (25% in the class) Will be written exam that covers all the topis.

Course Policies

Honor Code: The NJIT Student Council dictates **"**NJIT has a zero-tolerance policy for cheating of any kind and for student behavior that disrupts learning by others" The NJIT Student Senate has requested a zero-tolerance policy for cheating of any kind and for student behavior that disrupts learning. The Senate wants fairness for all students. The Dean of Students determines punishments and requires professors to report any incidents. The penalties include failure in the course plus disciplinary probation up to expulsion from NJIT. Avoid situations where anyone could misinterpret your behavior as dishonorable. Students are required to agree to the NJIT Honor Code on each exam, assignment, quiz, etc. for the course. Turn off all cellular phones, wireless devices, computers, and messaging devices of all kinds during classes and exams. Please do not eat, drink, or create noise in class that interferes with the work of other students or instructors.

Late work: No extensions are allowed unless there is an unusual circumstance (primarily of medical nature), and the students must contacts me before the assignment deadline.

Resources for NJIT Students

Technology Support:

IST Service Desk Links to an external site. Links to an external site.

The IST Service Desk is the central hub for computing information and first point of contact for getting help and reporting issues related to computing technology at NJIT.

Students can put in a ticket with the service desk: *https://servicedesk.njit.edu/CherwellPortal/IST*Links to an external site. Links to an external site. or call **(973) 596-2900** Monday - Friday from 8:00am – 9:00pm

Other Services:

Academic Advising Success CenterLinks to an external site. Links to an external site.

"...assist in the advisement of students who are undecided in their major, transitioning into another major at NJIT, and those students who need additional support to graduate successfully and in a timely manner."

Academic IntegrityLinks to an external site. Links to an external site."New Jersey Institute of Technology is an institution dedicated to the pursuit of knowledge through teaching and research. The university expects that its graduates will assume positions of leadership within their professions and communities. Within this context, the university strives to develop and maintain a high level of ethics and honesty among all members of its community. Imperative to this goal is the commitment to truth and academic integrity. This commitment is confirmed in this NJIT University Code on Academic Integrity."

Academic Support and Student AffairsLinks to an external site. Links to an external site.

"From questions about becoming a student at NJIT – to student engagement – to searching for information on career development, the Division of Academic Support and Student Affairs Staff is here to help."

Additional Tutoring CentersLinks to an external site. Links to an external site.
Math Learning CenterLinks to an external site.;Links to an external site. Links to an external site.Chemistry Learning CenterLinks to an external site.;Links to an external site. Links to an external site.The Writing CenterLinks to an external site.;Links to an external site. Links to an external site.ECE Study GroupsLinks to an external site. Links to an external site.

BookstoreLinks to an external site. Links to an external site.
"Show your New Jersey Institute Of Technology pride all year long with our authentic assortment of New Jersey Institute Of Technology collegiate apparel...Plus, our selection of textbooksLinks to an external site.,Links to an external site. Links to an external site.computersLinks to an external site.,Links to an external site. and suppliesLinks to an external site. Links to an external site.will ensure every New Jersey Institute Of Technology student is prepared for success."

Center for Counseling and Psychological ServicesLinks to an external site. Links to an external site.

“The NJIT Center for Counseling and Psychological Services (C-CAPS) is committed to assisting students in the achievement of their academic goals as well as benefiting from their personal experience on campus. College life can be personally challenging and stressful at times. We believe that the educational process is an important component of the development of the individual as a whole person. Our goal is to optimize the college experience and improve the quality of the lives of our students by promoting their mental health and facilitating students’ personal, academic and professional growth.”

Disability Support ServicesLinks to an external site. Links to an external site.

“The Disability Support Services office works in partnership with administrators, faculty and staff to provide reasonable accommodations and support services for students with disabilities that have provided our office with documentation to receive services.”

The Learning CenterLinks to an external site. Links to an external site.

“Our mission is to assist students both in the classroom and beyond by providing tutorial services, academic coaching, academic and personal enrichment workshops and staff and peer support so students can meet the demands of their coursework and are prepared for life after graduation.”

Robert W. Van Houten LibraryLinks to an external site. Links to an external site.

“The Van Houten Library offers electronic and print resources essential to the mission of New Jersey's science and technology university, including a core collection of academic books, databases, and journals, as well as research and consultation services.”

Student Financial Aid ServicesLinks to an external site. Links to an external site.

“Student Financial Aid Services (SFAS) at NJIT is committed to providing you with every opportunity to obtain funding to support your undergraduate educational costs at NJIT.”