Introduction to Modern Cryptography

CIS 5371 (all sections)
Class Periods: T Period 4 (10:40a-11:30a) / R Periods 4-5 (10:40a-12:35p)
Location: CSE 121
Academic Term: Spring 2023

Instructor:
Tom Shrimpton
teshrim@ufl.edu
+1 352 294 2092
Office Hours: To be determined

NOTE: this is the official, university required syllabus. I will post a extended, supplementary syllabus document on the course Canvas site. Please make sure to read that!

Course Description
[Required, official catalog description**:** Introducing classical and modern cryptography and cryptanalysis, including symmetric and asymmetric (public key) ciphers. It covers cryptographic hash functions, block and stream ciphers, as well as differential and linear cryptanalysis. It reviews BAN logic, applications of cryptography, cryptographic standards and protocols, and analyzes case studies of failed implementations. (3 hours)]

We are going to learn about Modern Cryptography. I expect to lecture on some, or all, of the following topics:

- blockciphers and tweakable blockciphers
- symmetric encryption schemes (e.g., CBC and counter modes-of-operation)
- cryptographic hash functions (e.g., MD5, SHA1, SHA2) • message authentication schemes (e.g., CBC-MAC, HMAC)
- authenticated encryption schemes (e.g,. encrypt-then-MAC, OCB)
- "hard problem" primitives for public-key crypto (e.g., discrete log, RSA)
- public-key encryption schemes (e.g., El Gamal and the KEM-DEM paradigm)
- digital signature schemes (e.g., FDH-RSA)
- zero-knowledge proofs
- multiparty computation (e.g., garbled circuits, oblivious transfer)
- randomness extraction

For each of these bulleted items, I could add "and their associated security notions", but don't for space reasons. (It would also be really repetitive.) Just assume it's there, because security notions are a big part of the course.

Course material is subject to change depending on how fast we go, and on student interests. For additional information, hints for doing well, etc., please see the syllabus made available through the course Canvas site.

Course Pre-Requisites / Co-Requisites
COT 3100 Applications of Discrete Structures or equivalent ; Coreq: COT 5405 Analysis of Algorithms or equivalent. Exceptions by instructor approval.

Course Objectives
My goal is to for you to understand the theoretical foundations of modern, real-world cryptographic primitives and protocols. Your understanding will be measured through homework sets, and a written summary (with, potentially, an associated oral presentation) of a current research publication.

Materials and Supply Fees
N/A

Required Textbooks and Software

Nothing is required. We will loosely follow some online course notes, links to be provided on the course website.

Recommended Materials

- Title: **Introduction to Modern Cryptography**
- Authors: Jonathan Katz and Yehuda Lindell
- Publication date and edition: November 2014, 2nd
- ISBN 9781466570269

Course Schedule (tentative, subject to change)

Week 1: Introduction to the main ideas and goals of modern cryptography; notation; formalizing key-recovery attacks

Week 2: Function families and blockciphers; pseudorandom permutations and functions, and the PRP/PRF security notions; ECB, CTR, CBC modes of encryption and the syntax they suggest for encryption schemes

Week 3: Formalizing IV-based encryption schemes; perfect secrecy/perfect indistinguishability; indistinguishability under a chosen-plaintext attack (IND-CPA) notion for IV-based encryption schemes

Week 4: IND-CPA/IND-CCA notions; security of ECB, CTR modes

Week 5: Security of CBC mode; issues of padding; beginnings of authenticated encryption

Week 6: Notions of ciphertext/plaintext authenticity; formalizing authenticated encryption with associated data (AEAD); AEAD via generic composition; padding-oracle attacks

Week 7: PRFs with variable input lengths (VIL-PRFs); building them from hash functions and fixed-input-length PRFs

Week 8: Hash functions and notions of security (collision resistance, preimage resistance, etc.)

Week 9: Merkle-Damgard constructions, length-extension attacks; NMAC and HMAC constructions

Week 10: Hash functions with parameters, epsilon-almost-universal hash functions, polynomial hashing

Week 11: Blockcipher designs, tweakable blockciphers, ciphers with "strange domains"

Week 12: Basics of key-exchange protocols, simple security notions; Diffie-Hellman key exchange; discrete-log, computational DH, and decisional DH notions; cyclic groups

Week 13: Public-key encryption; El Gamal from DDH assumption, hashed El Gamal from CDH in the random-oracle model; generic 1-to-q query IND-CPA security result; key-encapsulation mechanisms (KEM)

Week 14: The RSA function and associated hardness assumption(s); RSA-KEM; key-transport for key exchange; hybrid (public-key) encryption and KEM-DEM schemes; digital signature schemes

Week 15: RSA signatures (PKCS#1, full-domain hash, PSS); Schorr signatures and the Fiat-Shamir heuristic; basics of interactive proofs and zero-knowledge proofs

Attendance Policy, Class Expectations, and Make-Up Policy

Attendance is not mandatory, but is *strongly* recommended. If you miss multiple classes, it will (almost certainly) make it more difficult for you to fully comprehend the material. The following statement is required: Excused absences must be in compliance with university policies in the Graduate Catalog (http://gradcatalog.ufl.edu/content.php?catoid=10&navoid=2020#attendance) and require appropriate documentation.

[This statement is required:
Excused absences must be consistent with university policies in the Graduate Catalog (https://catalog.ufl.edu/graduate/regulations) and require appropriate documentation. Additional information can be found here: https://catalog.ufl.edu/UGRD/academic-regulations/attendance-policies/]

Evaluation of Grades

Assignment	Total Points	Percentage of Final Grade
Homework Sets (~6)	variable	85%
Paper review	100	15%
		100%

When computing the overall contribution of homework to your final grade, I will throw out the lowest (percentage-wise) of your scores. You may work in groups of up to three people on homework assignments. Note: Please see the extended syllabus on the course Canvas site for additional discussion and guidance on how to best complete homework assignments.

Grading Policy

See the extended syllabus on the course Canvas site for more details. At the end of the term, letter grades will be assigned according to the following scale.

Percent	Grade	Grade Points
93- 100	A	4.00
90.0 - 93	A-	3.67
87 - 89	B+	3.33
83 - 86	B	3.00
80.0 - 83	B-	2.67
77 - 79	C+	2.33
73 - 76	C	2.00
70 - 73	C-	1.67
67 - 69	D+	1.33
63 – 66	D	1.00
60 - 62	D-	0.67
0 - 59	E	0.00

More information on UF grading policy may be found at:
http://gradcatalog.ufl.edu/content.php?catoid=10&navoid=2020#grades

Students Requiring Accommodations

(Required statement) Students with disabilities who experience learning barriers and would like to request academic accommodations should connect with the disability Resource Center by visiting https://disability.ufl.edu/students/get-started/. It is important for students to share their accommodation letter with their instructor and discuss their access needs, as early as possible in the semester.

Course Evaluation

(Required statement) Students are expected to provide professional and respectful feedback on the quality of instruction in this course by completing course evaluations online via GatorEvals. Guidance on how to give feedback in a professional and respectful manner is available at https://gatorevals.aa.ufl.edu/students/. Students will be notified when the evaluation period opens, and can complete evaluations through the email they receive from GatorEvals, in their Canvas course menu under GatorEvals, or via https://ufl.bluera.com/ufl/. Summaries of course evaluation results are available to students at https://gatorevals.aa.ufl.edu/public-results/.

In-Class Recording

(Required statement) Students are allowed to record video or audio of class lectures. However, the purposes for which these recordings may be used are strictly controlled. The only allowable purposes are (1) for personal educational use, (2) in connection with a complaint to the university, or (3) as evidence in, or in preparation for, a

criminal or civil proceeding. All other purposes are prohibited. Specifically, students may not publish recorded lectures without the written consent of the instructor.

A "class lecture" is an educational presentation intended to inform or teach enrolled students about a particular subject, including any instructor-led discussions that form part of the presentation, and delivered by any instructor hired or appointed by the University, or by a guest instructor, as part of a University of Florida course. A class lecture does not include lab sessions, student presentations, clinical presentations such as patient history, academic exercises involving solely student participation, assessments (quizzes, tests, exams), field trips, private conversations between students in the class or between a student and the faculty or lecturer during a class session.

Publication without permission of the instructor is prohibited. To "publish" means to share, transmit, circulate, distribute, or provide access to a recording, regardless of format or medium, to another person (or persons), including but not limited to another student within the same class section. Additionally, a recording, or transcript of a recording, is considered published if it is posted on or uploaded to, in whole or in part, any media platform, including but not limited to social media, book, magazine, newspaper, leaflet, or third party note/tutoring services. A student who publishes a recording without written consent may be subject to a civil cause of action instituted by a person injured by the publication and/or discipline under UF Regulation 4.040 Student Honor Code and Student Conduct Code.

University Honesty Policy

(Required statement) UF students are bound by The Honor Pledge which states, "We, the members of the University of Florida community, pledge to hold ourselves and our peers to the highest standards of honor and integrity by abiding by the Honor Code. On all work submitted for credit by students at the University of Florida, the following pledge is either required or implied: "On my honor, I have neither given nor received unauthorized aid in doing this assignment." The Conduct Code (https://sccr.dso.ufl.edu/process/student-conduct-code/) specifies a number of behaviors that are in violation of this code and the possible sanctions. If you have any questions or concerns, please consult with the instructor or TAs in this class.

Commitment to a Safe and Inclusive Learning Environment

(Required statement) The Herbert Wertheim College of Engineering values broad diversity within our community and is committed to individual and group empowerment, inclusion, and the elimination of discrimination. It is expected that every person in this class will treat one another with dignity and respect regardless of gender, sexuality, disability, age, socioeconomic status, ethnicity, race, and culture.

If you feel like your performance in class is being impacted by discrimination or harassment of any kind, please contact your instructor or any of the following:

- Your academic advisor or Graduate Program Coordinator
- Jennifer Nappo, Director of Human Resources, 352-392-0904, jpennacc@ufl.edu
- Curtis Taylor, Associate Dean of Student Affairs, 352-392-2177, taylor@eng.ufl.edu
- Toshikazu Nishida, Associate Dean of Academic Affairs, 352-392-0943, nishida@eng.ufl.edu

Software Use

(Required statement) All faculty, staff, and students of the University are required and expected to obey the laws and legal agreements governing software use. Failure to do so can lead to monetary damages and/or criminal penalties for the individual violator. Because such violations are also against University policies and rules, disciplinary action will be taken as appropriate. We, the members of the University of Florida community, pledge to uphold ourselves and our peers to the highest standards of honesty and integrity.

Student Privacy

(Required statement) There are federal laws protecting your privacy with regards to grades earned in courses and on individual assignments. For more information, please see: https://registrar.ufl.edu/ferpa.html

Campus Resources:

Health and Wellness

U Matter, We Care:
Your well-being is important to the University of Florida. The U Matter, We Care initiative is committed to creating a culture of care on our campus by encouraging members of our community to look out for one another and to reach out for help if a member of our community is in need. If you or a friend is in distress, please contact umatter@ufl.edu so that the U Matter, We Care Team can reach out to the student in distress. A nighttime and weekend crisis counselor is available by phone at 352-392-1575. The U Matter, We Care Team can help connect students to the many other helping resources available including, but not limited to, Victim Advocates, Housing staff, and the Counseling and Wellness Center. Please remember that asking for help is a sign of strength. In case of emergency, call 9-1-1.

Counseling and Wellness Center: https://counseling.ufl.edu, and 392-1575; and the University Police Department: 392-1111 or 9-1-1 for emergencies.

Sexual Discrimination, Harassment, Assault, or Violence
If you or a friend has been subjected to sexual discrimination, sexual harassment, sexual assault, or violence contact the **Office of Title IX Compliance**, located at Yon Hall Room 427, 1908 Stadium Road, (352) 273-1094, title-ix@ufl.edu

Sexual Assault Recovery Services (SARS)
Student Health Care Center, 392-1161.

University Police Department at 392-1111 (or 9-1-1 for emergencies), or http://www.police.ufl.edu/.

COVID-19

- You are expected to wear approved face coverings at all times during class and within buildings even if you are vaccinated.
- If you are sick, stay home and self-quarantine. Please visit the UF Health Screen, Test & Protect website about next steps, retake the questionnaire and schedule your test for no sooner than 24 hours after your symptoms began. Please call your primary care provider if you are ill and need immediate care or the UF Student Health Care Center at 352-392-1161 (or email covid@shcc.ufl.edu) to be evaluated for testing and to receive further instructions about returning to campus.
- If you are withheld from campus by the Department of Health through Screen, Test & Protect, you are not permitted to use any on campus facilities. Students attempting to attend campus activities when withheld from campus will be referred to the Dean of Students Office.
- UF Health Screen, Test & Protect offers guidance when you are sick, have been exposed to someone who has tested positive or have tested positive yourself. Visit the UF Health Screen, Test & Protect website for more information.
- Please continue to follow healthy habits, including best practices like frequent hand washing. Following these practices is our responsibility as Gators.

Academic Resources

E-learning technical suppor*t*, 352-392-4357 (select option 2) or e-mail to Learning-support@ufl.edu. https://lss.at.ufl.edu/help.shtml.

Career Resource Center, Reitz Union, 392-1601. Career assistance and counseling; https://career.ufl.edu.

Library Support, http://cms.uflib.ufl.edu/ask. Various ways to receive assistance with respect to using the libraries or finding resources.

Teaching Center, Broward Hall, 392-2010 or 392-6420. General study skills and tutoring. https://teachingcenter.ufl.edu/.

Writing Studio, 302 Tigert Hall*,* 846-1138. Help brainstorming, formatting, and writing papers. https://writing.ufl.edu/writing-studio/.

Student Complaints Campus*:* https://sccr.dso.ufl.edu/policies/student-honor-code-student-conduct-code/;https://care.dso.ufl.edu.

On-Line Students Complaints*:* http://www.distance.ufl.edu/student-complaint-process.