Intro to Cryptology

CIS 5371 Section 11413
Class Periods: T/R, 2-3/3, 8:30a-10:25a/9:35a-10:25a
Location: CSE E222
Academic Term: Fall 2019

Instructor:
Tom Shrimpton
teshrim@ufl.edu
352-294-2092
Office Hours: W, 10:30-11:30 or by appointment, MSE 207

Teaching Assistant/Peer Mentor/Supervised Teaching Student:
None

Course 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)

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
We are going to learn about Modern Cryptography. **The main objective is to for you to understand the theoretical foundations of modern, real-world cryptosystems.**

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. RSA)
- public-key encryption schemes (e.g. El Gamal and the KEM-DEM paradigm)
- digital signature schemes (e.g. FDH-RSA)
- zero-knowledge proofs
- multiparth 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 depending on student interests.

Your understanding of the course material will be tested (and extended!) via a sequence of challenging homework assignments. At the end of the course, you will be required to read and provide an executive summary for a current crypto research paper.

Materials and Supply Fees
None

Required Textbooks and Software
None

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

Course Schedule (example, subject to modifications based on student comprehension and interests)

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.

Evaluation of Grades

Assignment	Total Points	Percentage of Final Grade
Homework Sets (5-6)	100 each	85%
Final Exam/Project	100	15%

Your score for each homework assignment will be determined by the correctness of your solutions, and by the clarity of your presentation. Let me stress this point: if your solution is correct, but your presentation is sloppy, you will not receive full credit. Learning to communicate with logical, well organized, and concise prose and mathematics is an important part of academic maturity; these are skills that good scientists continue to hone throughout their careers. So, please, put serious effort into your solution write-ups.

You may work in groups of up to *three* people on homework assignments. If you work with one or more person then you should turn in a single writeup. I urge you to understand everything that you turn in. If you let group-mates carry you on homework assignments, it *will* be obvious and I will take a negative view on this when grading.

Late homeworks will be accepted only under extreme circumstances, e.g. death in the family, incapacitating personal illness, emergency involving your children, attending a conference. Please talk to me as soon as possible if you think you will need to be late turning in an assignment.

Fully acknowledge the source of any outside ideas, whether it be a book, paper, website, or colleague. It's the right thing to do, and it's necessary for writing good research papers. You may share ideas with someone else as long as you acknowledge them. **All forms of academic dishonesty, cheating, and fraud will be treated in accordance with UF policy**. If you are not clear as to what constitutes academic dishonesty in this course, please come and talk to me. Better safe than sorry!

Grading Policy

When computing the overall contribution of homework to your final grade, I will throw out the lowest of your scores. This is an elective course, so I expect that you are in the class because you are interested in the material and are prepared to put in serious effort. I reserve the right to adjust your final course grade up or down by as much as 5%, depending on the trend of your homework scores, your participation in class, etc. (I've never actually downgraded anyone, as people I might be tempted to downgrade usually weed themselves out. But I still reserve the right to do so.) After all adjustments are made, the letter grade will be assigned as follows.

Percent	Grade	Grade Points
90.0 - 100.0	A	4.00
87.0 - 89.9	A-	3.67
84.0 - 86.9	B+	3.33
81.0 – 83.9	B	3.00
78.0 - 80.9	B-	2.67
75.0 - 79.9	C+	2.33
72.0 – 74.9	C	2.00
69.0 - 71.9	C-	1.67
66.0 - 68.9	D+	1.33
63.0 - 65.9	D	1.00
60.0 - 62.9	D-	0.67
0 - 59.9	F	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
Students with disabilities requesting accommodations should first register with the Disability Resource Center (352-392-8565, https://www.dso.ufl.edu/drc) by providing appropriate documentation. Once registered, students will receive an accommodation letter which must be presented to the instructor when requesting accommodation. Students with disabilities should follow this procedure as early as possible in the semester.

Course Evaluation
Students are expected to provide feedback on the quality of instruction in this course by completing online evaluations at https://evaluations.ufl.edu/evals. Evaluations are typically open during the last two or three weeks of the semester, but students will be given specific times when they are open. Summary results of these assessments are available to students at https://evaluations.ufl.edu/results/.

University Honesty Policy
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 Honor Code (https://sccr.dso.ufl.edu/policies/student-honor-code-student-conduct-code/) specifies a number of behaviors that are in violation of this code and the possible sanctions. Furthermore, you are obligated to report any condition that facilitates academic misconduct to appropriate personnel. 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
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
- Robin Bielling, Director of Human Resources, 352-392-0903, rbielling@eng.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
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
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: http://www.counseling.ufl.edu/cwc, 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/.

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://www.crc.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://www.dso.ufl.edu/documents/UF_Complaints_policy.pdf.

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