Introduction to Cryptology

CIS 4362 Class Number: 11334 Section: 2F66

Class Periods: MWF Period 4 (10:40 AM - 11:30 AM)
Location: online
Academic Term: Fall 2020

Nota bene: to complete email addresses append @ufl.edu
Instructor:
Richard Newman
email: nemo – use CIS4362 in subject line
Phone Number: 352-283-1083 (text OK – include your name and CIS4362)
Office Hours: MWF 11:30-12:30 online

Teaching Assistants: N/A

Course Description
Credits: 3; Introduces classical and modern cryptography and cryptanalysis, including symmetric and asymmetric (public key) ciphers. Covers cryptographic hash functions, block and stream ciphers, as well as differential and linear cryptanalysis. Reviews applications of cryptography, cryptographic standards and protocols, and analyzes case studies of failed implementations.

Course Pre-Requisites: *COT 3100 or the equivalent; knowledge of C, C++, or Java*

Course Objectives

Students will study the design and implementation of cryptographic primitives, cryptographic systems, and cryptographic protocols. The successful student will be able to analyze the design and implementation of these systems, explain cryptographic primitives, and apply modern proof techniques to cryptographic designs.

Materials and Supply Fees: N/A

Professional Component (ABET):

Engineering science is addressed in the theoretical aspects of performance analysis and the mathematical proof systems used. Engineering design is addressed in cryptographic protocols and standards.

Relation to Program Outcomes (ABET):

Outcome	Coverage*
a. Apply knowledge	High
b1. Conduct experiments	Low
b2. Statistical design of experiments	Medium
c. Design	High
d. Function on teams	
e. Solve problems	Medium
f. Professional and ethical responsibility	Medium
g. Communicate	Low
h1. Economic impact	Low
h2. Global, societal, and environmental impact	Low

i. Lifelong learning	
j. Contemporary issues	Low
k. Techniques, skills, and tools for degree program	Medium

*Coverage is given as high, medium, or low. An empty box indicates that this outcome is not part of the course.

Required Textbooks and Software

- Title: INTRODUCTION TO MODERN CRYPTOGRAPHY
- Author: KATZ & LINDELL
- Publication date and edition: 2015, 2/e
- ISBN: 9781466570269
- Virtual Box 5.0.16 (suggested) or VMware
- Minix 3.2.1 (required)

Recommended Materials

- Title: CRYPTOGRAPHY: THEORY AND PRACTICE
- Author: STINSON & PATERSON
- Publication date and edition: 2018, 4/e
- ISBN: 9781138197015

- Title: THE C PROGRAMMING LANGUAGE
- Author: KERNIGHAN & RITCHIE
- Publication date and edition: 1988, 2/e
- ISBN: 0131103628

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.

Course Schedule (may be tweaked)

Week 1: Introduction / Substitutions, cryptanalysis
Week 2: Transpositions, Polygraphics, Multiliterals
Week 3: Rotor Machines, cryptanalysis
Week 4: Modern Block Ciphers, cryptanalysis
Week 5: Block Cipher Modes
Week 6: Theoretical Basis for Cryptography
Week 7: MACs, Authenticated Encryption
Week 8: Cryptographic Hash Functions
Week 9: PKCS, Cyclic Groups
Week 10: PKCS, Cyclic Groups
Week 11: DH, RSA,
Week 12: Digital Signatures
Week 13: Digital Signatures
Week 14: Key Distribution
Week 15: Key Distribution

Week 16: PKI
Detailed assignments are posted on Canvas.

Attendance Policy, Class Expectations, and Make-Up Policy

Attendance is highly encouraged. Most weeks there will be an on-line quiz. There are no makeups for missed quizzes, but the lowest quiz will be dropped. Three to four homework assignments will be done individually.

Questions are encouraged – please post in the chat window. Try to formulate the question before asking it, and wait to see if it is answered in a few minutes so we can maintain flow. Lengthy discussions will be deferred to office hours.

Projects and exercises are all to be done on an individual basis, but you are encouraged to discuss both textbook material and projects with others in the class. However, you may NOT share code.

Excused absences are consistent with university policies in the undergraduate catalog (https://catalog.ufl.edu/ugrad/current/regulations/info/attendance.aspx) and require appropriate documentation.

Late submissions: Late submissions will have one point deducted for day (rounded up for partial days) after the due date until the assignment closes. After closing, no work will be accepted. Quizzes will be closed shortly after their due date and time – there will be no makeups but the lowest quiz score will be dropped. Projects and exercises will have one-point penalty per day or partial day late until they close (usually a week after the due date).

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://www.dso.ufl.edu/sccr/process/student-conduct-honor-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.

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/.

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:
http://registrar.ufl.edu/catalog0910/policies/regulationferpa.html

Evaluation of Grades

Assignment	Total Points	Percentage of Final Grade
Homework Sets	variable	20%
Quizzes	10 pts each	20%
Exercises & Challenges	5-10 pts each	20%
Project	50 pts	40%
		100%

Grading Policy

Percent	Grade	Grade Points
88 - 100	A	4.00
84-88	A-	3.67
80-84	B+	3.33
76-80	B	3.00
72-76	B-	2.67
68-72	C+	2.33
64-68	C	2.00
60-64	C-	1.67
56-60	D+	1.33
52-56	D	1.00
48-52	D-	0.67
0 - 48	E	0.00

More information on UF grading policy may be found at:
https://catalog.ufl.edu/ugrad/current/regulations/info/grades.aspx

Campus Resources:

Health and Wellness

U Matter, We Care:
If you or a friend is in distress, please contact umatter@ufl.edu or 352 392-1575 so that a team member can reach out to the student.

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 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.