CIS 3362: Cryptography and Information Security - Fall 2022

Instructor: Arup Guha
Email: dmarino@ucf.edu
Office Hours: **http://www.cs.ucf.edu/~dmarino/ucf/OH.html**
Course Web Page: **http://www.cs.ucf.edu/courses/cis3362/fall2022** (Note: TA information and office hours will be on the course web page.)

Note: I do NOT check my WebCourses email. Please email me at dmarino@ucf.edu to contact me.

Course Description: This course provides an introduction to cryptography and primarily focuses on the algorithms that are used in classical and modern cryptosystems, as well as the mathematics necessary to understand the underpinnings of those algorithms. Security issues outside of the mathematics of the cryptosystems is not emphasized.

Class Days and Times: MWF 12:30 am – 1:20 pm
Classroom: HEC-125

Supplemental Books Used for Lectures:

Cryptography and Network Security by William Stallings (ISBN-13: 978-0-13-609704-4)
Cryptography Theory and Practice by Douglas R. Stinson (ISBN: 0-8493-8521-0)
The Code Book by Simon Singh (ISBN: 0-385-49532-3)
Classical and Contemporary Cryptology by Richard J. Spillman (ISBN: 0-13-1828312)
Applied Cryptography by Bruce Schneier (ISBN: 0-471-11709-9)
Cryptanalysis by Helen Fouche Gaines(ISBN: 0-486-20097-3)

Course Prerequisite: COP 3223

Outline of material covered:

1. Introduction to Cryptography
2. Mathematics Background for Classical Schemes
3. Classical Cryptosystems
4. Cryptanalysis of Classical Schemes
5. Cryptography related to World War II
6. DES
7. AES, Cipher Modes
8. Number Theory, Primality Testing
9. Public Key Cryptosystems
10. Brief summary of Hash Functions, Message Authentication Codes and Digital Signatures

Tentative Assignments and Grading Breakdown:

	worth(% of grade)
7 Homework Assignments (1%, 4%, 4%, 4%, 4%, 4%, 6%)	27%
Quizzes 1 - 4 (12% each)	48%
Final Exam	25%

Note: +/- grades may be given in this course if deemed appropriate.

Note About Financial Aid: A UCF policy involves looking at "course activity" via WebCourses to decide whether or not to disburse financial aid. To this end, I have created a relatively easy week one assignment to be submitted over WebCourses. Please, please, please, just turn *something* in for this.

Note: Some items on this syllabus may change based on how the class is going. These changes will only be announced in class, thus it's imperative to go to class, or speak to a friend who has attended class to get any announcements you may have missed.

Homework

All homework assignments will be done individually. Depending on the homework assignment, various aids will be allowed. These will be announced in class. Using resources beyond the allowed aids will be considered academic misconduct. The academic misconduct policy is shown below. **All homework will be due over WebCourses and no late homework will be accepted. Due dates and times will ONLY be posted in WebCourses.** In particular, when breaking codes, you can NOT use arbitrary websites. Furthermore, to get full credit, you **must explain your process, step by step**. Namely, a majority of your grade is NOT for the answer, but the **communication** of the process you used. Thus, to earn a good grade, you must use a process which I approve of **AND** appropriately communicate that process.

Community Service Opportunity

If you would like to earn an automatic 100% for the last homework assignment (worth 6% of the course grade), you can perform 5 hours of community service in between August 22nd and November 17th, 2022. The community service you complete must not be for another course or program here at UCF. (Thus, Honors students can't use their symposium-related service, which is required of them for Honors.) In order to get this credit, you must complete the community service **and turn in the requisite form and essay signed** by the **November 18th, 2022, in class.** ***Note: Your community service MUST BE with a registered 501(c)(3) organization to count for this assignment. Also note that the service must be completed one or more days before the form is due.***

Quizzes/Exams

You will be allowed to use some aids on each of the quizzes and final exam. The specific aids allowed will be described in class only during each of the corresponding exam reviews.

Academic Misconduct Policy

Only designated aids will be allowed for exams and homework assignments. Failure to adhere to these policies may result in a 'Z' designation and in the lowering of the final class grade by a whole letter grade, on the first offense. **If there is any question about what constitutes academic dishonesty, please ask me before you use a particular resource! (Note: For example, websites that automatically crack substitution ciphers are not an allowed resource.)**

Getting Help During the Course

There are four TAs who will hold office hours in addition to my office hours. Office Hours will be held in the mode which is preferable to each TA. The course instructor will have both online office hours and in person office hours.

Make Up Work Policy

If a student has a good reason to require a make-up exam or quiz, the student MUST make the request **before** the exam or quiz with documentation for the reason. Reasons that will be accepted include: military service, illness, family issues, UCF club activities, religious exemptions, and work. For things like work and UCF club activities, it is expected that students show they've made an effort to rearrange their schedule with their boss/supervisor, if that is a reasonable thing to do for the situation. Requests need to be made via email to dmarino@ucf.edu. Typically, make ups will NOT be granted for homework unless a student is incapacitated for 70% or more of the time period the homework was posted. (Namely, students are expected to plan their homework and can't get extensions if they didn't start on their homework and get sick 3 days before it is due, for example. Note: this is the most common reason I get the request for which I deny the request.)

Tentative Course Schedule

Week	Monday	Wednesday	Friday
Aug 22-26	Syllabus	Affine	Euclid's Alg ***HW #1 due***
Aug 29 - Sept 2	Substitution	Vigenere	IC+MIC
Sept 6-9	**Labor Day**	**Quiz #1**	Playfair ***HW #2 due***
Sept 12-16	ADFGVX	Hill Cipher	Enigma
Sept 19-23	Navajo Code	Transposition ***HW #3 due***	**Quiz #2**
Sept 26-30	Coding Bitwise Operators	DES	DES
Oct 3-7	AES	AES	AES ***HW #4 due***
Oct 10-14	**Quiz #3**	Euler Thm	Disc Log
Oct 17-21	Miller Rabin	Factoring	Fast Mod Expo
Oct 24-28	Diffie-Hellman ***HW #5 due***	RSA	El Gamal **WD Deadline**
Oct 31 – Nov 4	ECC	ECC	Quiz 4 Review
Nov 7-11	Guest Lecture ***HW #6 due***	**Quiz #4**	**Veteran's Day**
Nov 14-19	Quantum Crypto	Group DH	Hash Functions
Nov 21-23	Birthday Attack	**Thanksgiving**	**Thanksgiving**
Nov 28-Dec 2	El Gamal Dig Sig ***HW #7 due***	FE Review	FE Review
Dec 5-9	No Class		**Final Exam, Dec 9 (10am – 1pm)**

Note: Assignments will be given in class and will be due over WebCourses. Tentative dates are given above for the assignments but consult WebCourses for the final due dates and times. Also, this schedule may change based on the pace of lectures, so please watch the class videos within 24 hours of when they are given live to have a completely accurate gauge of what is being covered on which day.

Also, I have built in three review days for Quiz 4 and the Final Exam. If I find a new topic that I feel confident enough in teaching that I think may be valuable, then I'll remove one or more of those review days.