CIS 3362: Cryptography and Information Security - Fall 2020

Arup Guha
dmarino@cs.ucf.edu, (321) 663-7749
Office Hours: **http://www.cs.ucf.edu/~dmarino/ucf/OH.html**
Course Web Page: **http://www.cs.ucf.edu/courses/cis3362/fall2020**

Note: I do NOT check my WebCourses email. Please email me at dmarino@cs.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 11:30 am – 12:20 pm
Classroom: Your House or Wherever, Really
Recommended Textbook: Cryptography and Network Security by William Stallings (ISBN-13: 978-0-13-609704-4)
Supplemental Books Used for Lectures:

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:

	Resource
1. Introduction to Cryptography	Cht. 1
2. Mathematics Background for Classical Schemes	Notes
3. Classical Cryptosystems	Cht. 3 + Notes
4. Cryptanalysis of Classical Schemes	Notes
5. Cryptography related to World War II	Notes
5. DES	4
6. AES, Cipher Modes	5, 6, 7
8. Number Theory, Primality Testing	Cht 2 + Notes
9. Public Key Cryptosystems	9, 10
10. Brief summary of Hash Functions, Message Authentication Codes and Digital Signatures	11, 12, 13

Tentative Assignments and Grading Breakdown:

	worth(% of grade)
7 Homework Assignments (1%, 4%, 4%, 4%, 4%, 4% 4%)	25%
Quizzes 1 - 5 (10% each)	50%
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 listen to class lectures within 24 hours of when they are given live.

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.**

Exams

You will be allowed to use some aids on each of the exams. 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 via Zoom and the links will be provided in Webcourses only.

COVID-19 Statement

Please read UCF's required statement about COVID-19 applicable to all syllabi this semester:

https://fctl.ucf.edu/teaching-resources/course-design/syllabus-statements/

My intention is for this course to be fully online unless the university informs me otherwise. To that end, I will record live lectures during each of the regularly scheduled class times. It is suggested that students watch the lectures when I give them, but not required. Students are required to watch the lectures within 24 hours of when they are given, to make sure they don't fall behind. If you view lectures in a location that has people outside of your "pod" who are potentially near you (less than 10 feet), please do wear a face mask while viewing.

All quizzes and exams will be given in real time (during scheduled class times) as short timed assignments via Webcourses. These dates and times are posted on the syllabus and it is expected for students to take these quizzes and exams at the dates and times stated. These times are **NOT flexible**, like the lecture viewing times.

If you become ill during the semester and are unable to continue doing work in the class, please email me and we can decide together what the most appropriate action would be (make up assignments during the semester, regular withdrawal, medical withdrawal or incomplete). If you are ill but can still work from home, there is no need to let me know, unless you believe you need some special accommodation.

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@cs.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 24-28	Syllabus	Affine	Euclid's Alg ***HW #1 due***
Aug 31 - Sept 4	Substitution	Vigenere	IC+MIC
Sept 8-11	**Labor Day**	**Quiz #1**	Playfair ***HW #2 due***
Sept 14-18	ADFGVX	Hill Cipher	Enigma
Sept 21-25	Navajo Code	Transposition ***HW #3 due***	**Quiz #2**
Sept 28-Oct 2	Coding Bitwise Operators	DES	DES
Oct 5-9	AES	AES	AES ***HW #4 due***
Oct 12-16	**Quiz #3**	Euler Thm	Disc Log
Oct 19-23	Miller Rabin	Factoring	Fast Mod Expo ***HW #5 due***
Oct 26-30	**Quiz #4**	Diffie-Hellman	RSA **WD Deadline**
Nov 2-6	El Gamal	ECC	ECC
Nov 9-13	ECC ***HW #6 due***	**Veteran's Day**	**Quiz #5**
Nov 16-20	Quantum Crypto	Hash Functions	MACs
Nov 23-25	Digital Signatures	DSA	**Thanksgiving**
Nov 30-Dec 4	TBA ***HW #6 due***	FE Review	FE Review
Dec 7-11	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.