CIS 3362: Cryptography and Information Security - Fall 2019

Arup Guha
dmarino@cs.ucf.edu, (407) 823- 1062
Office Hours: **http://www.cs.ucf.edu/~dmarino/ucf/OH.html**
Course Web Page: **http://www.cs.ucf.edu/courses/cis3362/fall2019**

Class Days and Times: MWF 12:30 pm – 1:20 pm
Classroom: MSB-359
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)
6 Homework Assignments (2%, 5%, 5%, 6%, 6%, 6%)	30
Exam #1	15
Exam #2	15
Exam #3	15
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 come to class.

Homework

All homework assignments will be done in pairs, ***except the first one, which will be done individually.*** Students may only confer with their partner assignments 2 - 6. Students may change partners for each assignment. ***If a student does not find a partner to work with for an assignment, they will be expected to do the assignment on their own.*** Please try to come see me if you are having difficulty on assignments instead of students in a separate group. **All homework will be due over WebCourses and no late homework will be accepted. Due dates and times will ONLY be posted in WebCourses.**

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 26th and October 31st, 2019. 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 1st, 2019, 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.***

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 Dishonesty 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.)**

Tentative Course Schedule

Week	**Monday**	**Wednesday**	**Friday**
Aug 26-31	Syllabus	Affine	Euclid's Alg ***HW #1 due***
Sept 3-6	**Labor Day**	**Dorian Day**	Substitution
Sept 9-13	Vigenere IC+MIC	Playfair	ADFGVX
Sept 16-20	Hill ***HW #2 due***	E1 Review	**Exam #1**
Sept 23-27	Enigma	Navajo Code ***HW #3 due***	Transposition
Sept 30-Oct 4	Coding Bitwise Operators	DES	DES
Oct 7-11	AES	AES	Cipher Modes ***HW #4 due***
Oct 14-18	E2 Review	**Exam #2**	Euler Thm
Oct 21-25	Disc Log	Miller Rabin	Factoring
Oct 28-Nov 1	Fast Mod Expo	Diffie-Hellman ***HW #5 due***	RSA ***Com Serv Due*** **WD Deadline**
Nov 4-8	El Gamal	E3 Review ***HW #6 due***	**Exam #3**
Nov 12-15	**Veteran's Day**	ECC	ECC
Nov 18-22	Quantum Crypto	Hash Functions	MACs
Nov 25-26	Digital Signatures	**Thanksgiving**	**Thanksgiving**
Dec 2-6	FE Review	**No Class**	**Final Exam, Dec 6 (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 attend class to have a completely accurate gauge of what is being covered on which day.