CIS 3362: Cryptography and Information Security - Fall 2018

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/fall2018**

Class Days and Times: MWF 11:30 am – 12:20 pm
Classroom: HEC-103
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)

Elementary Cryptanalysis by Abraham Sinkov (ISBN: 0-883-85622-0)

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. 2 + Notes
4. Cryptanalysis of Classical Schemes	Cht. 2 + Notes
5. DES	3
6. AES, Cipher Modes	4, 5, 6
7. Random Number Generation	Notes
8. Number Theory, Primality Testing	8
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
Final Project	15
Final Exam	25

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

Note About Financial Aid: A second year 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 20th and October 25th, 2018. 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 **October 26th, 2018, 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.

Final Project

All students will have to complete a final project in groups of size 4 or 5 on a topic of their choice, related to computer security. All project topics must be personally approved by me. The goal of the project will be to explore a specific security topic in detail, give a polished presentation to the class about it and turn in a paper summarizing the findings.

Groups will be chosen during the fourth or fifth week of class based on what topics students are interested in pursuing. You **must** attend class to be part of a group. (I only approve groups where all members are in class physically on the days that we select groups.) If you are not in a group, you will earn a 0 for this rather large portion of the course grade. Thus, it's ***imperative*** you come to class on at least one of the days that I allow you to choose final project groups. (I will state these days in class sometime during week three.)

Three years ago there was a very embarrassing situation where two students were assigned to a group but never came to class and never checked Webcourses to see who was in their group. When I collected a project update from each group, both students submitted to me updates on separate projects, at which point I informed them that they were in a group together. While this situation was hilarious, I don't want it to ever happen again. Moral of the story: ***Show up to class. Pay attention when I assign you to a group. Communicate frequently with all of your group members.***

Academic Dishonesty Policy

Only designated aids will be allowed for exams and homework assignments. The final project must represent only the work of the group members and sources for all information and data quoted in the presentation and failure must be properly cited. 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 20-24	Syllabus	Affine	Euclid's Alg ***HW #1 due***
Aug 27-31	Substitution	Vigenere	IC+MIC
Sept 4-7	**Labor Day**	Playfair	ADFGVX ***HW #2 due***
Sept 10-14	Hill	Transposition	Transposition
Sept 17-21	Enigma ***HW #3 due***	E1 Review	**Exam #1**
Sept 24-28	Coding Bitwise Operators	DES	DES
Oct 1-5	AES	AES	Cipher Modes ***HW #4 due***
Oct 8-12	Random Nums	Euler Thm	Disc Log
Oct 15-19	Miller Rabin	Factoring	Fast Mod Expo ***HW #5 due***
Oct 22-26	Diffie-Hellman RSA	El Gamal	ECC ***Com Serv Due*** **Withdrawal Deadline**
Oct 29-Nov 2	ECC ***HW #6 due***	E2 Review	**Exam #2**
Nov 5-9	Tree-based Group Diffie-Hellman	Hash Functions	Final Proj Day
Nov 13-16	**Veteran's Day**	Digital Signatures	FE Review
Nov 20-22	Presentations	Presentations	**Thanksgiving**
Nov 26-30	Presentations	Presentations	Presentations
Dec 3-7		**Final Exam, Dec 5 (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.