CIS 3362: Cryptography and Information Security - Fall 2015

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/fall2015**

Class Days and Times: MWF 11:30 am – 12:20 pm
Classroom: HEC-117
Recommended Textbook: Cryptography and Network Security by William Stallings (ISBN-13: 978-0-13-609704-4)
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	4, 5
7. Public Key Cryptosystems	8, 9, 10
10. Hash Functions	11
11. Message Authentication Codes	12
12. Digital Signatures	13

Tentative Assignments and Grading Breakdown:

	worth(% of grade)
Week One Assignment	1
5 Homework Assignments (4%, 5%, 5%, 5%, 5%)	24
Exam #1	15
Exam #2	20
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

Homework assignments will be done individually, which is different than past years for this course. However, I will experiment with a new modality of homework this year. During the first week of class, students may choose to be in one of the two following groups:

(1) Coding intensive group

(2) Coding light group

Those in the first group will create software that is useful in solving typical homework questions I ask in the course. Those in second group must choose one of the programs written by the students in the first group in helping them complete their homework assignments. Thus, the coding intensive group will complete their assignments earlier (about 2-3 weeks earlier on average) than the coding light group.

I expect those who are confident in coding and who enjoy coding to join the first group. I expect those who aren't confident in their coding skills to join the second group. Grades for students in the first group will be based upon the correctness of their programs ***as well as*** how many students in the second group choose to use their software. The grades of the students in the second group will be based upon how well they answer the questions posed on their assignments and how well they make use of the software tools they were given.

I reserve the right to give the same homework to both groups, if coding isn't a large part of that assignment to begin with. In this case, the homework would be due at the same time for both groups.

Details about due dates will be posted on WebCourses later during the semester, thus it's very important to check WebCourses ***in between each class meeting.***

Please try to come see me if you are having difficulty on assignments. **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 5% of your course grade (coming from the final exam grade), simply complete 5 (or more) hours of community service in between August 24th and November 29th, 2015. 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 30th, 2015, 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 3 or 4 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.)

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, but the programs that students in the class write are allowed.)**

Tentative Course Schedule

Week	**Monday**	**Wednesday**	**Friday**
Aug 24	Syllabus	Affine	Euclid's Alg
Aug 31	Substitution	Vigenere	IC+MIC
Sept 8	**Labor Day**	Playfair	ADFGVX
Sept 14	Hill	Transposition	Transposition
Sept 21	Enigma	Rev E1	**Exam #1**
Sept 28	DES	DES	AES
Oct 5	AES	AES	Cipher Modes
Oct 12	Random Nums	Euler Thm	Disc Log
Oct 19	Prime Test	Factoring	RSA
Oct 26	Rev E2	**Exam #2**	Knapsack
Nov 2	ECC **Withdrawal Deadline**	ECC	ECC
Nov 9	Hash Functions	**Veteran's Day**	Hash Functions
Nov 16	MACs	MACs	Dig Sigs
Nov 23	Dig Sigs	Dig Sigs	**Thanksgiving**
Nov 30	Presentations	Presentations	Presentations
Dec 7	FE Review	**Final Exam (10am – 1pm)**	

Note: Assignments will be given in class and will be due over WebCourses. Consult WebCourses for all due dates.