

CIS 3362: Cryptography and Information Security - Fall 2026

Instructor: Arup Guha

Email: dmarino@ucf.edu

Office Hours: <https://www.cs.ucf.edu/~dmarino/ucf/OH.html>

Course Web Page: <https://www.cs.ucf.edu/courses/cis3362/fall2026> (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: MW 9:00 am – 10:15 am

Classroom: VAB-132

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 2500 or 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:

	<u>worth(% of grade)</u>
7 Homework Assignments (1%, 3%, 4%, 4%, 4%, 4%, 5%)	25%
Exams (15% each)	45%
Final Exam	30%

The grading scale will be based on the class average, standard deviation and overall difficulty of the assignments and exams. For further details, consult the grading philosophy posted on my web page (<http://www.cs.ucf.edu/~dmarino/ucf>).

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 stated in a different section on the next page. **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. Code breaking is a time consuming and tedious process. There's no way to skip the time or the tedium while still gaining these code breaking skills. Also, there will be times you get stuck and can't finish a homework problem on time. This is normal, don't feel bad if this happens. All you can ask of yourself is to put forth reasonable effort.

Community Service Opportunity

If you would like to earn an automatic 100% for the last homework assignment (worth 5% of the course grade), you can perform 5 hours of community service in between August 24th and November 15th, 2026. 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 16th, 2026, at the beginning of 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.*

Note, you will only get full credit if I receive the signed form and write up by 9:00 am on the due date. If I receive it at 9:10 am on November 16th, then you'll have to do the last homework assignment to earn the requisite credit. **Every semester, a couple students are just a couple minutes late and I don't count their forms. Please do the community service early and submit the forms to me way in advance, so that this doesn't happen to you.**

Exams

You will be allowed to use some aids on each of the exams. The specific aids allowed will be described in the class meeting directly prior to the exam.

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 will be 2 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 in person office hours only, but individuals can request Zoom meetings, if necessary.

Make Up Work Policy

If a student has a good reason to require a make-up exam, the student **MUST** make the request **before** the exam 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.) **Note: In almost all cases, when a make up is requested, a different assignment will be given so that I can post the solution to the regular course assignment on time.**

Tentative Course Schedule

Week	Monday	Wednesday	Sunday
Aug 24 – 28	Syllabus/Affine	Euclid's Alg	<i>HW #1 due</i>
Aug 31 – Sept 4	Substitution	Vigenere/ IC+MIC	
Sept 7 – 11	Labor Day	Playfair	<i>HW #2 due</i>
Sept 14 – 18	Transposition ADFGVX	Hill Cipher	
Sept 21 – 25	Enigma Navajo Code	EXAM #1	<i>HW #3 due</i>
Sept 28 – Oct 2	Coding Bitwise Operators	DES	
Oct 5 – 9	DES	AES	<i>HW #4 due</i>
Oct 12 – 16	AES, Symmetric Cipher Modes	EXAM #2	
Oct 19 – 23	Primes, Fermat Thm, Euler Thm	Miller Rabin, Disc Log	
Oct 26 – 30	Factoring, Fast Mod Expo	Diffie-Hellman WD Deadline	<i>HW #5 due</i>
Nov 2 – 6	RSA, El Gamal	ECC	
Nov 9 – 13	ECC	Veterans Day	<i>HW #6 due</i>
Nov 16 – 20	EXAM #3	Quantum Crypto	
Nov 23 – 27	Thanksgiving	Thanksgiving	
Nov 30 – Dec 3	Hash Functions, MAC & Dig Sigs	FE Review	<i>HW #7 due</i>
Dec 7 – 11	No Class	Final Exam, Dec 9 (7 am – 10 am)	

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.