Course Information

Course Number:	Math 4380 & 6380
Course Name:	Cryptography
CRN:	33801 & 31209
Location:	MCS 220
Class Hours:	2:00-3:00pm Monday, Wednesday, Friday
Textbook:	Required: Introduction to Cryptography with Mathematical Foundations and Computer Implementations by Stanoyevitch
Prerequisites:	MATH 2335 and Consent of Instructor

Instructor Information

Name:	Dr. Jeffrey Beyerl
Office Location:	MCS 231
E-mail:	jbeyerl@uca.edu
Phone:	501-450-5681

Course Description

Cryptography is the science of keeping information secure in an insecure medium. You use it when you check your e-mail, or go to a website, when you store data on the cloud or use a credit card. It's used seamlessly to verify your bank's identity when you use their app, and to hide your wireless traffic from an onlooker. This course is going to study [TBD based on pretest]

Office Hours

My availability changes every day. Go to the website below for up to date availability.

You can either schedule a virtual (Zoom) appointment, or in person. For in person office hours you will need to wear a mask and maintain social distance. Meet me at my office, but when possible, we'll meet in a conference room.
Appointments can be scheduled from 24 to 120 hours in advance.

Office Hours Website: https://ucamath.youcanbook.me/

Course Objectives and Requirements

The primary objectives in this course are to learn the number theory required for modern $\mathbb{Z}_n$ based cryptosystems; how these cryptosystems work and why; theory surrounding their security; then if time permits a mathematical description of modern symmetric cryptosystems and approaches toward quantum computing resistant cryptosystems.

Student Learning Objectives

Upon completion of the course, student will be able to:

- Describe conceptual ideas and solve key number theory problems related to cryptography
- Construct a modern cryptosystem
- Cryptanalyze a modern cryptosystem in multiple ways

Grading Policy

Undergraduate Grading Scale	
Attendance	20%
Homework	30%
Tests & Final Exam	50%

Graduate Grading Scale	
Attendance	20%
Homework	20%
Tests & Final Exam	50%
Project	10%

Homework and tests will be structured in an unusual but clever manner meant to marry the standard 10-point grading scale with the expectations associated with this kind of content. The first homework assignment will make it make a lot more sense, but here is a brief description:

- Each assignment & test will be split into 4 sections.
- There is no partial credit, you earn points only for what you have mastered.
- Credit is given for correct answers, or *nearly* correct answers.
  (I won't split hairs on minor mistakes)
- There are more problems per part than is required for the maximum score
  (Balances out no partial credit)
- In each section you cannot earn more points than the maximum score
  (No extra credit)

Part	Number of questions	Points per question	Maximum Score
1	Many	Lots	59 (Cumulative 59)
2	Lots	A little less	20 (Cumulative 79)
3	Several	A bit	10 (Cumulative 89)
4	A few	Very little	11 (Cumulative 100)

The idea behind this grading method is that part 1 has very simple things. There's plenty of problems and you choose enough of them to easily get up to an almost-passing score.

Parts 2 and 3 start to flesh out some of the things we are learning in some depth. Part 2 will reflect a basic understanding and has enough points to get almost up to a B. Part 3 will start to require some deep understanding and can almost get you up to an A.

Part 4 are the hardest problems that require true mastery of the content. Solving even one problem in part 4 is enough to put you into an A, assuming you scored all the points from parts 1-3. More than that is icing on the cake.

Important Dates

Last day to Drop Drop means the course is not on your record	January 20th
Test 1	Friday, February 18th
Test 2	Friday, March 18th
Last day to Withdraw Withdraw means the course is on your record with a "W" but does not factor into your GPA. Talk to your professor, advisor, and financial aid officer before withdrawing.	April 8th
Test 3	Friday, April 28st
Final Exam	Friday, May 6th 10:00am-noon

Outside of class resources

- The Textbook
  - Description of material
  - Example and exercise problems
- Blackboard
  - Test solutions
  - PowerPoints from class
  - Other class materials
- Office Hours
  - Individual help
  - Availability changes every day. See https://ucamath.youcanbook.me/.
- The Math Resource Lab
  - Study Area
  - Tutors available throughout the day (albeit, they will be of no help)

Late Work

Late work from an excused absence can be turned in with no penalty within 1 week; 20% after that.
Late work from an unexcused absence can be made up with a 20% penalty within 1 week; 50% after that.

Excused Absences

If you have a pre-arranged absence or an extenuating circumstance, let me know so we can discuss if it is excused or unexcused.
VERY IMPORTANT DO NOT COME TO CLASS IF YOU THINK YOU MIGHT BE SICK. If you have a fever or persistent cough or other coronavirus symptoms, take the appropriate recommended action and E-mail me when you are able to.

Attendance Policy

Your active participation in this course is expected and required for you to learn the material and earn a passing grade. If you miss more than two weeks of class meetings throughout the term, you may be administratively dropped from the course.

Academic Integrity Statement

The University of Central Arkansas affirms its commitment to academic integrity and expects all members of the university community to accept shared responsibility for maintaining academic integrity. Students in this course are subject to the provisions of the university's Academic Integrity Policy, approved by the Board of Trustees as Board Policy No. 709 on February 10, 2010, and published in the Student Handbook. Penalties for academic misconduct in this course may include a failing grade on an assignment, a failing grade in the course, or any other course-related sanction the instructor determines to be appropriate. Continued enrollment in this course affirms a student's acceptance of this university policy.
Academic integrity is taken seriously: cheating on a test will result in a failing grade in the course; allowing another student to copy off of your test will result in a one-letter-grade penalty.

Americans with Disabilities Act Statement

The University of Central Arkansas adheres to the requirements of the Americans with Disabilities Act. If you need an accommodation under this Act due to a disability, please contact the UCA Office of Disability Services, 450-3613.

Title IX disclosure:

If a student discloses an act of sexual harassment, discrimination, assault, or other sexual misconduct to a faculty member (as it relates to "student-on-student" or "employee-on-student"), the faculty member cannot maintain complete confidentiality and is required to report the act and may be required to reveal the names of the parties involved. Any allegations made by a student may or may not trigger an investigation. Each situation differs and the obligation to conduct an investigation will depend on those specific set of circumstances. The determination to conduct an investigation will be made by the Title IX Coordinator. For further information, please visit: https://uca.edu/titleix. *Disclosure of sexual misconduct by a third party who is not a student and/or employee is also required if the misconduct occurs when the third party is a participant in a university-sponsored program, event, or activity.

Sexual Harassment and Academic Policies Statement

All students are required to familiarize themselves with the University of Central Arkansas policy on sexual harassment and on academic policies. These policies are printed in the Student Handbook.

Building Emergency Plan Statement

An Emergency Procedures Summary (EPS) for the building in which this class is held will be discussed during the first week of this course. EPS documents for most buildings on campus are available at http://uca.edu/mysafety/bep/. Every student should be familiar with emergency procedures for any campus building in which he/she spends time for classes or other purposes.

Pandemic Information

- You need to follow all university policies including those on masks. Specifically All students are expected to comply with the University policy regarding face coverings (see https://uca.edu/coronavirus/students/)
- At the time of this writing, the university requires masks in nearly all indoor areas specifically including classrooms.
- I've been vaccinated. You are encouraged to get vaccinated if you haven't yet. If I had access to information that everyone in our course has been vaccinated for COVID, that would be stated here so that we could all be more comfortable with our classmates. As of the time of this writing, I cannot say that everyone in our class has been vaccinated and so you are encouraged to keep your distance from your classmates.
- If you are sick, do not come to class. E-mail me and I will made individual accommodations based on the information you provide.
- If we are directed to pivot online and cease in person meetings, we will meet synchronously on Zoom.
- If we are directed to limit in-person seating below the enrollment of the course, we will cease in person meetings and meet synchronously on Zoom.