CLASSIFIED

SYLLABUS

MATH 408-01 (CSCI 408-01) Cryptography

Fall 2016

Head of Agency

Agent:	Dr. Ho (Code Name: Anne)
Office:	Wall 124B
Telephone:	843-349-4075
E-mail:	aho@coastal.edu
Office Hours:	M 2-3:30pm, T 10:15-11am, W 1:30-3:30pm, F 9-10am
Outreach:	MW 12:30-1:30pm on the second floor of the library

Description

Schedule: TTh 3:05-4:20pm Wall 309 (8/23/16-12/6/16)

Prerequisite: A grade of C or better in MATH 220 or MATH 174.

Textbook: *Introduction to Cryptography with Coding Theory* (2nd edition) by Trappe and Washington

Software: We will be using SageMath (https://cloud.sagemath.com), which is a Python-based open-source math software system.

Moodle: I will be using Moodle (http://moodle.coastal.edu) to post training materials and grades.

Topics: Modular arithmetic, classical encryption schemes, modern encryption schemes, password security, digital signatures, and secret sharing.

Objectives: We will cover the fundamentals of cryptography and current-day issues through computational, proof-based, and coding exercises.

Priority Missions (aka Exams): There will be three opportunities (take-home exams) for you to demonstrate your expanding set of secret agent skills on:

- Thursday, 9/29 at 11:59pm
- Thursday, 10/27 at 11:59pm
- Thursday, 12/15 at 11:59pm

Missions (aka Assignments): Missions consist of homework and in-class assignments. Doing all of the missions is necessary for you to pass. You are encouraged to discuss problems with fellow agents-in-training. In fact, if you help someone with a mission, you will get one extra credit point per assignment (up to 10 points throughout the semester, and up to 100% on your assignments grade). If you receive help on a mission, you must write down the name of the person who helped you. Helping someone is *not* doing the assignment for the other person though, and you are still expected to individually write up your solutions. You are responsible for your own understanding of the material. *Absolutely no late assignments will be accepted*. If you must be gone, turn in your assignments early. Please ask questions!

Grade Guidelines: Assignments (Missions) = 40%, Exams (Priority Missions) = 60%

Grade Scale: A = 90-100%, B = 80-89%, C = 70-79%, D = 60-69%, F = below 60%

Important Dates:

Monday, Sept 5	Labor Day holiday
Friday, Oct 7	Student holiday
Thursday, Oct 27	Last day to drop with grade of “W"
Tuesday, Nov 8	Election Day
Nov 21-25	Thanksgiving break
Wednesday, Dec 7	Last day of classes

Students with Disabilities: Any student with a documented disability needing academic adjustments is requested to speak with me during the first week of class. All discussions will remain confidential.

Attendance Policy: Students are obligated to attend class regularly. Absences, excused or not, do not absolve students from the responsibility of completing all assigned work promptly. Read the following for details: http://www.coastal.edu/policies/pdf/acad-125classattendance.pdf.

Statement of Academic Integrity: CCU is an academic community that expects the highest standards of honesty, integrity and personal responsibility. Members of this community are accountable for their actions and reporting the inappropriate action of others and are committed to creating an atmosphere of mutual respect and trust. Please review the revised Code of Conduct that is available at: https://www.coastal.edu/conduct/

Math 408 / CSCI 408 – Student Learning Outcomes

Upon successful completion of the course, agents will be able to:

1. Solve basic number theory problems involving modular arithmetic, primes, factoring, the Euclidean algorithm, and the Chinese Remainder Theorem.
2. Utilize classical ciphers for encryption and decryption.
3. Be familiar with possible attacks and cryptanalysis of classical ciphers.
4. Understand and use the Data Encryption Standard.
5. Understand and use RSA as well as attacks on RSA.
6. Understand and use ElGamal and the Digital Signature Algorithm.
7. Be comfortable with basic coding problems in SageMath (Python).
8. Be familiar with current issues and research, including quantum cryptography.

The syllabus is for planning purpose only and is subject to change anytime.