CSCI 4481: Cryptography & Data Security

Fall 2026 Syllabus

Instructor: Dr. Vincent A. Cicirello **Office:** USC2-313
E-mail (course related): Use course Blackboard Course Messages tool. **Phone (office):** x3526
E-mail (other than this course): See campus directory for address.

Course Time / Location:
- Tuesdays (D009) / Thursdays (C008), 12:30pm-2:20pm.

Office Hours:
- Thursday 10:30am - 12:00noon (Office: USC2-313)
- Wednesday 10:00am – 3:00pm (Zoom by appointment)
- Other days/times by appointment either in my office or via Zoom.
- You can also just drop by my office, and if I'm there I'm happy to assist you.

Course Description:
Cryptography has become an essential tool for data security. It is used to provide data confidentiality, integrity, and availability. It supports the authentication of data and protection of privacy. However, cryptography is only one component of a security system. There are hardware, software engineering, social and political issues that also must be considered. This course provides a broad view of security with practical applications of cryptography to data security. Specific topics include classical and modern encryption techniques, steganography, and human factors.

Prerequisites: Minimum grade of C in all of the following: MATH 2216 Calculus II, CSCI 2226 Foundations of Computer Science, and CSCI 2102 Programming & Problem Solving II

Q2: This course is a Q2 (Quantitative Reasoning Across the Disciplines). Among the math concepts from prior courses that you will be using in this course are the following: (a) discrete math topics including set theory, logic, number theory, and several other topics covered in CSCI 2226 and its pre-req MATH 2225; and (b) calculus at the level of Calculus II (MATH 2216). Additionally, there are some math topics that most of you would not have encountered previously, that we'll cover in the course, which include: (c) linear algebra (if you've had MATH 3323, you will be ahead here, otherwise we'll cover what we need in the course), and (d) abstract algebra (this will be totally new to all of you).

Required Textbook:
- *Cryptography and Network Security: Principles and Practice*, 8th edition, William Stallings, 2021. ISBN: 9780135764213 (ebook) or 9780136707226 (print book). https://www.pearson.com/en-us/subject-catalog/p/cryptography-and-network-security-principles-and-practice/P200000003477/9780135764213

Other Requirements:
- **Calculator:** You are allowed to use a calculator during exams, but it must be a simple (non-programmable, no-wifi, etc) calculator. You are not allowed to use a cell phone, smart watch, or any other device as your calculator. Your calculator must be a calculator and nothing else (otherwise you'll do without one).

Stockton Computer Science Student Outcomes:
This course supports students in their development of the following Computer Science student outcomes:

- Outcome 1: An ability to analyze a complex computing problem and to apply principles of computing and other relevant disciplines to identify solutions.
  - 1.a: Students will analyze a complex computing problem.
  - 1.b: Students will apply principles of computing and other relevant disciplines to identify solutions to a complex computing problem.
- Outcome 2: An ability to design, implement, and evaluate a computing-based solution to meet a given set of computing requirements in the context of the program's discipline.
  - 2.a: Students will design a computing-based solution to meet a given set of computing requirements.
  - 2.b: Students will implement a computing-based solution to meet a given set of computing requirements.
  - 2.c: Students will evaluate a computing-based solution to meet a given set of computing requirements.
- Outcome 6: An ability to apply computer science theory and software development fundamentals to produce computing-based solutions.
  - 6.a: Students will apply computer science theory to produce computing-based solutions.
  - 6.c: Students will evaluate the effects of alternative data representations and algorithms on the performance of computing-based solutions.

Course IDEA Objectives:
The IDEA objectives of this course include:

- Gaining a basic understanding of the subject (knowledge of cryptography including the field's terminology and methods, as well as modern trends in applying cryptography to data security; fundamental principles and theories underlying cryptographic algorithms, including the mathematical foundations of cryptography).
- Learning to apply cryptography to solving data security problems.
- Developing specific skills, competencies, and points of view needed by professionals in the field most closely related to this course.
- Learning appropriate methods for collecting, analyzing, and interpreting numerical information.

Grading:

Exams (3 equally weighted exams)	50%
Homework assignments	50%

Grading Scale:

Letter grade and range	Letter grade and range	Letter grade and range
A: at least 90.00	A-: at least 89.50	B+: at least 89.00
B: at least 80.00	B-: at least 79.50	C+: at least 79.00
C: at least 70.00	D: at least 60.00	F: less than 60.00

Note: The chart above deliberately does not include C-, D+, or D-. Those grades are not used in this course.
Another note: I reserve the right to adjust the scale at the end of the semester. Such adjustments are rare, but will only be in your favor; and are highly unlikely to occur at the C/D or D/F boundaries. Note the 2 decimal places in the chart above (i.e., I do not round to the nearest whole number): e.g., unless I adjust the grade scale, an 89.99 is an A-, etc. If I adjust the scale, it is done using a semi-automated approach involving clustering (i.e., "automated" == a program I wrote suggests a new scale based on all of the grades of the class; "semi-" == if that program's output is crazy, I ignore it and leave the scale alone; and "clustering" == a statistical technique). I never simply add a constant number of points to everyone's overall course

score. What is clustering? For a non-technical explanation, consider the hypothetical question, "Are the grades of this student, who is currently in the B range, more like the grades of the A students, more like the grades of the rest of the B students, or somewhere in between the two?" Clustering may take a student in the B range from the scale above (at least 80.00), and either keep them in the B range if their grades are more like the rest of the B students, or bump them all the way up to the A range if their grades are more like the A students, or bump them partially up to either B+ or A- if they are somewhere in between.

Generative A.I. Prohibited:
Generative artificial intelligence (AI), such as but limited to ChatGPT, GitHub Copilot, and other similar systems, may **not** be used for any work or assignments required in this course. Although you will undoubtedly use such tools in your future careers, it is important that you develop your programming skills, problem solving skills, and mathematics skills so that you can later effectively use such tools to enhance your productivity. Copilot, ChatGPT, etc often produce solutions that are buggy, only partially correct, among other issues that one must address with their own knowledge. The use of generative AI programs defeats the programming requirements and critical thinking skills that are vital to achieving our learning outcomes. Submission of partial or complete work from generative AI programs is not permitted and will be treated as an Academic Honesty violation, and handled in accordance with the course Academic Honesty procedure (see below) as well as Stockton's Student Academic Honesty Procedure and handled in accordance with these Procedures. If I suspect that work submitted in the course may have been the product of a generative AI tool, I will likely begin by asking you to explain the solution (e.g., to explain the details of all of the calculation steps of any math involved, or to explain how code works, etc).

Academic Honesty:
Become familiar with Stockton's Student Academic Honesty Procedure. Each violation is penalized by a 0 on the assignment/exam/etc, plus a 10 point penalty on your overall course grade. For example, if you have one violation, you'll have a 0 on that assignment or exam plus 10 points off your overall average, but if you have two violations, you'll have grades of 0 on the two assignments/exams/etc and 20 points off your overall average. Example violations include, but are not limited to: (a) any form of cheating on an exam or assignment, (b) passing off the work of another as your own (including other students, former students, code or problem solutions found on the Internet written by someone else, code generated by generative A.I. such as but not limited to ChatGPT, GitHub Copilot, etc), (c) assisting someone in violating the academic honesty policy, (d) asking someone to assist you in cheating or other academic honesty violations (even if they refuse to help you cheat), etc. [Yes, I encountered that last one once in a General Studies course.]

Exams:
The exams are not cumulative. You are allowed one sheet of notes for each exam (both sides of an 8.5 by 11 piece of paper). You are also allowed to use (and strongly advised to use) a calculator during the exams, which must be a simple non-programmable calculator. Although the exams are on paper, I am deliberately scheduling Exam 2 on a day when we are in the computer lab, where I will give you access only to the Windows calculator app, which has a mode with hexadecimal and bit-level operations, which will be highly useful for that exam only. For exams 1 and 3, you will need your own simple (non-programmable) calculator. Although you are free to use your own handheld calculator during exams, you are NOT allowed to use any communications device (e.g., smart phone, smart watch, etc) during exams (not even for calculator purposes). **Your calculator must be a calculator only.**

Make-Up Exams: Make-up exams will not be given (i.e., missed exam = 0), with the following exceptions:
1. Medical excuse: Provide documentation to the Wellness Center who will then contact all of the instructors of your courses.

2. Based on University policy (https://stockton.edu/policy-procedure/documents/procedures/2030.pdf), if you are to be absent for a religious holiday on the date of an exam, you must notify me of that planned absence during the first 10 business days of the semester.

Homework Assignments:
A significant portion of your grade in this class comes from performance on homework assignments. The type of homework assignment will vary. Some will involve some programming. You may use either Java or Python for assignments involving programming. Other homework assignments will consist of sets of problems pertaining to the various cryptographic algorithms we will be covering in the course. Some of these may also include sets of problems for the underlying mathematics. All homework assignments are to be completed individually unless otherwise indicated by the instructor. You must also show all work for problems involving math.

- **Paper then Scan**: I strongly suggest that problems involving math are done on paper and then scanned to submit in Blackboard. It will probably take you less time to do it that way, then to try to format math in Word or some other word processing software.
- **Phone PDF Scanner Apps**: On Android, Google Drive has the ability to scan to a pdf. Something similar is available for iPhones.
- **Programming**: For assignments involving programming just submit the source code and anything else specified on the assignment page.

Due Dates: Homework Assignments are due in Blackboard by 11:59pm on the dates due (dates found in Blackboard on the assignment pages). Late assignments are penalized as follows: (a) 25% off if late by no more than 24 hours, (b) 50% off if late by no more than 48 hours, (c) 75% off if late by no more than 72 hours, and (d) a grade of 0 if late by more than 72 hours. The first time a homework assignment is late (within 72 hours), the late penalty is waived.

Incomplete Policy:
In general, no grades of incomplete will be given. The only exception to this rule is an institutionally documented medical emergency that necessitates your complete absence from Stockton for at least two continuous semester weeks. Additionally, you must be caught up on all work up to the point where your medical emergency began and currently in the "C" range or better overall at the point where the emergency began.

Participation:
There is no explicit participation grade in this course. However, you will likely achieve greater grades on assignments and exams if you are actively participating, such as asking questions about things you are uncertain about, attending class consistently, etc.

Timeline:
This schedule is subject to change. Changes will be announced via Blackboard (and in class). If tentative exam dates change, they will be announced at least one week prior.

Date (Tuesdays)	**Topic (Tuesday)**	**Date (Thursdays)**	**Topic (Thursday)**
Sept 8	Introduction and Overview of Cryptography	Sept 10	Classical Cryptosystems
Sept 15	Classical Cryptosystems	Sept 17	Classical Cryptosystems
Sept 22	Number Theory Background	Sept 24	Number Theory Background
Sept 29	Number Theory Background	Oct 1	Slack and/or Review for Exam
Oct 6	**EXAM 1**	Oct 8	The Data Encryption Standard
Oct 13	The Data Encryption Standard	Oct 15	The Advanced Encryption Standard
Oct 20	The Advanced Encryption Standard	Oct 22	The Advanced Encryption Standard
Oct 27	**NO CLASS: Precepting Day**	Oct 29	Slack and/or Review for Exam
Nov 3	**EXAM 2**	Nov 5	RSA and Public Key Cryptography
Nov 10	RSA and Public Key Cryptography	Nov 12	Discrete Logarithms and More Public Key Cryptosystems
Nov 17	Discrete Logarithms and More Public Key Cryptosystems	Nov 19	Hash Functions
Nov 24	Hash Functions	Nov 26	**NO CLASS: Thanksgiving**
Dec 1	Message Authentication Codes	Dec 3	Digital Signatures
Dec 8	Digital Signatures	Dec 10	Slack and/or Review for Exam
Dec 15	**EXAM 3: 12:30-2:30**		