CSIS 4481: Cryptography and Data Security
Fall 2016 Syllabus

Instructor: Dr. Vincent Cicirello
Office: G-116
E-mail: cicirelv@stockton.edu
Phone (office): 609-626-3526

Office Hours: Tuesdays/Thursdays, 1:15-2:15pm
Available other times by appointment
Or, feel free to drop-in any time I'm in my office (if I'm not on my way to a meeting or class, I'd be happy to talk to you).

Course Time and Location: Tuesdays & Thursdays, 10:30am-12:20pm, G-108

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.

CSIS Learning Outcomes: In this course, you will progress toward the following CSIS Learning Outcomes:

- **Outcome CSIS.a**: An ability to apply knowledge of computing and mathematics appropriate to the program's student outcomes and to the discipline.
  - **CSIS.a.2**: Students will use statistical concepts to model and interpret data.
  - **CSIS.a.3**: Students will apply discrete mathematics concepts and algorithms.
- **Outcome CSIS.c**: An ability to design, implement, and evaluate a computer-based system, process, component, or program to meet desired needs.
  - **CSIS.c.2**: Students will implement a computer-based system, process, component, or program from a given specification.
- **Outcome CSIS.e**: An understanding of professional, ethical, legal, security and social issues and responsibilities.
  - **CSIS.e.2**: Students will recognize and describe current issues in security.
- **Outcome CS.j**: An ability to apply mathematical foundations, algorithmic principles, and computer science theory in the modeling and design of computer-based systems in a way that demonstrates comprehension of the tradeoffs involved in design choices.
  - **CS.j.2**: Students will evaluate the effects of alternative data representations and algorithms on the performance of computer based systems.

IDEA Course Objectives: The objectives of the course include:

- **IDEA learning objective 1:** Gaining knowledge of cryptography including the field's terminology and methods, as well as modern trends in applying cryptography to data security
- **IDEA learning objective 2:** Learning the fundamental principles and theories underlying cryptographic algorithms, including the mathematical foundations of cryptography
- **IDEA learning objective 3:** Learning to apply cryptography to solving data security problems

Prerequisites: CSIS 2101 and MATH 2216 and (either CSIS 2226 or MATH 3325) and (either CSIS 2102 or MATH 3323). You must have completed Programming/Problem Solving I as well as Calculus II. You also must have knowledge of Discrete Mathematics beyond the level of MATH 2225 (this means either Foundations of CS or Foundations of Math). The couple topics needed that are usually covered in CSIS 2102 and the couple topics needed from MATH 3323 will be covered at an accelerated pace within the course as they are needed (thus the requirement that you must have had one or the other of these courses previously).

Required Textbooks: *Cryptography and Network Security: Principles and Practice* (7th Edition), by W. Stallings, 2017. ISBN: 0-13-444428-0.

Other Requirements: The Blackboard course management system will be used to provide access to copies of classroom presentation materials and other resources. Additionally, I will periodically post announcements within Blackboard; and Blackboard will also be used for all e-mail correspondence for this course. You are responsible for checking your Blackboard mail on a daily basis. Any e-mail that I may send regarding assignments, tests, etc will be within Blackboard. Some assignments will be submitted via Blackboard.

Grading:	Exam 1	12%
	Exam 2	12%
	Exam 3	12%
	Homework assignments / Problem sets	60%
	Participation	4%

Grading Scale:

A: Overall Average at least 90.00 **AND** Exam Average at least 80.00.	**A-:** Overall Average at least 89.00 **AND** Exam Average at least 80.00.	**B+:** Overall Average at least 88.00 **AND** Exam Average at least 80.00.
B: Overall Average at least 80.00 **AND** Exam Average at least 70.00.	**B-:** Overall Average at least 79.00 **AND** Exam Average at least 70.00.	**C+:** Overall Average at least 78.00 **AND** Exam Average at least 70.00.
C: Overall Average at least 70.00 **AND** Exam Average at least 60.00.	**C-:** Overall Average at least 69.00 **AND** Exam Average at least 60.00.	**D+:** Overall Average at least 68.00 **AND** Exam Average at least 60.00.
D: Overall Average at least 60.00 **AND** Exam Average at least 50.00.	**D-:** Overall Average at least 59.00 **AND** Exam Average at least 50.00.	**F:** Overall Average less than 59.00 **OR** Exam Average less than 50.

I reserve the right to adjust the scale at the very end of the semester. Such adjustments are rare, but will only be in your favor.

Exam 1, Exam 2, Exam 3: 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. If your calculator supports hexadecimal, that will be especially beneficial.

Homework Assignments / Problem Sets: The largest part of your grade in this class comes from performance on homework assignments. The type of homework assignment will vary. Some will involve some programming. I'm assuming most of you will likely use Java for programming aspects of assignments since that is the language currently taught in the programming & problem solving sequence, but if you wish to use some other language (e.g., C, C++, Python) you can do so, provided you get approval from the instructor for your language of choice. 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 worked on individually unless otherwise indicated by the instructor.

Participation: A portion of your overall grade will come from participation. This will include general participation elements such as contributing to class discussion, etc. I do not explicitly factor attendance into your grade. However, if you miss class frequently, then you must not be participating very well, and your class participation grade will be affected. Participation grades are most often negatively affected by disruptive behavior, such as the following: ringing cell phones, making phone calls, answering phone calls, arriving late or leaving early in a distracting way (e.g., dropping books, talking, using front door to classroom while class is in session), using computers/devices for non-course purposes, etc.

Due Dates: Depending on the nature of the homework assignment, they will either be due: (a) on paper at the beginning of a class session; or (b) electronically via Blackboard for assignments involving programming. Assignments (involving programming) that must be submitted electronically will be due by 11:59pm. Problem Sets can optionally be submitted electronically, but will be due by class time whether submitted on paper or electronic. Late assignments are penalized by 25% if less than 24 hours late, 50% if less than 48 hours late, and 75% if less than 72 hours late. The first time an assignment is late (within 72 hours of deadline), the late penalty will be waived. **Late assignments won't be accepted after class time on Dec 8.**

Academic Honesty: Please familiarize yourself with Stockton's policy on academic honesty. The in-class exams are closed book---no texts, other students tests, or other aids may be consulted during these tests. You will, however, be allowed one sheet of 8.5x11 paper of notes for the exams. **A calculator may also be used during exams.** "Other aids" that are not allowed include cell phones (not even for calculator purposes), pagers, PDAs, and other communications devices. Unless indicated for a specific assignment, all problem sets and other homework assignments are to be your own individual work. You are to individually solve problems. You are to do individually any required programming. Code found on the Internet, etc is prohibited. **Any first violation will be penalized with a 0 on the relevant exam or assignment, AND 10 points off your overall average. Any subsequent violation will result in a course grade of F.**

Make-Up Exams: Make-up exams in general will not be given (i.e., if you miss an exam, you get a 0). The only exceptions to this rule are the following:

1. Documented medical excuse: provide documentation via Stockton's Wellness Center.
2. Other institutional excuses: If a Stockton-related conflict arises (e.g., an away game for a Stockton team that you are on, a fieldtrip for a Stockton course, etc). I must be notified of the conflict one week prior to the missed exam, with written documentation (e.g., letter from Stockton coach or Stockton sponsor of field trip, etc).

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 absence from Stockton for a period greater than 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 your emergency began.

Tentative Schedule:
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	Text and Topic
September 6	Introduction and Overview of Cryptography
8	Classical Cryptosystems
13	Classical Cryptosystems
15	Classical Cryptosystems
20	Number Theory Background
22	Number Theory Background
27	Number Theory Background
29	Slack and/or Review for Exam
October 4	**EXAM 1**
6	The Data Encryption Standard
11	The Data Encryption Standard
13	The Advanced Encryption Standard
18	The Advanced Encryption Standard
20	The Advanced Encryption Standard
25	**NO CLASS: Preceptorial Advising Day**
27	The RSA Algorithm and Public Key Cryptography
November 1	The RSA Algorithm and Public Key Cryptography
3	Slack and/or Review for Exam
8	**EXAM 2**
10	Discrete Logarithms and More Public Key Cryptosystems
15	Discrete Logarithms and More Public Key Cryptosystems
17	Hash Functions
22	Hash Functions
24	**NO CLASS: Thanksgiving**
29	Message Authentication Codes
December 1	Digital Signatures
6	Digital Signatures
8	Slack and/or Review for Exam
15	**EXAM 3 (Thursday, December 15, 10:30-12:30)**