CSIS 4481: Cryptography and Data Security
Fall 2018 Syllabus

Instructor: Dr. Vincent A. Cicirello **Office:** G116
E-mail: Please use course Blackboard mail tool. **Phone (office):** x3526

Office Hours: Tuesday/Thursday 10:30am-11:30am
Available other times by appointment; drop-ins also welcome

Course Time and Location: Tuesdays & Thursdays, 2:30pm-4:20pm, 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.

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

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 either of the following CSIS 2226 or MATH 3325; 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 probably be totally new to all of you).

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 electronic communications 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:	Exams (3 equally weighted exams)	50%
	Homework assignments / Problem sets	50%

Grading Scale:

A: at least 90.00	A-: at least 89.00	B+: at least 88.00
B: at least 80.00	B-: at least 79.00	C+: at least 78.00
C: at least 70.00	C-: at least 69.00	D+: at least 68.00
D: at least 60.00	D-: at least 59.00	F: less than 59.00

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; and are highly unlikely to occur at the D-/F boundary. 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.

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. Since our class meets in a computer lab, even on exam days, I will allow you access to Window's calculator app (but nothing else) during exams. The Window's calculator has a programmer mode that supports arithmetic in hexadecimal, along with the various bit level operations, so don't go out and buy a new calculator just for this course. 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).

Homework Assignments / Problem Sets: 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 worked on individually unless otherwise indicated by the instructor.

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.

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 (assignments are not accepted if more than 72 hours late). The first time an assignment is late (within 72 hours of deadline), the late penalty will be waived.

Academic Honesty: Please familiarize yourself with Stockton's policy on academic honesty. Each violation will be penalized by a 0 on the relevant 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. Examples of 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 found on the Internet written by someone else, 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.

Make-Up Exams: Make-up exams will not be given (i.e., missed exam = 0), with the following exceptions:

1. Medical excuse: Provide documentation the first class you return after the missed exam. I suggest providing the documentation to the Wellness Center who will then contact all of the instructors of your courses.
2. Other institutional excuses: Situations may arise related to Stockton that prevents you from being able to attend an exam. In most such cases, you should be aware of the conflict beforehand. Thus, I must be notified one week prior to the missed exam. Send me e-mail via Blackboard with the details of the planned absence, and provide documentation (e.g., memo from sports coach, from other faculty sponsoring a 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 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.

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
11	Classical Cryptosystems
13	Classical Cryptosystems
18	Classical Cryptosystems
20	Number Theory Background
25	Number Theory Background
27	Number Theory Background
October 2	Slack and/or Review for Exam
4	**EXAM 1**
9	The Data Encryption Standard
11	The Data Encryption Standard
16	The Advanced Encryption Standard
18	The Advanced Encryption Standard
23	**NO CLASS: Preceptorial Advising Day**
25	The Advanced Encryption Standard
30	The RSA Algorithm and Public Key Cryptography
November 1	The RSA Algorithm and Public Key Cryptography
6	Slack and/or Review for Exam
8	**EXAM 2**
13	Discrete Logarithms and More Public Key Cryptosystems
15	Discrete Logarithms and More Public Key Cryptosystems
20	Hash Functions
22	**NO CLASS: Thanksgiving**
27	Hash Functions
29	Message Authentication Codes
December 4	Digital Signatures
6	Digital Signatures
11	Slack and/or Review for Exam
13	**EXAM 2: (Slightly) different time: 2:30-4:30**
18	**NO CLASS (finals week)**