CARNEGIE MELLON UNIVERSITY

Heinz College

95-749 Cryptography

Spring 2024 (Mini 4)

Syllabus, v2.0

General

Instructor / Course Support

Instructor: Dr. Robert Beveridge: rbeverid@andrew.cmu.edu

Office Hours and Location: *By appointment; set up via email

TA: TBD

Book:

Cryptography and Network Security, 8th edition, by William Stallings:

1. Go to cmu.redshelf.com. Search for the title with the ISBN 9780135764268 which will cost $34.99 for 180 day digital rental or $54.99 for digital purchase. View details, add to cart, check out. The eBook will be on the RedShelf shelf.
2. Go to bookstore.web.cmu.edu. Click on the arrow down below "Textbooks" and choose "Online Bookstore." Find the course and choose which option you want. All 3 options will appear there: 180 day digital rental ($34.99), digital purchase (54.99), or loose-leaf ($73.50). Any digital content will be on the VitalSource Bookshelf.

RedShelf and VitalSource both provide access to the same digital content and both are very similar with highlighting options, notes, etc. Some students may have a preference for one over the other so it is nice to offer either option. The print option is only available through option #2 above.

Course Description

This course emphasizes practical employment of cryptography. Topics in this course include:

* the techniques used to design cryptographic mechanisms (block ciphers, stream ciphers, hash algorithms, digital certificates, and others)

* how these mechanisms have been incorporated into modern security technologies

* when/how to apply these methods to incorporate security into cyber activities

Learning Objectives

Cryptography: Purpose and Ethical Considerations

The Mechanisms Behind Cryptography

Block Ciphers
Stream Ciphers
Hash Functions
Public Key Cryptography
Public Key Infrastructures
Digital Signatures
Extensible Authentication and Cryptography
Commercial Cryptography Deployments

Prerequisites

No prerequisites; however, there is an expectation that students have a general knowledge of IT principles and cyber security topics, and familiarity with mathematical principles. This includes the use of Virtual machine software such as VMware for windows and or Mac and/or Virtualbox. Student computers should have enough resources to run at least 1 virtual machine (4 GB of memory and 20GB of free disk space is recommended)

Course Management

All course materials will be managed through Canvas, including assignments and other information. Check frequently to ensure you have the latest information about the course. Topical readings that support the course lectures may be added. These readings will be posted under the course schedule portion of the syllabus. *Students are expected to read the material as part of the course materials.* In some cases, these readings will be integrated to homework assignments.

Course Updates and Changes

This syllabus represents the course plan as conceived at the beginning of the semester but is ***subject to change and modification by the instructor at any time***. Advanced notice will be provided to students through Canvas announcements, and when necessary, an updated syllabus will be issued.

Lectures, Assignments and Exams

1. The block quizzes are 30% of the course grade.
2. The midterm that is worth 30% of the grade.
3. Assignments and challenges throughout the course is worth 10% of the grade
4. There will be a final project to explain an implementation of a complete cryptosystem in enterprise environments. This project will be 30% of the total course grade. This may be a group assignment.

5. Late Submissions: Homework is due at 11:59 pm on the assigned due date (Eastern U.S. Time Zone). Penalty for late submissions is 25% per day. NOTE: Quizzes are only allowed to be 'made up' under exceptional circumstances. See the instructor (in advance if possible) to request an exception to this policy.

Recorded lectures will be posted (more information to come)

Grading Rubric

Grading Rubric Letter	Interpretation	Point Totals	GPA
A+	Exceptional	96.6 – 100	4.33
A	Excellent	93.3 – 96.5	4.00
A-	Very Good	90.0 – 93.2	3.67
B+	Good	86.6 – 89.9	3.33
B	Acceptable	83.3 – 86.5	3.00
B-	Fair	80.0 – 83.2	2.67
C+	Poor	76.6 – 79.0	2.33
C	Very Poor	73.3 – 76.5	2.00
C -	Minimal Passing	70.0 – 73.2	1.67
D	Failing	Below 70	0

Attendance Policy

Attendance is mandatory when being taught on campus. Online accommodation may be made if appropriate and if sanctioned by the university. Student progress will be driven by block quiz completions, so consistent work toward completion is expected.

Classroom Etiquette

This is a Master's level course taught as part of a professional degree program. Accordingly, you are expected to conduct yourself in a professional manner during the course and not engage in behavior in the class that would be considered unacceptable in the workplace. If you have a question about the content of the lecture, please direct it to me. If you are confused about an issue, chances are your classmates are confused as well. Sharing your questions with the group is a great way to help all students advance through the course and is encouraged.

Policy on Cheating and Plagiarism

For any assignment found to be the partial or complete result of cheating or plagiarism, your grade for that assignment will be zero. Cheating is defined as inappropriate collaboration among students on an assignment or failure to cite others' work used in the submissions, evaluation materials or presentations. This can include copying someone else's work with or without alteration. When students are found to be collaborating in this way, *ALL*

COLLABORATORS will pay the penalty regardless of who originated the work. Please refer to the University's policies here: http://www.cmu.edu/policies/StudentPolicy.html

Student Wellness and Student Accommodations

The College and this course always have the student's best interest as a foundational goal. As such, this course is conducted to support all University policies regarding accommodating verified student needs, and supporting student health in general.

Block Schedule Dates

Blocks below were mapped to weeks in the 8-week course. This summer course is designed around the schedule below. Materials will be available in advance and can be completed early but must be completed by the block end dates to avoid late penalties.

BLOCK 1:	March 11 - 13
BLOCK 2:	March 18 - 20
BLOCK 3:	March 25 - 27
BLOCK 4:	April 1 - 3
BLOCK 5:	April 8 - 10
BLOCK 6:	April 15 - 17
BLOCK 7:	April 22 – 2
BLOCK 8:	April 29 - 31
Final Deliverables:	Due May 8

Course Agenda

Block	Topic	Notes
1	**NETWORK SECURITY CONCEPTS**	
	CRYPTOGRAPHY BASICS AND BEGINNINGS	Stallings Ch1, Ch3
2	**BLOCK AND STREAM**	
	NIST-adopted—DES, 3DES, AES	Stallings Ch4
	Block and Stream	Stallings Ch6, 7, 8
3	**ASYMMETRIC ENCRYPTION**	
	PKI,key exchanges, digital signatures, Certificates	Stallings CH9, CH10
4	**HASH FUNCTIONS**	
	Message digest, Algorithms	Stallings Ch 11, CH12
	Hash functions	
5	**APPLIED CRYPTOGRAPHY**	
	E-mail, S/Mime, Third Party Trust	Stallings Ch 13, CH16 ,
	TLS /SSL	17, Ch 19
	Securing the host	
	Digital Signatures and secure e-mail	
6	**Network Security**	Stallings CH 18, CH20
	PKI systems and PKCS; SSL vs. TLS	
	Email and User Auth	
7	**Advanced topics**	
	Final Project handout	
8	**Final Project development**	