Course ID/Name: Comp 785 Applied Cryptography (rev 1/24/23)

Semester: Spring 2023

Instructor: Michael Jonas (**office:** room 141. **email:** mcy59@unh.edu)

Time and Location: Tuesday, 5:30 – 8:30pm, room 142

Office Hours: by appointment

Web Presence:

Website: http://stem.unh.edu/mcy59/comp/785

Course Description:

This course aims to give students an overview of cryptographic concepts and methods, a good knowledge of some commonly used cryptographic primitives and protocols, a sound understanding of theory and implementation, as well as limitations and vulnerabilities, and an appreciation of the engineering difficulties involved in employing cryptographic tools to build secure systems. Some programming required. Prerequisite: Open to seniors.

Learning Objectives:

Students should develop understanding of main goals of cryptography and illustrate this with a number of examples of how cryptographic services are integrated into modern systems. Students should be able to describe goals and design principles for and common structures of secret key primitives such as block and stream ciphers and be able to explain how basic public key primitives can be defined based on the difficulty of mathematical problems such as the discrete logarithm problem or factoring and analyze variants of these systems. Students should also understand the roles of hash functions as parts of other cryptographic primitives and protocols and the requirements this places on hash functions.

Textbook:

Primary: *Understanding Cryptography*, Chritof Paar. & Jan Pelzl, Springer, 2010 (ISBN 978-3-642-04100-6)

Software Tools:

Choice of programming languages (C/C++/Java) to implement complex algorithms to do encryption and decryption, hashing, digital signatures, and ways to attack those systems.

Student Work and Class Pedagogies:

Class will include both lectures and hands-on lab activity. Lectures will generally take the form of board presentation with questions and answers, although at times we may break into groups to take on a specific topic. The course is 4 credits for undergraduates and the expectation is a minimum of 3 hours engaged time per week per credit over 16-week semester (for graduate students it is 4 hours per credit).

Lab Work:

Some labs will be guided by the instructor whereas others, students will be given a task to solve in pairs or groups. Most lab work will translate to further assignments where student show individually what they have learned. Homework assignments will be reviewed upon completion and exam reviews will be held.

Homework Assignments:

A total of 4 problem sets are given during the semester covering topics discussed in class as well as requiring further investigation outside of class. All homework is expected to be done individually.

Schedule:

Date	***Class Topics***	***Lab Work (code)***	***Assignment Due***
Jan 24	Class beings: *overview of cryptography*		
Jan 31	Fundamentals: *random number generation* Basic symmetric key encryption: *stream ciphers, one-time pad ciphers, block ciphers* Message integrity: *definition and application, collision resistant hashing, authenticated encryption*		
Feb 7			
Feb 14		Scatter Plot	
Feb 21			Problem Set1
Feb 28		Stream Cipher	
Mar 7			
Mar 14	*Spring Break*		
Mar 21	Public key cryptography: *arithmetic modulo primes and their cryptography, public key encryption, arithmetic modulo composites* Digital Signatures: *definition and application, more signature schemes/applications,* Protocols: *authenticated key exchange & Diffie Hellmann, zero knowledge protocols*	Tri-Stream Cipher	Problem Set2
Mar 28			
Apr 4		3DES key-gen	
Apr 11			Problem Set3
Apr 18		Fermats Primality	
Apr 25			
May 2			Problem Set4
May 16	**Project presentations**		
			Exam *(take-home)*

Grading:

15% Participation[1]
This includes attendance, participation, and preparedness (5 points each)
40% Assignments[2]
There will be 4 problem sets worth 10 points each
20% Project[3]
More details in the first half of class
25% Exam[4]

Policies

Academic Honesty and Collaboration:

Collaboration is encouraged and supported in the classroom through lab activities and outside the classroom as directed by instructor. Note that homework assignments and tests you submit **must be entirely your own work.** Deviation from this policy will result in dismissal from the course.

See the University policy on **Academic Honesty** for more information.

Attendance:

Is mandatory and you will lose on class participation grade for absences. Since work is based off lecture and class activities it becomes difficult to do well with too many absences.

Late Assignments and Make-Up Exams:

Policies for late assignments and make-up exams are very strict and apply only in exceptional cases of student illness, accident, or emergencies that are properly documented. It is your responsibility to make arrangements with instructor before the deadline as soon as you are aware you will miss a deadline, exam or class. Unexcused late assignments are penalized 20% per day.

Use of Electronic Devices in Classroom:

Not allowed during examinations. Absolutely no cell phone use during class time.

Accessibility Services:

The University is committed to providing students with documented disabilities equal access to all university programs and facilities. If you think you have a disability requiring accommodations, you must register with Student Accessibility Services (SAS) office. The Student Accessibility Coordinator at UNHM is Jenessa Zurek (email jenessa.zurek@unh.edu).

Mental Health and Wellness

In partnership with The Mental Health Center of Greater Manchester, UNH Manchester offers free mental health sessions for students. For scheduling a session email unhm.advising@unh.edu.

[1] COMP 885 any lost points subtracted from overall grade
[2] COMP 885 additional 8% (4 problem sets at 12% each)
[3] COMP 885 project additionally worth 4%
[4] COMP 885 exam additionally worth 3%