COMP 655: Cryptography

Bulletin Description

Introduction to the design and analysis of cryptographic algorithms. Topics include basics of abstract algebra and number theory; symmetric and asymmetric encryption algorithms; cryptographic hash functions; message authentication codes; digital signature schemes; elliptic curve algorithms; side-channel attacks; and selected advanced topics.

General Course Info

Term: Fall 2018  
Department: COMP  
Course Number: 655  
Section Number: 001  

Time: 11:15am – 12:30pm on MW indicated on the web page  
Location: FB007  
Website: http://www.cs.unc.edu/~reiter/courses/fall2018/  

Instructor Info

Name: Prof. Michael Reiter  
Office: FB350  
Email: reiter@cs.unc.edu  
Web: http://www.cs.unc.edu/~reiter  
Office Hours: 10-11am on most Tuesdays (check course web page)  

Textbooks and Resources

There is no textbook for this class. The class lectures slides will be posted before class (usually), and some readings will be assigned. There are no plans to use Sakai.

Course Description

Cryptography refers to algorithmic techniques for protecting information from adversaries. While traditional goals of cryptography include preventing unintended disclosure of that information or detecting its unauthorized alteration, the field has grown in the last thirty years to include much richer primitives and protocols. Cryptographic techniques are already the basis for many security mechanisms in common use today, including secure communication protocols (e.g., TLS, IPSec), disk encryption facilities (e.g., Microsoft’s BitLocker), and signed code updates. The use of cryptography will undoubtedly grow in the future, and so an understanding of modern
cryptography is warranted for anyone developing technologies for use in environments where adversaries might be present.

*Cryptography* is a class that will focus on cryptographic primitives that are in common use today, with an emphasis on understanding why they are secure and for what purposes they should be used. To accomplish this, topics will be treated in a rigorous way, with an emphasis on definitions of security properties and, where possible, proofs of why particular constructions achieve those definitions.

**Target Audience**

The target audience for this class is computer science students, primarily upper-level undergraduates and graduate students.

**Prerequisites**

COMP455 (Models of Languages and Computation) and STOR 435 (Introduction to Probability) or their equivalent

**Goals and Key Learning Objectives (subject to change)**

Through this course, students will accumulate familiarity with the following techniques:

- Basics of abstract algebra
- Pseudorandom functions and permutations
- Symmetric encryption algorithms
- Cryptographic hash functions
- Message authentication codes
- Information-theoretic security
- Number theory and number-theoretic primitives
- Asymmetric encryption
- Digital signature schemes
- Elliptic curve algorithms
- Side-channel attacks

Time permitting, the class will also cover more advanced topics, such as

- Interactive proofs and zero-knowledge proofs
- Bilinear maps
- Advanced key management techniques
Course Requirements

The nature of work in this class is primarily in working problems presented through quizzes, homeworks, and exams, and in giving in-class presentations.

Key Dates

Exam dates and assignment due dates are unknown at this time and will be announced as soon as they are known.

Grading Criteria (subject to change, but roughly the following)

25% Homeworks
25% In-class presentation
25% Midterm exam
25% Final exam

Course Policies

Late assignments will not be accepted unless otherwise stipulated.

The course final is given in compliance with UNC final exam regulations and according to the UNC Final Exam calendar.

Honor Code

The degree of collaboration permitted and the resources that should be used will be specified per assignment. However, the default policy is that no collaboration or resources except those specifically provided as part of the class (e.g., class notes and recommended readings) should be used in completing assignments. All work must be your own.

Course Schedule

The course schedule is posted at the course web page and will be updated often. Please check it frequently.

Disclaimer

The professor reserves to right to make changes to the syllabus, including assignment due dates and test dates. These changes will be announced as early as possible.