CSCI 388: Cryptography
Reed College
Handout 1: Course Information

Spring 2023
Department of Computer Science
Instructor: Chanathip Namprempre

Course Information

Instructor: Chanathip Namprempre. Email: `chanathipn at reed edu`.

Lecture periods: MWF 11:00 - 11:50 PHYSIC 240A

Access: The course website is at `https://nchanath.github.io/388-S23/` Please check the syllabus before every class period.

Course description from the course catalog: One-unit semester course. An introduction to modern cryptography. Topics include private- and public-key encryption, message authentication codes, pseudorandomness, and digital signatures. Emphasis is placed on formal definitions of security, proofs of security, and key constructions. Prerequisite: Computer Science 382 or 387 or Mathematics 382, 387, or 332. Lecture-conference. Cross-listed as Mathematics 388.

Resources: The following textbooks are required for this course:

- *Symmetric Cryptography Basics* by Chanathip Namprempre. Thammasat University Press, 2014. ISBN: 978-616-314-090-6. This book is downloadable from the course website.
- *Introduction to Modern Cryptography* by Mihir Bellare and Phillip Rogaway, 2005. This is a draft of a book. It is also downloadable from the course website.
- *A Graduate Course in Applied Cryptography* by Dan Boneh and Victor Shoup, Jan 2020. This is also a draft. It can be downloaded at `https://toc.cryptobook.us/book.pdf`.

Coursework and grading:

- Reading: You are expected to have completed the reading assignment *before* arriving to class. The syllabus indicates the readings to be covered in each day's lecture.
- Problem sets: There will be about 6 problem sets most of which will be assigned in the first half of the course. This portion is worth 20% of the total grade.
- Applications: I will assign 11 application-oriented case studies to be researched throughout the course. Each will be covered by 1-2 people, referred to here as "owners." For each of the case studies, the following will happen.
  - Presentation: The owners will present the research that they have done about the case study. The class as a whole will participate in a discussion about the topic. The goal is to apply what we have learned so far to real problems as much as possible. (The term "apply" here could be either or both theory and practice, depending on the topic.) Your presentation should be well-organized, engaging, correct, and well-thought-out. It should demonstrate that you have put in a reasonable amount of effort to ensure that your audience follows the presentation and that the presentation helps encourage fruitful and engaging discussions. This portion will be worth 15% of the total grade for the owners.
  - Term paper: Toward the end of the course, the owners will submit one term paper on their topic. More details on the term paper below. This portion is worth 25 % of the total grade for the owners.

  - Summary and class participation: Approximately one week after the presentation on the topic, other participants (i.e., non-owners) will submit a one-page summary on the topic. The summaries and the class participation during the entire course are worth a total of 10% of the total grade for the participants.
  - Scribe notes: Two of the participants who are not the owners of the topic will separately submit scribe notes containing the details of the discussions that took place during the class period. (This is a minimum requirement. You can of course add more relevant material to your scribe notes if you so desire.) The scribe notes must follow a logical flow, be written in complete sentences, be written in the author's own words, and be well-typesetted using LaTeX. This portion is worth a total of 10% of your grade.
- Final exam: The final exam will cover all of the material explored during the entire semester. It is worth a total of 20% of your grade.

Other policies:

- Submitting work: All written work will be submitted online using Gradescope.
- Attendance: You need to attend class regularly. Missing in-class activities will greatly impact your performance in the course. If you need to be excused from class, please send me email as soon as possible. Some excuses (such as illness) may require documentation (such as a doctor's note). If you will be missing class for an excusable but predictable reason (say, a religious holiday) you should inform me before the absence. I will not excuse absences after the fact for reasons that were known ahead of time.
- Academic integrity: All work you turn in for this class should be yours and yours alone except for the term paper if you have a partner. You are of course encouraged to discuss the material with other students, but you are not allowed to share your written work with them.

Further Instructions

Term paper: The goal of this assignment is two-fold. One is to explore how solid definitional work and proof techniques can be applied to systems or protocols that are used in practice. The other is to give you a sense of how different kinds of research in modern cryptography are done.

That said, you are not expected to produce novel research results in your term paper as this course is only one semester long and is at an undergraduate level. My expectation is that you explore the topic to the fullest extent possible within this context then write about your findings in a coherent, logical, and well-structured paper.

With this goal in mind, your paper should have at least the following sections:

- Title page. This page contains the title of the paper, your names, the course name, the course code, the instructor's name, and the month and year the paper is submitted.
- Abstract. The abstract should contain the crux of the ideas presented in the paper. It should be precise and covers the main concepts of your paper.
- Introduction. This section "tells the story" about the topic and your findings, if any. The goal is to allow readers who may read only this section to learn about the main ideas in the paper.
- Literature review. This section provides a comprehensive and up-to-date overview of the existing research on the topic.

- Main sections. These sections describe your findings or research results in details. Be sure to structure these sections in such a way that a reader can logically follow the concepts, which often times build on each other.
- Conclusion. This section should provide a clear and concise summary of the main arguments, evidence, or research results presented in the paper, highlighting the most important and relevant points. It should also relate the findings to the broader context of the field and explain the contributions of the study, if any, to the field.
- References. Citations should be provided in the commonly-used formats such as the ACM or IEEE styles. (For real papers, the citation style to be used will depend on the venue in which the papers appear.)

Finally, the paper should be typesetted in LaTeX.