INF 521
Application of Cryptography to Information Security Problems

Class Structure

Instructor - Ranjan Pal
Instructor Email - rpal@usc.edu
Class Standing: Graduate Level (3 Units)
Lectures - Fridays, 12 noon to 2:30 PM in OHE 136
Office Hours - Monday, Wednesday, 3:30 PM to 5 PM
Grader Office Hours - Only after assignment grading (class will be notified by email)

Class Resources

Resources will be posted on the DEN website. The resources include:
1. Lecture notes
2. HW assignments and solutions
3. Additional useful materials

Course Readings

There will be NO standard textbooks for this course. Lectures notes will be combined from various print and web resources. It is SUFFICIENT to focus on the lecture materials, and additional course attachments to perform well. However, the following list consists of additional references for the interested student:

1. Handbook of Applied Cryptography, Menezes et.al.,
2. Invitation to Cryptology, Barr
3. Understanding Cryptography, Paar and Pelzl
4. Applied Cryptography, Schneier
5. Making and Breaking Codes and Applied Cryptography, Garett
7. Cryptography Engineering, Ferguson
8. Cryptanalysis: A Study of Ciphers and their Solutions, Gaines

Course Structure

- The first part (65% - 70%) of the course will cover the concepts and theory of cryptography.
- Second part of the course will focus on applications of cryptography in security domains we experience in our daily lives.
Course Takeaway

At the end of the course, the students will have achieved the following:

1. A strong grasp of the basic concepts underlying cryptography, and the fundamentals.
2. Increased awareness and intuitions about cryptology.
3. Gain the ability to apply appropriate cryptographic techniques to a security engineering (and management) problem at hand.

Nice Things about the Course

- Virtually no programming assignments :)
- Mathematical and engineering problem solving without the need to construct proofs
- Lots of fun and useful concepts to learn
- Lots of applications to study (e.g., ATM machines, Kerberos, Firewalls, cloud security, etc.)
- A balanced course load
- Collaborative learning and discussion with peers
- All math background will be covered as part of course material

Course Grading

- 25% in homeworks (4 HWs - one might have a small programming component).
- 15% in midterms (1 midterm).
- 35% on a final exam.
- 25% in mini quizzes (10-15 minutes quizzes each) at the beginning/middle/end of some lectures.
  - very simple multiple choice questions
  - only on material covered in the previous lecture
  - will choose the top $k$ from the all the quizzes (e.g., 4 out 6)
  - careful reading of the lecture materials should allow you to score very high on these quizzes
- HWs will be graded by graders.
- Quizzes and exams will be graded by the instructor.
- Final letter grade will be given by the instructor.
- Grading method will be relative and on the curve. Thus, getting a 90/100 can result in a B+, also getting a 50/100 can result in an A.
- Midterms and finals grading will include partial credit for showing a proper understanding of a problem.
- The same goes for HWs; however, I will leave it to the grader to chart out his own ways.
- I will hardly give any grade below a B or a B- (apart from special cases when a C grade can be given).
- Grading will be ‘fair’ (in both exams, HWs, and quizzes), so do not ask for special favors.
Course Homework Submission

- Homework submission in class (except for DEN students).
- 2% off every late day. 5% off every late day beyond 3 late days.
- No personal emergencies will be entertained (with the exception of university granted emergencies, in which case official documents need to be shown).
- Grader will arrange regrading sessions for HWs.

Academic Integrity

- You can collaborate with fellows to discuss and clarify concepts lectured in class, and those required to solve homeworks. As a matter of fact, I highly encourage you to study in groups (if possible) to better your own understanding of the subject. However, SOLVE the homework's ON YOUR OWN.
- The instructor is open to all sorts of questions during his office hours, and also via email (if possible to answer by email [with up to a 24 hour lag time])
- Any academic misconduct will be dealt with seriously (50% grade off every HW, and most likely a C grade after observed misconduct in two or more homeworks)

How to Study

- Periodically review lecture material carefully. Remember that the class quizzes form 25% of the grade and they will be quite easy so a periodic review of class material can boost your confidence (via high scoring in the quizzes) in getting a good grade at the end of the course. A periodic study also implies you keep chipping away at the basic concepts and put them to memory for ever, and this is one necessary condition to be able to quickly apply your learnings in the future work place (academia, government, industry, etc.).
- As mentioned before, collaborate with colleagues, and use office hours well to understand concepts better, but write your own answers. Simply copying answers will not help you to answer questions in the midterms and the finals, as they will be based on your understanding of the class material.
- Please try questions on your own first (after discussing concepts with colleagues/instructor). However, do not wait too long if you are stuck on a problem. The ideal thing to do here is to individually think hard for 1 to 2 hours on a difficult problem, and then ask for help/hints from the teaching staff during office hours.
- Advice on performing well in the midterm and the finals will be discussed in class.

BEST OF LUCK!
Course Syllabus (Tentative)

Week 1 and 2 (HW1 out on Week 1)
Course Introduction, Math Background - Elementary Number Theory + Functions, Course Overview

Week 3 and 4 (HW1 due on Week 4, HW2 out on week 4)
Symmetric Encryption Techniques - Classical + Modern, Cryptanalysis

Week 5 and 6
More Math Background - Digging Slightly Deeper into Elementary Number Theory, Non-Symmetric Encryption Techniques - Public Key Cryptography

Week 7 (HW2 due on Week 7, HW3 out)
Wrapping up Public Key Cryptography, Midterm Review

Week 8
MIDTERM examination, Cryptographic Hashing, Message Authentication, Digital Signatures

Week 8 and 9
Cryptographic Hashing, Message Authentication, Digital Signatures (continued)

Week 10
Key Management, Key Distribution, Authentication, Cryptographic Protocols

Week 11 to Last Day of Class [HW3 due on Week 11, HW4 out (due last day)]
Applications of cryptography in the real world
- ATM Machines
- Kerberos
- Email Security
- Software Security
- Cloud Security,
- IP Sec
- Wireless Network Security

FINAL EXAM - 9th December, 11 AM to 1 PM