
Problem Set 1

This problem set is due on *Wednesday, February 13, 2008* by 8AM. You must submit your homework to your edlab CS591d course directory. Make sure that your homework files have proper permissions set such that the course staff can read the files, but not other students. Do not make any modifications to your homework files after the due date, unless you notify the TA that you are using a late pass. You may write your solution in any program (Word, L^AT_EX, etc.), but you must convert your document to PDF for submission. We will accept only PDFs. Please contact the TA well ahead of the deadline if you have a question about these procedures.

This is an individual problem set. See Handout 1 (*Course Information*) for our policy on collaboration and late penalties. Mark the top of each page with your name, cs591d, the problem set number and question, and the date¹. Each solution must begin on a new page. Points may be deducted if your TA has problems understanding your solution. In mathematical problems, **show all your work**.

Problem 1-1. Principles of protection (5 points)

This is an individual problem. The length limit is 1 page, single-spaced, with an 11pt font and 1-inch margins. Text violating these constraints will lose points. We would like you to focus on quality rather than quantity.

Chapter 11, Section A of the Kaashoek and Saltzer POCS book discusses principles for secure system design. In Appendix C of the chapter (pages 131–156), you will find a large number of revealing and entertaining war stories on security system failures. Select one of the stories, and write an essay discussing (1) the design principle(s) that were violated, (2) an appropriate short-term response for redesign, and (3) an appropriate longer-term response for redesign.

Estimated time: 2 hours

¹We will distribute our favorite solution for each problem to the class as the “official” solution – this is your chance to become famous!

Problem 1-2. Number theory (5 points)

This is an individual problem. In these problems, we review number theory introduced by other classes. We also peek at future topics in this course in order to prepare you for the magic of public key cryptography.

(a) Modular arithmetic (2 points)

Do the following two problems. **Make sure to show all your work.** Problem (i) should reintroduce you to modular arithmetic, while problem (ii) gives you a flavor of key density in a precursor to public key cryptography.

i Evaluate the following and show all your work:

(a) $7582 \bmod 93$, (b) $(-7582) \bmod 93$, (c) $93 \bmod 7582$, (d) $(-93) \bmod 7582$

ii Determine the number of keys in an Affine Cipher over \mathbb{Z}_m for $m = 42, 484$, and 7875 .

Estimated time: 1-2 hours

For extra credit (1 point each), do problems 1.8, and 1.9 from Stinson. Problems 1.8 and 1.9 will become more relevant as we learn how key generation algorithms work in such cryptosystems as RSA.

(b) Experience the magic of modular exponentiation (3 points)

When computing a modular exponentiation such as $a^b \bmod m$, we can optimize by first reducing the exponent by $\phi(m)$. Theorem 1.2 in Stinson explains the formula for $\phi(m)$. In the vernacular, we can say that “downstairs” the operations are mod m while “upstairs” the operations are mod $\phi(m)$. Using this technique, compute the 2 rightmost decimal digits of 1234^{562} . Show all your work. Hint: You shouldn’t need a calculator for this.

Estimated time: 0-2 hours

Problem 1-3. Administration (0 points)

Please tell us approximately how many hours you spent on each problem set question. If any problem took more than two hours, please explain why.