
Problem Set 5

This problem set is due on *Friday, May 2, 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 problem set has both individual and group components. 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 date. 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**.

Each team member should turn in the individual problem on his or her own. For the group problems, have your team submit a *single solution*.

Problem 5-1. E-voting (2 pts)

Prof. Ron Rivest discussed several reasons why electronic voting is hard. List the six problems Prof. Rivest described for electronic voting. Explain each problem with one sentence, and then explain in detail why achieving voter privacy is extremely difficult by citing evidence from Prof. Rivest's lecture. Limit your answer to one page.

Problem 5-2. Three may keep a secret if two of them are dead (4 pts)¹

This is a group problem. Divide up the work amongst your team in an efficient manner. But **all** team members must contribute in some way. Each team member should list exactly what role you played. A couple sentences per team member is sufficient. If you receive any key insights from another person or resource, cite that person or resource.

(a) (t, w) -threshold secret sharing

Do problem 13.1 on page 514.

(b) Defective shares

Do problem 13.2 on page 514.

¹Benjamin Franklin, circa 1735

Problem 5-3. Multicast security (4 pts)

This is an individual problem. As customary, if you receive any key insights from someone else or some other resource, you must cite that person or resource. State the names of people you consulted and the knowledge you learned from each.

Do problem 14.5 in Stinson, pages 553–554

Although this problem is an **individual problem**, you may reuse code from the group work in the earlier problem if you properly cite each group member who contributed to the code. You may not share code for this problem.

This problem set is available in PDF on the class Web site. To avoid typos, we suggest you cut and paste these values:

$$p = 469197492537813978579427$$

$$q = 260665255385551$$

$$\alpha = 216009506684688951924147$$

User U_i receives $(x_i, y_i) = (122, 202688224274771)$

The blinded shares are:

$$(22, 44911778774799764175082)$$

$$(33, 436697642377597599529623)$$

$$(55, 423139372565945781217729)$$

$$(66, 130453044766194153200365)$$

$$(88, 9228050882659713297588)$$

The special blinded random number $\gamma = 239688503750480728519031$.