
Problem Set 1

This problem set is due on *Monday, September 20, 2010* by 8AM. You must submit your homework via SPARK¹. You may write your solution in any program (plaintext, Word, L^AT_EX, etc.), but you must either (A) convert your document to PDF for attachment in SPARK or (B) use the textbox dialog box in SPARK to submit a plaintext response. While you may write your solution in any format for your own use, we will not accept attachments other than PDFs in SPARK. 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. When appropriate, mark the top of each page with your name, cs466, the problem set number and question, and the date². Please begin each solution 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. 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 .

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 $3^{40000005}$. **Show all your work.** Hint: You shouldn’t need a calculator for this.

¹<http://spark.oit.umass.edu>

²We will distribute our favorite solution for each problem to the class as the “official” solution—this is your chance to become famous!