

CSCI-E2 BITS - Problem Set 3 (60 points total)
Due March 24th 2011 at Noon

Question 1 (10 points)

What is :

- a. (2 points) $22 \bmod 3$
- b. (2 points) $39 \bmod 8$
- c. (2 points) $67 \bmod 11$
- d. (2 points) $70 \bmod 5$
- e. (2 points) $93 \bmod 16$

Question 2 (16 points)

This question is about efficiently computing modular arithmetic.

- a. (4 points) What is the minimum number of multiplications required to compute $7^{41} \bmod 9$?
- b. (6 points) Compute $7^{41} \bmod 9$ using the repeated squares method. Show your work.
- c. (2 points) Besides requiring fewer multiplications, what is the advantage of computing modulo operations at each step?
- d. (4 points) Let's now think generally about the number of multiplications required in modular arithmetic. Suppose we need to compute $q^a \pmod{p}$. Exactly how many multiplications are required? (*Hint: state your answer in terms of the binary representation of a . Try $a=8$ and $a=10$ as well as $a=35$ and see if you can find the pattern.*)

Question 3 (20 points)

Suppose you want to set up a shared key with your friend Bob. You decide to use the Diffie-Hellman key exchange protocol and agree in advance that $g=17$, and $p=13$. Suppose you select your "private" key to be 11.

- a. (4 points) What is your "Public" key?
- b. (4 points) Suppose Bob's "Public" key is 8. What is your "shared key"?
- c. (6 points) Find Bob's secret key by brute force, exhaustive search.
- d. (4 points) Show that Bob gets the same shared key when he does the computation.
- e. (2 points) Why does Diffie-Hellman use modular arithmetic rather than ordinary arithmetic?

Question 4 (14 points)

Attached is an actual page from the Code of Federal Regulations specifying when health records have been sufficiently stripped of identifying information that the data can be made public.

- a. (6 points) Regardless of whether these standards are adequate to protect privacy, why should such information EVER be made public?
- b. (8 points) These standards were subsequently deemed inadequate. Do a little research and explain why.