CSE 235 Homework 05 Fall 2007

Due 1:30PM, Wednesday, November 28th, 2007

Name/CSE Login _____

Name/CSE Login _____

Instructions Follow instructions *carefully*, failure to do so may result in points being deducted. Clearly label each problem and submit the answers *in order*. It is highly recommended that you typeset your homework using LaTeX or a similar typesetting system. Staple this cover page to the front of a hardcopy of your assignment for easier grading. Late submissions *will not be accepted*. Be sure to show sufficient work to justify your answer(s). If you are asked to prove something, you must give as formal, rigorous, and complete proof as possible. You are to work individually, and all work should be your own. The CSE academic dishonesty policy is in effect (see `http://www.cse.unl.edu/undergrads/academic_integrity.php`).

Partner Policy You may work in pairs, but you must follow these guidelines:

1. You must work on *all* problems *together*. You may not simply partition the work between you.
2. You must use LaTeX and you may divide the typing duties however you wish.
3. You may not discuss problems with other groups or individuals.
4. Hand in only one hard copy under the first author's name.

Problem	Points	Score
A	5	
B	5	
C	5	
D	5	
3.4.6	5	
3.4.24	5	
3.4.28	5	
3.6.24ef	5	
3.7.20	5	
4.1.6	5	
4.1.20	5	
4.1.32	5	
Program		
Correctness	25	
Style/Doc	15	
Total	100	

Topics: Number Theory & applications (3.4–3.7), Induction (4.1–4.2).

Comments: on 3.6.24, use the Extended Euclidean algorithm and find s, t.

Problem A

Bob wants to send a short 40-byte reply message to Alice using her 256-bit (n) RSA protocol. Bob doesn't fully understand RSA and so treats the 40-byte ASCII text as a single number x and encrypts it using Alice's public key, $e_K(x)$. Alice later says that Bob's message was garbage. Why didn't it work?

Problem B Dumbbell weight sets are available in packages of n pairs starting at 5 lbs with weights increasing in 5lbs increments. What is the total weight of a dumbbell set in terms of n?

Problem C Consider the following algorithm to compute a^n. Does it run in polynomial-time? Why or

```
product = 1;
for i = 1, ..., n - 1 do
    product = product × a;
end
return product;
```

why not?

Problem D Let $f(x) = x^r$. Could we use induction to show that $\forall r \in \mathbb{R}$,

$$f'(x) = rx^{r-1}$$

Why or why not?

Programming Assignment

Your programming assignment will be to break an RSA cryptosystem. Specifically, you must decrypt a cipher text (available on the web page) that has been encrypted by an RSA cryptosystem with the following public-key components:

$$\begin{aligned} n &= 151195179798994573461212346876799067599400 63 \\ a &= 187458734148965351970172647934141597409 57 \end{aligned}$$

Note that breaking this system is *feasible* since n is a 144-bit number (a product of two 72-bit primes).

A plain text (ASCII) file was encrypted using this system as follows. A block of 16 ASCII characters (16 bytes) was read in and treated as a 128-bit number x. This number was then encrypted using the public key above.

$$e_K(x) = x^a \bmod n$$

resulting in another number y. This number was then converted to a hexadecimal representation (for compactness) and each was output on a single line in the cipher file. Note that the resulting number is (bound by) 144 bits given the modulus above. Your job is to break the given RSA protocol and decrypt the message.

You may use any language or computer tools that you wish. You will handin all the source files of the tools you developed in this exercise along with relevant readme files describing how to compile/use the tools to verify that you successfully broke the encryption. Of course, you will also handin the decrypted plaintext file.

Along with the hard copy of your homework, you should provide a short write-up about how you broke this system. Include a discussion about the algorithms/procedures/tools you used to do it. Be sure to properly cite any extra tools that you used and discuss the techniques used to break the cipher. The point of the write up is to develop your technical writing skills. Several resources are available on the web page to help you with this.