CS70 Discrete Mathematics for Computer Science, Fall 2011

Section 4

1. In the RSA encryption algorithm let $p = 3$, $q = 5$ and $e = 7$.

(a) What is the public key?

(b) What is the private key?

(c) Encrypt the message $x = 3$.

(d) Decrypt the message $y = 10$.

2. Suppose n is a positive natural number whose prime factorization is: $n = p_1^{a_1} p_2^{a_2} \dots p_k^{a_k}$, where $p_1 \dots p_k$ are natural, distinct prime numbers, and $a_1, \dots a_n$ are positive natural numbers. Use induction to show that the number of divisors of n is $(1 + a_1)(1 + a_2) \cdots (1 + a_k)$. Example: $n = 12 = 2^2 \times 3$ has exactly $3 \times 2 = 6$ divisors.

3. Let $a \in \mathbb{N}$ be a natural number, and define the *sign* of a to be the quantity formed by alternatively adding and subtracting the digits of a. For example, if $a = 39250$ then the sign of a is $3 - 9 + 2 - 5 + 0 = -9$. Prove that a is divisible by 11 if and only if its sign is divisible by 11.

4. SBNs Books were, until 2007, identified by an **International Standard Book Number (ISBN)**, a 10-digit code $x_1 x_2 \dots x_{10}$ assigned by the publisher. These 10 digits consist of blocks identifying the language, the publisher, the number assigned to the book by its publishing company, and finally, the last digit is a "check digit" that is either a digit or the letter X (used to represent the number 10). This check digit is selected so that $\sum_{i=1}^{10} i \cdot x_i \equiv 0 \pmod{11}$.

(a) The ISBN for the original 1970 *Anarchist's Cookbook* starts with "0-9623032-0-". The dashes in ISBN are meaningless — they're only inserted for readability. What is the last digit?

(b) Wikipedia says that you can get the check digit by computing $\sum_{i=1}^{9} i \cdot x_i \mod 11$. Show that Wikipedia's description is equivalent to the above description.

(c) Prove that changing any single digit of the ISBN will render the ISBN invalid. That is, the check digit allows you to *detect* a single-digit substitution error.

(d) Can you *switch* any two digits in an ISBN and still have it be a valid ISBN? (E.g., could both 01**2**34**5**678X and 01**5**34**2**678X both be valid ISBNs?

(e) Canada decides to change its ISBN system by doing the check digit computation modulo 12 rather than modulo 11 (if the check digit needs to be "11", they'll use "Y"). That is, the digits now have to satisfy $\sum_{i=1}^{10} i \cdot x_i \equiv 0 \pmod{11}$. Shall we blame Canada for reducing the error-detecting capabilities of the check digit?

5. [Sharing a Password]

A certain course has one professor and three GSIs on its staff. The staff want to password-protect the software that lets them alter student midterm grades. To prevent malicious tinkering, they don't want to allow anyone to access the system alone. Instead, they would like it so that the system can be entered only with the consent of either (1) the professor and any one GSI, or (2) all three GSIs together. Suppose the password is some message m, and let p be a prime.

Consider the following scheme:

Generate two numbers s_1 and s_2 at random and choose s_3 such that $s_1 + s_2 + s_3 \equiv m \pmod{p}$. Let $t_1 = s_2 + s_3, t_2 = s_1 + s_3$, and $t_3 = s_1 + s_2$. Give s_1 to the first GSI, s_2 to the second GSI, and s_3 to the third GSI. Finally, give t_1, t_2 and t_3 to the professor. If the three GSIs want to compute the password, they can pool their information to compute $s_1 + s_2 + s_3 \equiv m \pmod{p}$. If a GSI and the professor want to comptue the password, they can compute $s_i + t_i \equiv m \pmod{p}$.

(a) Is this a valid solution? Why or why not?

(b) Modify the above scheme to make it more secure.