Cryptography cs 4995
Instructor: Prof. Michael Rabin

Problem Set 1

Due: Tuesday, Jan. 30 2007

1. **(Addition of large integers.)** Consider a computer which has the following primitive operations on integers in the range $[0, 2^{64})$ (we will refer to the variables storing such integers as *words*):

   - Addition. Given two words a, b, evaluation of $a+b$ returns the result $a+b \bmod 2^{64}$ and also sets a *carry bit* to 1 if $a + b \geq 2^{64}$ (the carry bit remains 0 otherwise).
   - Bitwise shifting of a word (right or left).

   A very large integer (say an integer of 10,000 binary digits) can be represented with k words. Discuss how to implement addition and subtraction of large integers represented in this way. Give the running time of your algorithm (in terms of primitive operations) as a function of the integer lengths.

2. **(Extended gcd computation.)** In class, we showed am algorithm to compute $\gcd(a, b)$ for positive integers a, b. A useful number-theoretic fact is that for any positive integers a, b there exist integers X, Y (not necessarily positive) such that $Xa + Yb = \gcd(a, b)$. Extend the gcd algorithm so that in addition to computing $\gcd(a, b)$, the algorithm also outputs X, Y with this property.

3. **(Number theory.)** Without using a computer, calculate $102^{4,800,000,023} \bmod 35$. Hint: The really fast way uses Chinese remaindering.

4. **(The meaning of Aha!)** An evil dictator has access to a nuclear device which can only be set off using a 64-bit password K. The dictator has 56 not-so-trusted generals, conveniently named $g_{1,1}, \ldots, g_{1,8}, g_{2,1}, \ldots, g_{2,8}, \ldots, g_{7,8}$. In the mornings, the dictator likes to arrange his generals in a rectangle as follows:

$$\begin{array}{cccc} g_{1,1} & g_{1,2} & \cdots & g_{1,8} \\ g_{2,1} & \ddots & & g_{2,8} \\ \vdots & & & \vdots \\ g_{7,1} & g_{7,2} & \cdots & g_{7,8} \end{array}$$

   The dictator wants to share K among the generals so they can set off the nuclear device in case of the dictator's death. However, since he does not completely trust the generals, he wants to share K according to the following rules (where G represents a group of generals):

   (a) If G contains all generals in any row of the above arrangement, or contains all generals in any column of the above arrangement, then the generals in G should be able to reconstruct K. (For example, generals $g_{3,1}, g_{3,2}, \ldots, g_{3,8}$ should be able to reconstruct K, as should generals $g_{1,5}, g_{2,5}, \ldots, g_{7,5}$.)

(b) If G does *not* contain all generals in any row or all generals in any column, then the generals in G should have *no information* about K. (For example, the group consisting of all generals *except* $g_{1,1}, g_{2,2}, \ldots, g_{7,7}, g_{7,8}$ should have no idea what K is.)

Suggest a scheme for the dictator to distribute K. Prove the correctness of your scheme. This problem is somewhat challenging. But when you find the solution you will exclaim: Aha!

5. Google Challenge: Using only a straight edge, draw a line segment which divides the figure below into two figures of equal area. The line segment should be contained entirely in the figure.