Cryptographic Engineering
Assignment 4, Monday, May 22, 2017

Handing in your answers: Submission via Blackboard (`http://blackboard.ru.nl`)

Deadline: Monday, June 12, 2017, 23:59 (UTC+2)

1. In this exercise, consider integers modulo $2^{221} - 3$ in radix-2^{16} unsigned representation. (**Hint:** You make your life much easier if you use redundant representation and use `int64_t` to represent the limbs)

   (a) Implement schoolbook or product-scanning multiplication of two such big integers (without modular reduction) in C. Write a unit test for this multiplication (hint: use the same approach of output that, piped through a command-line calculator like bc, produces 0 if multiplication is correct).

   (b) Implement Karatsuba multiplication (only one level, no recursive application of Karatsuba) of two such big integers (without modular reduction) in C. Use the unit test of the previous part to test that it's correct.

   (c) Implement refined Karatsuba multiplication of two such big integers (without modular reduction) in C. Use the unit test of the first part to test that it's correct.

   (d) Implement modular reduction after multiplication and implement a unit test to make sure that the result is correct.

   (e) Implement a carry routine after modular multiplication. Make sure that all coefficients of the result of a modular multiplication have only up to 17 bits, if the coefficients of both of the inputs have up to 20 bits. Extend your unit test to check for this output condition.
   Note: Neither part (d) nor (e) require you to reduce to a unique representation.