Cryptography

Priv.-Doz. Dr. Adrian Spalka, Konstantin Ziegler

Assignment 8: Primality testing and factoring

Due: Monday, 10 January 2011, 10^{00}

Exercise 8.1 (Miller-Rabin)**.** (6 points)

(i) Implement the Miller-Rabin primality test and determine primes of several sizes to make an estimate on the implicit constant of the runtime.

(ii) Run the Miller-Rabin primality test with $t = 5$ iterations for $n = 50$-bit numbers. On average, which ratio of the "probably prime" numbers is composite? How does this change by increasing t?

Exercise 8.2 (primality testing with Fermat's Little Theorem)**.** (6 points)

(i) Determine the 10 smallest Carmichael numbers.

(ii) For how many integers smaller than 1 000 000 is 2 a Fermat liar? How many integers smaller than 1 000 000 are primes?

Exercise 8.3 (Fermat's factorization)**.** (6 points) If the Fermat test detects a composite number, you might be interested in computing its factorization. Implement Fermat's factorization (also called "congruent squares method") and also implement factoring by trial division. Provide examples for composite numbers, where one method clearly beats the other. In which situation would you pick which method? Try and formulate general criteria.

Exercise 8.4 (ISBN)**.** (+2 points) Determine the missing digits (marked by x) of the following ISBN.

$$0 - 201 - 07981 - x, 0 - 8053 - x340 - 2, 0 - 19 - 8x3171 - 0$$