Cryptography, homework sheet 2

Due for 2MMC10: 21 September 2017, 10:45

and for Mastermath: 12 Ocotber November 2017, 10:45 by email to `crypto.course@tue.nl`

Team up in groups of two or three to hand in your homework. We do not have capacity to correct all homeworks individually. Do not email Tanja your homework or put homework in mailboxes.

You may use computer algebra systems such as mathematica, gp, or sage or program in C, Java, or Python. Please submit your code if any) as part of your homework. If you do, make sure that your programs compile and run correctly; my students will not debug your programs. The program should also be humanly readable.

1. Use Pollard's rho method for factorization to find a factor of 27887. Use starting point $x_0 = 17$, iteration function $x_{i+1} = x_i^2 + 1$ and Floyd's cycle finding method, i.e. compute $\gcd(x_{2i} - x_i, 27887)$ until a non-trivial gcd is found. Make sure to document the intermediate steps.

2. Use the $p - 1$ method to factor 27887 with basis $a = 2$ and exponent $s = \text{lcm}\{1, 2, 3, 4, 5, \ldots, 11\}$.

3. Use Dixon's factorization method to factor
   the number $n = 403$ using $a_1 = 22$.

4. Perform one round of the Fermat test with base
   $a = 2$ to test whether 31 is prime.
   What is the answer of the Fermat test?

5. Perform one round of the Miller-Rabin test with base
   $a = 2$ to test whether 31 is prime.
   What is the answer of the Miller-Rabin test?

6. Read up on Pocklington's test.