Cryptography, homework sheet 2

Due for 2MMC10: 17 September 2020, 10:45 by email to `crypto.course@tue.nl`
and for Mastermath: 01 October 2020, 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.
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; the TAs will not debug your programs. The program should also be humanly readable.
You do not need to document intermediate results of exponentiations or modular inversion. However, you should include all intermediate results of the algorithms that constitute a step.

1. 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?

2. Use the Pocklington test to prove that 157 is prime. You may use that 13 is prime.

3. 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 in a table as shown in the lecture, i.e., do the gcd computations after each step. Watch out which gcds you're allowed to compute.

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

5. Use Dixon's factorization method to factor
   the number $n = 403$ using $a_1 = 22$.
   Note: This lists all the bases you need.