Cryptography I, homework sheet 13

Due: 9 January 2014, 10:45

Please submit your homework electronically; the TAs do not want to receive homework on paper. Please bundle your scans into one pdf file. Team up in groups of two or three to hand in your homework. We do not have capacity to correct all homeworks individually. To submit your homework, email it to `crypto13@tue.nl`.
In general, you may use computer algebra systems such as mathematica and sage; please submit your code as part of your homework if you end up using a system. Accepted systems/languages: Sage, mathematica, matlab, Pari-GP, Java.
The last two exercises on this sheet require use of a computer.

Before the exam please train yourself in doing moduluar arithmetic. Better calculators are programmabge and is useful for you to teach it to do arithmetic modulo numbers; also XGCD is a useful program to implement. Do this before the exam. Of course you can also print and bring huge multiplication tables and hope that I use those numbers. My exercises will not assume that you have polynomial arithmetic.

1. Let $n = 263$. Run the Fermat test for $k = 3$ with $a = 2, 3$, and 5.
2. Let $n = 263$. Run the Miller-Rabin test for $k = 3$ with $a = 2, 3$, and 5.
3. Factor $n = 110545695839248001$ using the Pollard rho method with $a_0 = 1$ and $c = 1$.
4. Factor $n = 53098980256925153592047$ using the $p - 1$ method with $B = 128$ and $a = 2$.