Cryptography I, homework sheet 12

Due: 8 January 2015, 10:45

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 `crypto14@tue.nl` or place it on the lecturer's table before the lecture. Do not email Tanja or put homework in mailboxes.

This is a good moment to figure out how your pocket calculator can do computations modulo biggish primes.

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 $a = 2$.

The $p-1$ method uses that modulo a prime p we have $a^{p-1} \equiv 1 \bmod p$, so taking some a to a large power s modulo n we can hope that $a^s \equiv 1 \bmod p$ but not $a^s \equiv 1 \bmod n$, so that $\gcd(a^s - 1, n)$ is non-trivial and divisible by p. This happens if the order of a modulo p divides s but there is another factor q in n for which $a^s \not\equiv 1 \bmod q$. A common choice is to take $s = \operatorname{lcm}(2, 3, 4, 5, 6, 7, 8, \ldots, B)$ so s is a very smooth number (divisible by a lot of small primes). If $p-1$ itself is a divisor of s, which requires $p-1$ to be smooth, then $a^s \equiv 1 \bmod p$; it is actually enough if only the order of a modulo p is a divisor of s to get this behavior.

This means the steps in the $p-1$ method are to compute s given B (or in general to select B appropriately), then to compute $c = a^s \bmod n$ and finally to compute $\gcd(c - 1, n)$.