Cryptography, homework sheet 2

Due for 2MMC10: 19 September 2019, 10:45

and for Mastermath: 03 Ocotber 2019, 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. 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. The 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.

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

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

Just because some people might not have seen XGCD as an algorithm, here is a description of XGCD. This description assumes that the input elements f, g live in some ring R in which the greatest common divisor is defined. We will usually use the XGCD on integers or polynomials. If the inputs are integers you can ignore the part the leading coefficient.

Algorithm 1 (Extended Euclidean algorithm)
IN: $f, g \in R$
OUT: $d, u, v \in R$ *with* $d = uf + vg$

1. $a \leftarrow [f, 1, 0]$
2. $b \leftarrow [g, 0, 1]$
3. `repeat`
   (a) $c \leftarrow a - (a[1] \operatorname{div} b[1])b$
   (b) $a \leftarrow b$
   (c) $b \leftarrow c$

   `while` $b[1] \neq 0$
4. $l \leftarrow LC(a[1])$, $a \leftarrow a/l$ */*LC = leading coefficient, this only applies to polynomials*/*
5. $d \leftarrow a[1]$, $u \leftarrow a[2]$, $v \leftarrow a[3]$
6. `return` d, u, v

In this algorithm, div denotes division with remainder. The first component of c is thus easier written as $c[1] \leftarrow a[1] \bmod b[1]$ but by operating on the whole vector we get to update the values leading to u and v, too. At each step we have

$$a[1] = a[2]f + a[3]g \text{ and } b[1] = b[2]f + b[3]g.$$

To see this, note that this holds trivially for the initial conditions. If it holds for both a and b then also for c since it computes a linear relation of both vectors. So each update maintains the relation and eventually when $b[1] = 0$, we have that $a[1]$ holds the previous remainder, which is the gcd of f and g. If the inputs are polynomials, at the end the gcd is made monic by dividing by the leading coefficient $LC(a[1])$.

Example 2 *Let* $R = \mathbb{R}[x]$ *and* $f(x) = x^5 + 3x^3 - x^2 - 4x + 1$, $g(x) = x^4 - 8x^3 + 8x^2 + 8x - 9$. *So at first we have* $a = [f, 1, 0], b = [g, 0, 1]$.

We have $(a[1] \operatorname{div} b[1]) = x + 8$ *and so end the first round with*

$$\begin{aligned} a &= [g, 0, 1], \\ b &= [59x^3 - 73x^2 - 59x + 73, 1, -x - 8]. \end{aligned}$$

Indeed $b[1] = f(x) + (-x - 8)g(x)$.

With these new values we have $(a[1] \operatorname{div} b[1]) = 1/59x - 399/3481$ *and so the second round ends with*

$$\begin{aligned} a &= [59x^3 - 73x^2 - 59x + 73, 1, -x - 8], \\ b &= [2202/3481x^2 - 2202/3481, -1/59x + 399/3481, 1/59x^2 + 73/3481x + 289/3481]. \end{aligned}$$

In the third round we have $(a[1] \operatorname{div} b[1]) = 205379/2202x - 254113/2202$ *and obtain*

$$\begin{aligned} a &= [2202/3481x^2 - 2202/3481, -1/59x + 399/3481, 1/59x^2 + 73/3481x + 289/3481], \\ b &= [0, 3481/2202x^2 - 13924/1101x + 10443/734, -3481/2202x^3 - 6962/1101x + 3481/2202]. \end{aligned}$$

Since $b[1] = 0$ *the loop terminates. We have* $LC(a[1]) = 2202/3481$ *and thus normalize to*

$$a = [x^2 - 1, -59/2202x + 133/734, 59/2202x^2 + 73/2202x + 289/2202].$$

We check that indeed

$$\begin{aligned} x^2 - 1 = &(-59/2202x + 133/734)(x^5 + 3x^3 - x^2 - 4x + 1) + \\ &(59/2202x^2 + 73/2202x + 289/2202)(x^4 - 8x^3 + 8x^2 + 8x - 9). \end{aligned}$$