Cryptography I, homework sheet 2
Due: 25 September 2010, 10:45

Attention: one-line answers using a computer algebra system do *not* count. But it is a good moment to familiarize yourself with some system(s) so that you know how to solve similar problems for real life examples and to verify your answers. You may use a computer algebra system to compute subresults, such as f div g.

1. Compute the extended gcd of $f(x) = x^5 + 3x^3 + x^2 + 2x + 1$ and $g(x) = x^4 - 5x^3 - 5x^2 - 5x - 6$ in $\mathbb{Q}[x]$ using Algorithm 1.

2. This exercise is about m-RSA: Why is n an integer? Why does the system work? Show how to obtain the secret key corresponding to the target pubic key $(118, 857)$.

3. The integer $p = 1009$ is prime. You are the eavesdropper and know that Alice and Bob use the Diffie-Hellman key-exchange in a cyclic subgroup of $(\mathbb{Z}/p, +)$ with generator $g = 123$. You observe $h_a = 234$ and $h_b = 456$. What is the shared key of Alice and Bob?

The rest is for your entertainment:
Here is one version of the extended Euclidean (XGCD) algorithm. Feel free to use any one that you are more familiar with, but if you have never see it, use this one. 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.

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

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

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