Cryptography, winter 2013/2014

PROF. DR. JOACHIM VON ZUR GATHEN, DR. DANIEL LOEBENBERGER

1. Exercise sheet
Hand in solutions until Saturday, 02 November 2013, 23:59:59

Reminder.

- For the course we remind you of the following dates:
  - Lectures: Monday and Thursday 13:00h-14:30h **sharp**, b-it bitmax.
  - Tutorial: Monday 14:45h-16:15h, b-it bitmax.
- A word on the exercises. They are important. Of course, you know that. In order to be admitted to the exam it is necessary that you earned at least 50% of the credits. You need 50% of the marks on the final exam to pass the course. If you do, then as an additional motivation, you will get a bonus for the final exam if you attended the tutorial regularly **and** earned more than 70% or even more than 90% of the credits.

Exercise 1.1 (The Extended Euclidean Algorithm). (8 points)

Integers: We can add, subtract and multiply them. And there is a division with remainder: Given any $a, b \in \mathbb{Z}$ with $b \neq 0$ there is a quotient $q \in \mathbb{Z}$ and a remainder $r \in \mathbb{Z}$ such that $a = q \cdot b + r$ and $0 \leq r < |b|$. (We write $a \operatorname{quo} b := q$, $a \operatorname{rem} b := r \in \mathbb{Z}$. If we want to calculate with the remainder in its natural domain we write $a \bmod b := r \in \mathbb{Z}_b$.) Using that we give an answer to the problem to find $s, t, d \in \mathbb{Z}$ with $sa + tb = d$ and $d = \gcd(a, b)$.

We start with one example: Consider $a = 35 \in \mathbb{Z}$ and $b = 22 \in \mathbb{Z}$. Our aim is to find $s, t \in \mathbb{Z}$ such that $sa + tb$ is positive and as small as possible. By taking $s_0 = 1$ and $t_0 = 0$ we get $s_0 a + t_0 b = a$ (identity_0) and by taking $s_1 = 0$ and $t_1 = 1$ we get $s_1 a + t_1 b = b$ (identity_1). Given that we can combine the two identities with a smaller outcome if we use $a = q_1 b + r_2$ with r smaller than b (in a suitable sense); namely we form $1(\text{identity}_0) - q_1(\text{identity}_1)$ and obtain

$$\underbrace{(s_0 - q_1 s_1)}_{=:s_2} a + \underbrace{(t_0 - q_1 t_1)}_{=:t_2} b = \underbrace{a - q_1 b}_{=r_2}.$$

We arrange this in a table and continue with identity_1 and the newly found identity_2 until we obtain 0. This might be one step more than you think necessary, but the last identity is very easy to check and so gives us a cross-check of the entire calculation. For the example we obtain:

i	r_i	q_i	s_i	t_i	comment
0	$a = 35$		1	0	$1a + 0b = 35$
1	$b = 22$	1	0	1	$0a + 1b = 22, 35 = 1 \cdot 22 + 13$
2	13	1	1	-1	$1a - 1b = 13, 22 = 1 \cdot 13 + 9$
3	9	1	-1	2	$-1a + 2b = 9, 13 = 1 \cdot 9 + 4$
4	4	2	2	-3	$2a - 3b = 4, 9 = 2 \cdot 4 + 1$
5	**1**	4	**-5**	**8**	$-5a + 8b = 1, 4 = 4 \cdot 1 + 0$
6	0		22	-35	$22a - 35b = 0,$ DONE, check ok!

We read off (marked in blue) that $1 = -5a + 8b$ and the greatest common divisor $\gcd(a, b)$ of a and b is 1. This implies that $8 \cdot 22 = 1$ in $\mathbb{Z}_{35}$, in other words: the multiplicative inverse of 22, often denoted 22^{-1} or $\frac{1}{22}$, in $\mathbb{Z}_{35}$, the set of integers modulo 35 is 8. (Brute force is no solution! That is, guessing or trying all possibilities is not allowed here!)

$\boxed{2}$ (i) Find $s, t, d \in \mathbb{Z}$ such that $s \cdot 14 + t \cdot 36 = d = \gcd(14, 36)$.

$\boxed{2}$ (ii) Find an integer $s \in \mathbb{Z}$ such that $s \cdot 17 = 1$ in $\mathbb{Z}_{35}$.

Actually, there are other things which can be added, subtracted, multiplied, and allow a division with remainder. A concrete example is the set $\mathbb{Z}_2[X]$ of univariate polynomials with coefficients in $\mathbb{Z}_2$. (The elements of $\mathbb{Z}_2$ are 0 and 1, addition and multiplication are modulo 2, so $1 + 1 = 0$. The expression $1 + X + X^3 + X^4 + X^8$ is a typical polynomial with coefficients in $\mathbb{Z}_2$; note that the coefficients know that '$1 + 1 = 0$' where they live. It's square is $1 + X^2 + X^6 + X^8 + X^{16}$, any occurrence of $1 + 1$ during squaring yields 0.)

$\boxed{4}$ (iii) Find $s, t \in \mathbb{Z}_2[X]$ such that $s \cdot (1 + X) + t \cdot (1 + X + X^3 + X^4 + X^8) = 1$.

Exercise 1.2. (2 points)

$\boxed{2}$ Let $m \in \mathbb{N}_{\geq 1}$ be a positive integer. Show that the set

$$\mathbb{Z}_m^\times = \{a \in \mathbb{Z}_m \mid \gcd(a, m) = 1\}$$

with multiplication modulo m is a group.

Exercise 1.3 (Diffie Hellman key exchange). (6+1 points)

Perform a toy example of a Diffie Hellman key exchange. Fix $p = 47$ and $g = 2 \in G = \mathbb{Z}_p^\times$. For all the exponentiations use the repeated squaring algorithm from the lecture.

2 (i) Show that the order of g is 23, i.e. $g^{23} = 1$ but $g^k \neq 1$ for $1 \leq k < 23$.
[If you are clever then you only need to calculate g^{23}.] +1

(ii) Take $x = 7 \in G$ and calculate $h_A := g^x$. 1

(iii) Take $y = 8 \in G$ and calculate $h_B := g^y$. 1

(iv) Now compute h_B^x and h_A^y and compare. 2