# Advanced Cryptography: Algorithmic Cryptanalysis

DANIEL LOEBENBERGER, KONSTANTIN ZIEGLER

## 9. Exercise sheet
## Hand in solutions until Saturday, 18 June 2011, 23:59h.

To estimate the average effort you put into solving the following exercises, please add after each exercise the amount of time you spent for it.

**Exercise 9.1** (Breaking truncated linear congruential generators). (19+5 points)

We consider the truncated homogenous linear congruential generators with $x_i = sx_{i-1} \operatorname{rem} m$. We are given that $m = 1009$, $k = \lceil \log_2(m)/2 \rceil = 5$ and $a = 25$. The sequence $y$ is defined as $y_i := x_i \operatorname{div} 2^k$ which you intercepted as

$$0, 10, 21, 25, 30, 8, 13, 13, 24, 14, 7, 6, 15, 28, 10, 3, 17, 25, 0, 15, 12, \ldots$$

Our task is to break this generator completely. To do so, we will recover the sequence $z_i$ with $x_i = y_i 2^k + z_i$.

(i) Write down the matrix (over $\mathbb{Z}$!) [1]

$$A = \begin{bmatrix} m & 0 & 0 & 0 & 0 & 0 \\ -s & 1 & 0 & 0 & 0 & 0 \\ -s^2 & 0 & 1 & 0 & 0 & 0 \\ -s^3 & 0 & 0 & 1 & 0 & 0 \\ -s^4 & 0 & 0 & 0 & 1 & 0 \\ -s^5 & 0 & 0 & 0 & 0 & 1 \end{bmatrix}$$

(ii) Compute the sequence $c_i := (s^{i-1}y_1 - y_i)2^k$ over $\mathbb{Z}$ for $i = 1, \ldots, 6$. [1]

(iii) Using lattice basis reduction compute a reduced basis $B$ and a unimodular transformation $U$ such that $B = UA$. [2]

(iv) Compute $Uc$ and take the balanced system of representatives modulo $m$ of your result, i.e. divide each entry $c'_i = (Uc)_i$ with rest by $m$ and if it is larger than $m/2$ write it as $c'_i - m$. [2]

(v) Now solve $Bz = Uc$ using Gaussian elimination, obtaining the $z_i$. [2]

(vi) Finish by writing down the sequence $x_i$. [2]

(vii) Compute the next 10 values of the above sequence of $y$'s. [2]

(viii) Argue that you have broken the generator. [2]

(ix) Explain in detail why we had to use basis reduction at all. [5]

(x) Play a bit around with your algorithms. Try different values of $m$, $s$ and $k$ and report on the successes and failures of your algorithm. [+5]

**Exercise 9.2** ($\varphi$-asco). (4 points)

4 Let $p, q \in \mathbb{N}$ be two different prime numbers. Let $N = p \cdot q$. Then $\varphi(N) = (p-1) \cdot (q-1)$. Give a quadratic formula which allows you to compute $p$ and $q$ from $N$ and $\varphi(N)$. Use it to factor $N = 168149075693$ knowing $\varphi(N) = 168148245408$.

**Exercise 9.3** (Factoring $x$ modulo $N$). (10 points)

Let $p \neq q$ be prime numbers, $N = p \cdot q$, $f = x \in \mathbb{Z}_N[x]$.

2 (i) Show that $p^2 + q^2$ is a unit in $\mathbb{Z}_N^\times$, i.e. $\gcd(p^2 + q^2, pq) = 1$.

1 (ii) Let $u \in \mathbb{Z}_N$ be the inverse of $p^2 + q^2$. Show that $f = u(px + q)(qx + p)$.

5 (iii) Prove that the two linear factors in (ii) cannot be written as a product of two polynomials of degree at least 1 and that they cannot be inverted in $\mathbb{Z}_N[x]$. Hint: Consider the situation in $\mathbb{Z}_p$ and and $\mathbb{Z}_q$ separately.

2 (iv) Conclude that if you can factor polynomials over $\mathbb{Z}_N$ then you can factor the integer $N$.

**Exercise 9.4** (A lattice basis). (14 points)

Let $e, d, p, q, N$ be positive natural numbers defines as in the specification of the RSA cryptosystem. In the lecture we discussed a lattice whose elements are the exactly the pairs $(x_1, x_2) \in \mathbb{Z}^2$ of solutions to the equation $ex_1 + x_2 = 0$ in $\mathbb{Z}_N$. In this exercise we will explore a more general problem: Let $a_1, \ldots, a_n \in \mathbb{Z}$ and $N \in \mathbb{N}$ with $\gcd(a_n, N) = 1$ and consider the lattice

$$L = \{(x_1, \ldots, x_n) \in \mathbb{Z}^n \mid a_1 x_1 + \cdots + a_n x_n = 0 \text{ in } \mathbb{Z}_N\}.$$

2 (i) Solve the defining equation of the lattice for $x_n$.

2 (ii) Rewrite the resulting equation in $\mathbb{Z}_N$ as an equation over the integers.

7 (iii) Find a basis for $L$.

3 (iv) Describe how you can use the above lattice to find solutions for the following problem: Input is a positive integer $N$ and integers $a_1, \ldots, a_n$. Find $x_1, \ldots, x_n \in \{0, 1\}$ such that $\sum_{1 \leq i \leq n} a_i x_i = 0$ in $\mathbb{Z}_N$.