The art of cryptography: Lattices and cryptography, summer 2013

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

3. Exercise sheet
Hand in solutions until Sunday, 05 May 2013, 23:59h.

Exercise 3.1 (Breaking truncated linear congruential generators). (19+10 points)

We consider the truncated homogenous linear congruential generators with $x_i = sx_{i-1} \in \mathbb{Z}_m$. We are given that $m = 1009$, $\ell = \lceil \log(2, m)/2 \rceil = 5$ and $s = 25$. The sequence y is defined as $y_i := \lfloor x_i/2^\ell \rfloor$ 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 $x_i = y_i 2^\ell + z_i$.

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

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

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

(iii) Using lattice basis reduction compute a reduced basis B and a unimodular transformation U such that $B = UA$. $\boxed{2}$

(iv) Compute Uc and take the balanced system of representatives modulo m of your result. $\boxed{2}$

(v) Now solve $Bz = Uc$ using Gaussian elimination, obtaining the z_i. $\boxed{2}$

(vi) Finish by writing down the sequence x_i. $\boxed{2}$

(vii) Compute the next 5 values of the above sequence of y's. $\boxed{2}$

(viii) Argue that you have broken the generator. $\boxed{2}$

(ix) Explain in detail why we had to use basis reduction at all. $\boxed{5}$

(x) Play a bit around with your algorithms. Try different values of m, s and ℓ and report on the successes and failures. $\boxed{+10}$

Exercise 3.2 (Dual lattices). (10 points)

Let L be a lattice generated by the basis $B \in \mathbb{R}^{\ell \times n}$, and let L^* be its dual.

$\boxed{5}$ (i) Prove that $D = (BB^T)^{-1}B$ is a basis of L^*. Hint: We have $\text{span}_{\mathbb{R}}(B) = \text{span}_{\mathbb{R}}(D)$ and $DB^T = I$, where I is the identity matrix.

$\boxed{1}$ (ii) Show that $(L^*)^* = L$.

$\boxed{1}$ (iii) Prove that $|L^*| = |L|^{-1}$.

$\boxed{1}$ (iv) Show that $\lambda(L)\lambda(L^*) \leq n$. Hint: Use Minkowski's bound $\lambda(L) \leq \sqrt{n}\det(L)^{1/n}$.

$\boxed{2}$ (v) Let L be the lattice generated by the basis

$$B = \begin{pmatrix} 1 & 2 & 3 \\ 4 & 5 & 6 \end{pmatrix}.$$

Compute a basis of L^*.