Heads and tails, summer 2015

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

2. Exercise sheet
Hand in solutions until Saturday, 25 April 2015, 23:59:59

Exercise 2.1 (Linear congruential generators). (17+7 points)

We consider linear congruential generators with $x_i = sx_{i-1} + t$ in $\mathbb{Z}_m$.

(i) Compute *by hand* the sequence of numbers resulting from [2]

(a) $m = 10$, $s = 3$, $t = 2$, $x_0 = 1$ and

(b) $m = 10$, $s = 8$, $t = 7$, $x_0 = 1$.

What do you observe?
Can you explain the behavior? [+3]

(ii) You observe the sequence of numbers [3]

$$13, 223, 793, 483, 213, 623, 593, \ldots$$

generated by a linear congruential generator. Find matching values of m, s and t

(iii) Implement the linear congruential generator in a programming language of your choice. Generate 500kB of output in the following way: Fix the prime $m = 2^{31} - 1$. Set $s = 70423329$, $t = 1135629868$ and $x_0 = 35690178$. Now generate sufficiently many 31 bit outputs of the generator and return the least significant three bytes of the result (discarding the most significant 7 bits. Hand-in source code and the first twenty bytes of the output. [6]

(iv) Similar to Exercise 1.2 compute the byte distribution of the output bytes. [2]

(v) Compute the byte-entropy of the distribution. What do you observe? [2]

(vi) What can you conclude? Explain detailed. [2]

[+4]

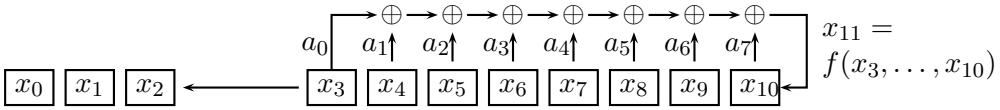
Exercise 2.2 (Linear feedback shift register). (8 points)

A Linear feedback shift register (LFSR) is a linear Boolean function $f : \mathbb{B}^n \to \mathbb{B}$ with $f(y_0, \ldots, y_{n-1}) = \bigoplus_{0 \le i < b} a_i y_i$ and fixed $a_0, \ldots, a_{n-1} \in \mathbb{B}$. We obtain a mapping $\mathbb{B}^n \to \mathbb{B}^*$ by applying f recursively, starting with a seed $(x_0, \ldots, x_{n-1}) \in \mathbb{B}^n$ and

8

$$x_i = f(x_{i-n}, \ldots, x_{i-1}) \text{ for } i \ge n. \tag{2.3}$$

We illustrate the fourth computation step, with $n = 8$:



Such a structure is convenient to implement in hardware. Show that an LFSR that produces the same sequence of bits can be efficiently computed from $x_0, \ldots, x_{2n-1}$. Conclude that such an LFSR is not useful as a cryptographic pseudorandom generator.

[Hint: consider the smallest value of n for which (2.3) holds with some linear f for the given values. Set up a system of linear equations over $\mathbb{F}_2$ for the coefficients of this f, and show that it is nonsingular.]