MATHEMATISCHES INSTITUT
DER UNIVERSITÄT MÜNCHEN
Prof. Otto Forster

SS 2005
May 19, 2005

Cryptography

Problem Sheet #5

Problem 17 We define a binary operation $\boxtimes : \mathbb{Z}_{256} \times \mathbb{Z}_{256} \to \mathbb{Z}_{256}$ using the bijective map

$$\phi : \mathbb{Z}_{256} \to \mathbb{F}_{257}^*, \quad x \mapsto \phi(x) := \begin{cases} 256 & \text{if } x = 0, \\ x & \text{if } x \neq 0, \end{cases}$$

as follows: $x \boxtimes y := \phi^{-1}(\phi(x) \cdot \phi(y))$, where '$\cdot$' denotes multiplication in the field $\mathbb{F}_{257}$.

a) Prove that $(\mathbb{Z}_{256}, \boxtimes)$ is a group, which is isomorphic to $(\mathbb{Z}_{256}, +)$.

b) Show that $(\mathbb{Z}_{256}, +, \boxtimes)$ is not a ring.

Problem 18 A map of the form

$$f : \mathbb{Z}_m \longrightarrow \mathbb{Z}_m, \quad x \mapsto f(x) = (ax + b) \bmod m,$$

where a, b are given integers, defines a *linear congruential generator* in $\mathbb{Z}_m$:
For any initial value $x_0 \in \mathbb{Z}_m$, a sequence $(x_i)_{i \geq 0}$ is defined by the recursion relation $x_{i+1} = f(x_i)$.
The following is the beginning of a sequence by a linear congruential generator in $\mathbb{Z}_{25}$, which has been identified with the alphabet `A` – `Z` without the letter `J`.

`TEA`

Calculate a, b, and complete the sequence until it becomes periodic.

Problem 19

a) Show that the polynomial $F(T) := T^7 + T + 1 \in \mathbb{F}_2[T]$ is irreducible.

b) Prove that for every initial vector $v = (b_0, b_1, \ldots, b_6) \in \mathbb{F}_2^7 \smallsetminus \{\vec{0}\}$ the LFSR sequence defined by

$$b_{k+7} = b_k + b_{k+1}$$

has period length 127.

Problem 20 Use the sequence (b_i) of 19b) to "shrink" the sequence (x_i) of problem 18 as follows: Define $z_i := x_{k_i}$, where k_i is the position of the i-th '1' in the sequence (b_i) (all counts are 0-based).

What is the period of the shrunk sequence (z_i) for the initial vector

$$v = (b_0, \ldots, b_6) = (1, 1, \ldots, 1).$$

What about other initial vectors?

Due: Friday, May 27, 2005, 14:10 h