RUHR UNIVERSITÄT BOCHUM

Lehrstuhl für Kryptologie und IT-Sicherheit
Prof. Dr. Alexander May
Elena Kirshanova

Präsenzübungen zur Vorlesung

Kryptanalyse I

SS 2015

Blatt 3 / 11 Juni 2015

Aufgabe 1:
In the Pollard's ρ method for collision-finding with the 'tail'-length i and 'loop'-length k show that a collision $s_m = s_{2m}$ will appear for

$$m = k \left\lceil \frac{i}{k} \right\rceil .$$

Aufgabe 2:
Pollard's ρ for the factorization problem.
In this exercise we develop a variant of the Pollard's ρ method for factoring n. We assume that $p|n$ is the smallest (but still large to brute-force) divisor of n.
The idea is to find two distinct $x, x' \in \mathbb{Z}_n$, s.t. $x - x' = 0 \mod p$ (note that we do not know p, but $\gcd(x - x', n)$ reveals p). The tuple (x, x') defines a *collision*.
To find a collision efficiently, we define a random walk on $\mathbb{Z}_n$ as

$$f(x) = x^2 + a \mod n, \quad a \in \mathbb{Z}_n$$

and consider a sequence $x_0, x_1, x_2, \ldots$ such that $x_i = f(x_{i-1})$ (we fix some initial x_0).

1. Describe a Pollard's ρ algorithm for factoring having the running time of $\widetilde{\mathcal{O}}(\sqrt{p})$.
2. Explain why the following choices for $f(x)$ are bad:
   - $f(x) = ax + b \mod n$, $a, b \in \mathbb{Z}_n$,
   - $f(x) = x^2 \mod n$,
   - $f(x) = x^2 - 2 \mod n$.
3. Given $f(x) = x^2 + 1$ and $x_0 = 1$, factor $n = 899$.

Aufgabe 3:
4-List Problem.

1. Solve the following 4-List problem:

$$L_1 = \{101111, 101001, 001101, 010100\}, \quad L_2 = \{011101, 001100, 101011, 100011\},$$
$$L_3 = \{101000, 001110, 100011, 111101\}, \quad L_4 = \{100010, 100001, 110100, 010111\}.$$

2. Show how to solve an 'inhomogeneous' version of the 4-List problem: for four lists $L_1, L_2, L_3, L_4, |L| = 2^{n/3}$ and $c \in \mathbb{F}_2^n$, give an algorithm that finds $x_i \in L_i, i = 1 \dots 4$ s.t.

$$x_1 \oplus x_2 \oplus x_3 \oplus x_4 = c$$

in time $\widetilde{\mathcal{O}}(2^{n/3})$.

3. Using the previous result, solve the following 4-List problem for $c = 101101$:

$$L_1 = \{101111, 101001, 001101, 010100\}, \quad L_2 = \{110000, 100001, 000110, 001110\},$$
$$L_3 = \{101000, 001110, 100011, 111101\}, \quad L_4 = \{100010, 100001, 110100, 010111\}.$$