Ruhr-Universität Bochum
Lehrstuhl für Kryptologie und IT-Sicherheit
Prof. Dr. Alexander May
Elena Kirshanova, Ilya Ozerov

Präsenzübungen zur Vorlesung

Kryptanalyse

SS 2014

Blatt 3 / 05. Mai 2014

AUFGABE 1:

Führen Sie Pollards Rho Algorithmus aus der Vorlesung mit folgenden Werten aus. Der Algorithmus bekommt als Eingabe die Primzahl $p = 17$, $\alpha = 5$ (ein Generator von $\mathbb{Z}_p^*$), sowie ein Element $\beta = 10$. Die Ausgabe soll $z = \text{dlog}_\alpha(\beta) \bmod n$ sein, d.h. die Lösung der Gleichung $\alpha^z = \beta \bmod p$.

Partitionieren Sie $\mathbb{Z}_p^*$ in $S_1 = \{s \in \mathbb{Z}_p^* \mid s = 0 \bmod 3\}$, $S_2 = \{s \in \mathbb{Z}_p^* \mid s = 1 \bmod 3\}$ und $S_3 = \{s \in \mathbb{Z}_p^* \mid s = 2 \bmod 3\}$. Wie viele Schritte sind nötig? Wie oft muss die Funktion f aufgerufen werden?

AUFGABE 2:

Sei $N = pq$ ein RSA-Modul mit $p < q$. Angenommen, wir haben eine zufällige Funktion $f : \mathbb{Z}_N \to \mathbb{Z}_N$.

(a) Zeigen Sie, dass die Faktorisierung von N in erwarteter Zeit $\widetilde{\mathcal{O}}(\sqrt{p})$ und vernachlässigbarem Platz bestimmt werden kann. Geben Sie dazu einen Pollard Rho Algorithmus an, der s_i, s_{2i} mit $s_i \neq s_{2i}$, aber $s_i = s_{2i} \bmod p$ findet.

(b) Berechnen Sie die Faktorisierung von $N = 35$ mit der Funktion $f(x) = x^2 + 1$, $s_0 = 1$.

AUFGABE 3:

Seien L_1, L_2, L_3, L_4 Listen mit unabhängig gleichverteilt gewählten Elementen aus $\mathbb{F}_2^n$ und $c \in \mathbb{F}_2^n$. Geben Sie einen Algorithmus an, der $x_1 \in L_1, x_2 \in L_2, x_3 \in L_3, x_4 \in L_4$ findet mit $x_1 \oplus x_2 \oplus x_3 \oplus x_4 = c$ in $\mathbb{F}_2^n$. Zeigen Sie, dass die Laufzeit Ihres Algorithmus $\widetilde{\mathcal{O}}(2^{n/3})$ ist, wenn $|L_1| = |L_2| = |L_3| = |L_4| = 2^{n/3}$ gilt.

AUFGABE 4:

(a) Lösen Sie das folgende 4 Listen Problem mit $c = 100000$.

$$L_1 = \{100111, 110101, 001110, 111001\}, L_2 = \{011011, 100011, 011010, 100101\},$$
$$L_3 = \{010010, 001011, 000110, 111101\}, L_4 = \{001011, 111010, 001001, 101101\}$$

(b) Lösen Sie das folgende 4 Listen Problem mit $c = 1100$. Beachten Sie, dass $n = 4$ gilt.

$$L_1 = \{0011, 0000\}, L_2 = \{0000, 1000\}, L_3 = \{0100, 0101\}, L_4 = \{0010, 1000\}$$