RUHR UNIVERSITÄT BOCHUM

RUB

Lehrstuhl für Kryptologie und IT-Sicherheit
Prof. Dr. Alexander May
Mathias Herrmann, Enrico Thomae

Hausübungen zur Vorlesung

Kryptanalyse

WS 2010/2011

Blatt 3 / 11. Oktober 2010 / Abgabe bis spätestens 03. November 2010, 10 Uhr (vor der Übung)

Hinweis: Sie können die `sage` Programm-Codes per Email direkt an **ilya.ozerov@rub.de** schicken.

AUFGABE 1 (5 Punkte)**:**
Sei $N = pq$ ein RSA-Modul mit $p < q$. Angenommen, wir haben eine zufällige Funktion $f : \mathbb{Z}_N \to \mathbb{Z}_N$. Zeigen Sie, dass die Faktorisierung von N in erwarteter Zeit $\tilde{\mathcal{O}}(N^{\frac{1}{4}})$ und Platz $\tilde{\mathcal{O}}(1)$ bestimmt werden kann.
Hinweis: Finden Sie s_i, s_{2i}, $s_i \neq s_{2i}$ mit $s_i = s_{2i} \bmod p$.

AUFGABE 2 (5 Punkte)**:**
Schreiben Sie eine Funktion in sage, die den Pollard-Rho Algorithmus durchführt. Die Funktion soll als Eingabe ein Element α, die Ordnung von α, sowie ein Element β erhalten. Die Ausgabe der Funktion ist

$$x = \mathrm{dlog}_\alpha \beta \bmod \mathrm{ord}(\alpha).$$

(Wählen Sie die Partitionierung von $\mathbb{Z}_p^*$ als $S_1 = \{s \in \mathbb{Z}_p^* \mid s \equiv 0 \bmod 3\}, S_2 = \{s \in \mathbb{Z}_p^* \mid s \equiv 1 \bmod 3\}, S_3 = \{s \in \mathbb{Z}_p^* \mid s \equiv 2 \bmod 3\}$.)

Berechnen Sie mit Ihrem Algorithmus den diskreten Logarithmus von $\beta = 1580240$ zur Basis $\alpha = 897139$ in $\mathbb{Z}_p^*$ mit $p = 1827773$. Die Ordnung von α ist 456943. Wie viele Schritte sind nötig? Stimmt das mit der erwarteten Anzahl an Schritten überein?

AUFGABE 3 (10 Punkte)**:**
Polynomauswertung an n Punkten: Sei $f(x)$ ein Polynom vom Grad $n-1$ wobei n eine Zweierpotenz ist. Im Folgenden bezeichne mod das modulo auf dem Ring der Polynome in x. Wir setzen voraus, dass man $g(x) \bmod h(x)$ für beliebige Polynome des Grades höchstens $n-1$ in Zeit $O(n \log n)$ berechnen kann.
Gegeben seien $f(x)$ und n Stellen $x_0, \ldots, x_{n-1}$. Zu berechnen ist $f(x_i)$ für $i = 0, \ldots, n-1$. Für $0 \leq i \leq j \leq n-1$ definieren wir $p_{ij}(x) = \prod_{m=i}^{j}(x - x_m)$ und $q_{ij}(x) = f(x) \bmod p_{ij}(x)$.

(a) Zeigen Sie, dass $f(x) \bmod (x - z) = f(z)$ für alle z.

(b) Zeigen Sie, dass $q_{kk}(x) = f(x_k)$ und $q_{0,n-1}(x) = f(x)$.

(c) Zeigen Sie, dass für $i \leq k \leq j$ gilt $q_{ik}(x) = q_{ij}(x) \bmod p_{ik}(x)$ und $q_{kj}(x) = q_{ij}(x) \bmod p_{kj}(x)$.

(d) Konstruieren Sie einen Algorithmus, der in Zeit $O(n \log^2 n)$ die Werte $f(x_0), \ldots, f(x_{n-1})$ berechnet.