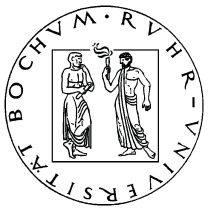
Ruhr-Universität Bochum
Lehrstuhl für Kryptologie und IT-Sicherheit
Prof. Dr. Alexander May
Maike Ritzenhofen, Alexander Meurer



Hausübungen zur Vorlesung

Kryptanalyse

SS 2008

Blatt 3 / 23. Mai 2008 / Abgabe 05. Juni 2008 bis 12Uhr in den Kasten auf NA 02

AUFGABE 1 (4 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 (4 Punkte)**:**
Benutzen Sie Pollard's Rho-Methode, um den diskreten Logarithmus $\log_3(5)$ in $\mathbb{Z}_{17}^*$ zu berechnen. Verwenden Sie dabei dieselbe Funktion f wie in der Vorlesung, und partionieren Sie $S_1 = \{1, 2, 3, 4, 5, 6\}, S_2 = \{7, 8, 9, 10, 11\}$ und $S_3 = \{12, 13, 14, 15, 16\}$. Geben Sie für jeden Schleifendurchlauf i die Werte (s_i, x_i, y_i) und (s_{2i}, x_{2i}, y_{2i}) an.

AUFGABE 3 (4 Punkte)**:**
Alice lernt weiter aus ihren Fehlern und verschickt auch keine Einladungen mehr an k Empfänger mit gleichem RSA-Exponenten k und verschiedenen RSA-Moduln. Bei nächster Gelegenheit will sie Bob, Berta, Birte und Bruno einladen. Diese besitzen die paarweise teilerfremden RSA-Moduln N_1, N_2, N_3 und N_4 und die öffentlichen Exponenten $e_1 = e_2 = 3$ sowie $e_3 = e_4 = 5$. Die von Alice verschickte Einladung soll ein gültiger Klartext für alle Moduln sein, d.h. $m < \min\{N_1, N_2, N_3, N_4\}$.
Eve ist auch zu dieser Feier nicht eingeladen. Zeigen Sie, dass Eve allerdings wieder m effizient berechnen kann.

AUFGABE 4 (8 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 $g(x) \mod h(x)$ 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 $q_{ij}(x) = f(x) \mod p_{ij}(x)$.

(a) Zeigen Sie, dass $f(x) \mod (x - z) = f(z)$ 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 $q_{ik}(x) = q_{ij}(x) \mod p_{ik}(x)$ und $q_{kj}(x) = q_{ij}(x) \mod p_{kj}(x)$.

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