



Hausübungen zur Vorlesung

Kryptanalyse

WS 2009/2010

Blatt 3 / 11. November 2009 / Abgabe bis spätestens 25. November 2009, 10
Uhr (vor der Übung)

AUFGABE 1 (4 Punkte):

Angenommen, wir haben einen Algorithmus DH, der das Diffie-Hellman Problem löst, d.h. $\text{DH}(p, \alpha, \alpha^a, \alpha^b) = \alpha^{ab}$.

Zeigen Sie, dass man daraus einen Algorithmus ELGAMAL konstruieren kann, der bei Eingabe einer ElGamal verschlüsselten Nachrichten den zugrundeliegenden Klartext ausgibt, d.h. $\text{ELGAMAL}(p, \alpha, \beta, \alpha^r, m\beta^r) = m$.

AUFGABE 2 (4 Punkte):

Sei $N = pq$ ein RSA-Modul mit $p < q$. Angenommen, wir haben eine zufällige Funktion $f : \mathbb{Z}_n \rightarrow \mathbb{Z}_n$. Zeigen Sie, dass die Faktorisierung von N in erwarteter Zeit $\tilde{O}(N^{\frac{1}{4}})$ und Platz $\tilde{O}(1)$ bestimmt werden kann.

Hinweis: Finden Sie s_i, s_{2i} , $s_i \neq s_{2i}$ mit $s_i = s_{2i} \bmod p$.

AUFGABE 3 (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 partitionieren 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 4 (8 Punkte):

Polynomauswertung an n Punkten: Sei $f(x)$ ein Polynom vom Grad $n - 1$, wobei n eine Zweierpotenz ist. Im Folgenden bezeichne $\bmod$ 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 $x_0, \dots, x_{n-1}$. Zu berechnen ist $f(x_i)$ für $i = 0, \dots, n - 1$. 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 $f(x_0), \dots, f(x_{n-1})$ berechnet.