Gitter und Kryptographie

Blatt 13, 03.02.2006, Abgabe 10.02.2006

Aufgabe 1. Kleine Dekodierexponent Angriff auf RSA

a) Erklären Sie, wie RSA funktionniert (mit Einzelheiten), mit Standard Notation (N, e, d, p, q).

Wir nehmen an, dass $\frac{\sqrt{N}}{2} < q < p < 2\sqrt{N}, e = N^{\alpha}, d = N^{\delta}, N > 64$.

b) Zeigen Sie, dass man (ein RSA-Modul) N faktorisieren kann, wenn er alle Lösungen (k, s) der folgenden Gleichung kennt:

$$k(A+s) = 1 \bmod e \quad \text{mit} \quad \begin{cases} |k| < 2e^{1+\frac{\delta-1}{\alpha}} \\ |s| < 4e^{\frac{1}{2\alpha}} \\ A = N+1 \end{cases}$$

Sei $f(x, y) = x(A+y) - 1$, dann bilden wir ein Gitter L so : für jedes $k = 0, \ldots, m$, das Gitter halt Basis Vektoren aus der folgenden Polynom-Menge: $\{e(xX)^k f^0(xX, yY), (xX)^{k-1} f(xX, yY), (xX)^{k-2} f^2 \frac{(nX,yY)}{e}, \cdots, \ldots, (xX)^0 f^k \frac{(xX,yY)}{e^{k-1}}\}$ in Basis $\{x^i y^j\}$.

c) Im Fall $m = 3$, bilden Sie die Matrix, die das Gitter herstellt, in einer günstigen Ordnung von den Basiselementen $\{x^i y^i\}$, so dass die Matrix dreieckig ist.

d) Im allgemeinen Fall berechnen Sie die Determinanten dieser Gitter (benutzen Sie $\sum_{i=1}^{k} i^2 = \frac{k}{6}(2k^2 + 3k + 1)$ als Beweis).

Im folgenden nehmen wir an, dass $\alpha = 1$ und dass die Bedingungen $\begin{cases} |k| < e^{\delta} \\ |s| < e^{1/2} \end{cases}$ erfüllt sind.

e) Bilden Sie die Ungleichung, die erfüllt werden muss, so dass wir ein Polynom mit k, s als Wurzel (über $\mathbf{Z}$) bekommen, nachdem die LLL-Reduktion durchgeführt wurde.

Um zu vereinfachen, nehmen wir an, dass die letzte Ungleichung erfüllt ist, wenn $\frac{\det L}{e^{\dim\ L}} \cdot (dim\ L)^{\frac{dim\ L}{2}} = e^{g(m,\delta)}$ verifiziert $g(m,\delta) < 0$.

f) Nennen Sie die Bedingung für δ, so dass $\exists m_0, \forall m > m_0,\ g(m,\delta) < 0$.

g) Schliessen Sie ab!