RUHR UNIVERSITÄT BOCHUM

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

Präsenzübungen zur Vorlesung

Kryptanalyse

WS 2010/2011

Blatt 6 / 17. November 2010

AUFGABE 1:
Sei $N \in \mathbb{N}$ und $f(x) = x^n + a_{n-1}x^{n-1} + \ldots + a_1 x + a_0$. Verwenden Sie die Coppersmith-Methode mit der folgenden Kollektion von Polynomen

$$f_i(x) = x^i N \text{ für } i = 0, \ldots, n-1 \text{ und } f_n(x) = f(x),$$

um die Gleichung $f(x) = 0 \bmod N$ zu lösen. Stellen Sie die Basismatrix aus den Koeffizientenvektoren der $f_i(xX)$ auf. Welche Schranke X and die Lösung x erhalten Sie? Vergleichen Sie mit der Schranke für Linearisierungsangriffe. Welche Vorteile bietet die Coppersmith-Methode?

AUFGABE 2:
Sei $N = pqr$ ein modifizierter RSA-Modul mit $p > q > r$. Sei ferner eine Approximation $\tilde{p}$ von p gegeben mit $|p - \tilde{p}| \leq N^{\frac{1}{9}}$.

(a) Zeigen Sie, dass die Faktorisierung von N in Zeit polynomiell in $\log N$ berechnet werden kann.

(b) Angenommen p, q und r haben gleiche Bitgröße. Welchen Bruchteil der Bits von p muss man bei dieser Parameterwahl kennen, um N effizient faktorisieren zu können?

(c) Vergleichen Sie mit normalen RSA-Moduln $N = pq$ und $p \approx q$.

AUFGABE 3:
Seien $sig_k(x), sig_k(x')$ zwei DSA-Signaturen unterschiedlicher Nachrichten $x \neq x' \bmod q$ unter Verwendung desselben r. Zeigen Sie, dass dann a effizient berechnet werden kann, sofern $\gamma \neq 0$.