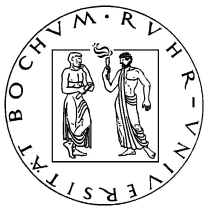
Ruhr-Universität Bochum
Lehrstuhl für Kryptologie und IT-Sicherheit
Prof. Dr. Alexander May
Mathias Herrmann, Alexander Meurer



Präsenzübungen zur Vorlesung

Kryptanalyse

WS 2009/2010

Blatt 6 / 23. Dezember 2009

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 $m = 1$ und der folgenden Kollektion von Polynomen

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

Stellen Sie die Basismatrix aus den Koeffizientenvektoren der $f_i(xX)$ auf. Welche Schranke erhalten Sie? Vergleichen Sie mit der Schranke für Linearisierungsangriffe. Welche Vorteile bietet die Coppersmith-Methode?

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

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

(b) Angenommen p und q haben gleiche Bitgröße. Welchen Bruchteil der Bits von p muss bei dieser Parameterwahl kennen, um N effizient faktorisieren zu können? Vergleichen Sie mit normalen RSA-Moduln $N = pq$.

AUFGABE 3:
Sei $M \in \mathbb{N}$ mit unbekanntem Teiler b und $f(x) \in \mathbb{Z}_M[x]$ mit Grad n. Sei A ein Algorithmus, der bei Eingabe M und $f(x)$ eine Nullstelle x_0 von $f(x)$ modulo b berechnet, die keine Nullstelle von $f(x)$ modulo M ist, d.h.

$$f(x_0) = 0 \bmod b \quad \text{und} \quad f(x_0) \neq 0 \bmod M.$$

Dann kann man einen nicht-trivialen Faktor von M in Zeit polynomiell in n und $\log M$ bestimmen.

AUFGABE 4:
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 $\gamma \neq 0$.