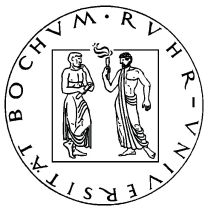
Ruhr-Universität Bochum
Lehrstuhl für Kryptologie und IT-Sicherheit
Prof. Dr. Alexander May
Maike Ritzenhofen, Alexander Meurer



Präsenzübungen zur Vorlesung

Kryptanalyse

SS 2008

Blatt 6 / 03.Juli 2008

AUFGABE 1:
Sei $N = p^2q$ 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 2:
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 Nullstellen 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 3:
Sei ein Algorithmus A gegeben, der bei Eingabe N einen nicht-trivialen Teiler von N in Zeit polynomiell in $\log N$ berechnet. Zeigen Sie, dass dann die komplette Primfaktorzerlegung von N in Zeit polynomiell in $\log N$ berechnet werden kann.

AUFGABE 4:
Faktorisieren Sie die Zahl 119 mit Hilfe der Faktorbasis $F = \{2, 3, 5\}$.