Ruhr-Universität Bochum
Lehrstuhl für Kryptologie und IT-Sicherheit
Prof. Dr. Alexander May
Elena Kirshanova, Ilya Ozerov

Präsenzübungen zur Vorlesung

Kryptanalyse

SS 2014

Blatt 2 / 28. April 2014

AUFGABE 1:

Seien p, q_1, q_2 prim, $r, B \in \mathbb{N}$, $q_1 > q_2 > p$ und $r \leq B < p$. Betrachten Sie das "approximative ggT Problem": Gegeben sind $N_1 = p \cdot q_1$ und $N_2 = p \cdot q_2 + r$, gesucht ist p.

(a) Zeigen Sie, dass es ein $1 \leq i \leq B$ mit $p = \text{ggT}(N_1, N_2 - i)$ gibt. Beschreiben Sie daraus einen Bruteforce Algorithmus, der das Problem in Zeit $\widetilde{\mathcal{O}}(B)$ löst. Zeigen Sie Korrektheit und Laufzeit.

(b) Zeigen Sie, dass $p \mid \text{ggT}\left(N_1, \prod_{i=1}^{B}(N_2 - i) \bmod N_1\right)$. Weshalb gilt nicht unbedingt auch Gleichheit? Beschreiben Sie einen Bruteforce Algorithmus, der das Problem in Zeit $\widetilde{\mathcal{O}}(B)$ mit nur $\mathcal{O}(\log B)$ ggT-Berechnungen löst. Zeigen Sie Korrektheit und Laufzeit.

AUFGABE 2:

Wir betrachten das Diskrete Logarithmus Problem: Es sind α, $\beta = \alpha^x$ und $n = \text{ord}(\alpha)$ gegeben. Gesucht ist $x \in \mathbb{Z}_n$. Beschreiben Sie einen Meet-in-the-Middle Angriff auf x mit Zeit und Platz $\widetilde{\mathcal{O}}(\sqrt{n})$.

Verwenden Sie Ihren Algorithmus um $\log_5(10)$ in $\mathbb{Z}_{17}^*$ zu berechnen.

AUFGABE 3:

Sei $N = pq$ ein RSA-Modul mit $p < q$. Zeigen Sie durch einen Meet-in-the-Middle Angriff auf den Parameter p, dass man die Faktorisierung von N in Zeit und Platz $\widetilde{\mathcal{O}}(\sqrt{p})$ berechnen kann.

AUFGABE 4:

Sei (N, e) ein öffentlicher RSA Schlüssel mit identischen CRT-Exponenten $d_p = d_q$.

(a) Zeigen Sie, dass dann die Faktorisierung von N in Zeit $\widetilde{\mathcal{O}}(d_p)$ und vernachlässigbarem Platz berechnet werden kann.

(b) Zeigen Sie, dass die Faktorisierung von N auch in Zeit und Platz $\widetilde{\mathcal{O}}(\sqrt{d_p})$ berechnet werden kann.