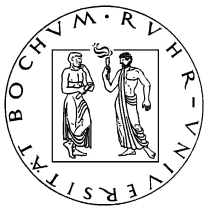
Ruhr-Universität Bochum
Lehrstuhl für Kryptologie und IT-Sicherheit
Prof. Dr. Alexander May
Maike Ritzenhofen, Alexander Meurer



Hausübungen zur Vorlesung

Kryptanalyse

SS 2008

Blatt 2 / 02. Mai 2008 / Abgabe 23. Mai 2008 bis 12Uhr in den Kasten auf NA 02

AUFGABE 1 (4 Punkte)**:**
Alice schickt eine Einladung m zu ihrer Geburtstagsparty an Bob und Berta. Dabei verschlüsselt Alice m mit den öffentlichen RSA-Schlüsseln (N, e_1) und (N, e_2) von Bob und Berta, wobei e_1 und e_2 teilerfremd sind.
Eve ist nicht zur Party eingeladen. Zeigen Sie, dass Eve trotzdem aus den Chiffretexten die Einladung m effizient berechnen kann.

AUFGABE 2 (4 Punkte)**:**
Alice hat aus ihren Fehlern gelernt und verschickt keine Einladungen mehr an Empfänger mit gleichen RSA-Moduln. Zu ihrer nächsten Feier will sie Bob, Berta und Birte einladen. Diese besitzen die paarweise teilerfremden RSA-Moduln N_1, N_2 und N_3 und verwenden alle den öffentlichen Exponenten $e = 3$. Die von Alice verschickte Einladung soll ein gültiger Klartext für alle Moduln sein, d.h. $m < \min\{N_1, N_2, N_3\}$.
Wiederum wurde die arme Eve nicht zur Party eingeladen. Zeigen Sie, dass Eve auch in diesem Fall m effizient berechnen kann.

AUFGABE 3 (4 Punkte)**:**
Sei (N, e) ein öffentlicher RSA-Schlüssel. Ein *Fixpunkt* dieser RSA-Verschlüsselung ist ein $x \in \mathbb{Z}_N$ mit $x^e \equiv x \pmod{N}$. Sei $N = pq$ die Primfaktorzerlegung von N. Zeigen Sie, dass genau

$$(\mathrm{ggT}(e-1, p-1)+1)\,(\mathrm{ggT}(e-1, q-1)+1)$$

Fixpunkte gibt.

AUFGABE 4 (4 Punkte)**:**
Angenommen, wir haben einen Algorithmus DH, der das Diffie-Hellman Problem löst, d.h. $\mathrm{DH}(p, \alpha, \alpha^a, \alpha^b) = \alpha^{ab}$.

Zeigen Sie, dass man daraus einen Algorithmus ELGAMAL konstruieren kann, der bei Eingabe einer ElGamal verschlüsselten Nachrichten den zugrundeliegenden Klartext ausgibt, d.h. $\text{ELGAMAL}(p, \alpha, \beta, \alpha^r, m\beta^r) = m$.

AUFGABE 5 (4 Punkte)**:**
Sei $N = pq$ ein RSA-Modul mit $p < q$. Zeigen Sie durch eine Meet-in-the-Middle Attacke auf den Parameter p, dass man die Faktorisierung von N in Zeit und Platz $\tilde{\mathcal{O}}(N^{\frac{1}{4}})$ berechnen kann.
Hinweis: Verwenden Sie analog zur Vorgehensweise in Abschnitt 3.1.2 des Skripts eine Polynomdarstellung.