



Hausübungen zur Vorlesung

Kryptanalyse

WS 2009/2010

Blatt 2 / 28. Oktober 2009 / Abgabe bis spätestens 11. November 2009, 10
Uhr (vor der Übung)

AUFGABE 1 (5 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 (5 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 (5 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 $\tilde{O}(N^{\frac{1}{4}})$ berechnen kann.

Hinweis: Verwenden Sie analog zur Vorgehensweise in Abschnitt 3.1.2 des Skripts eine Polynomdarstellung.

AUFGABE 4 (5 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

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

Fixpunkte gibt.