RUHR UNIVERSITÄT BOCHUM

Lehrstuhl für Kryptologie und IT-Sicherheit
Prof. Dr. Alexander May
Alexander Meurer, Ilya Ozerov

Präsenzübungen zur Vorlesung

Kryptanalyse

WS 2011/2012

Blatt 1 / 19. Oktober 2011

AUFGABE 1:
Sei (N, e) ein öffentlicher RSA-Schlüssel und (N, d) der zugehörige geheime Schlüssel. Zeigen Sie, dass auch für Nachrichten $m \in \mathbb{Z}_N \setminus \mathbb{Z}_N^*$ die Entschlüsselung korrekt ist.
(Der Satz von Euler sagt *nur* $a^{\varphi(N)} = 1 \bmod N$, falls $\gcd(a, N) = 1$.)

AUFGABE 2:
Alice feiert eine Party und möchte eine Einladung m an Bob, Berta und Birte verschicken. Diese besitzen paarweise teilerfremde RSA-Moduln N_1, N_2 und N_3. Außerdem benutzen alle drei den öffentlichen Schlüssel $e = 3$. Die von Alice verschickte Nachricht soll ein gültiger Klartext für alle Moduln sein, d.h. $m < \min_{i=1,2,3}\{N_i\}$.
Die arme Eve ist nicht zur Party eingeladen, würde aber liebend gerne wissen, wann und wo die Feier stattfindet. Helfen Sie Eve und zeigen Sie, wie man m effizient berechnen kann.

AUFGABE 3:
Sei N ein RSA-Modul und (e, d) ein Schlüsselpaar. Sei $\mathcal{O}$ ein Orakel, was zur Eingabe $m' \neq m$ eine gültige RSA-Signatur erzeugt, d.h. $\mathcal{O}(m')^e = m' \bmod N$. Zeigen Sie, dass man mit Hilfe dieses Orakels effizient eine Signatur von m berechnen kann, d.h. man kann RSA-Signaturen universell fälschen.

AUFGABE 4:
Sei (N, e) ein öffentlicher RSA Schlüssel mit zugehörigen CRT-Exponenten $d_p \neq d_q$. Zeigen Sie, dass dann die Faktorisierung von N in Zeit $\tilde{\mathcal{O}}(\min\{d_p, d_q\})$ und Platz $\tilde{\mathcal{O}}(1)$ berechnet werden kann.

Damit der Meet-in-the-Middle Angriff auf kleine CRT-Exponenten (siehe S. 24) tatsächlich in Zeit $\tilde{\mathcal{O}}(\min\{\sqrt{d_p}, \sqrt{d_q}\})$ läuft, müssen insbesondere die Schritte 3 und 4 mit dieser Komplexität realisierbar sein. Wir kümmern uns hier um Schritt 3. Der Beweis von Satz 25 impliziert Schritt 4 und ist Teil der Hausübung.

AUFGABE 5:
Seien $a_0, \ldots, a_{n-1}$ gegeben und sei $n = 2^k$ eine Zweierpotenz. Zeigen Sie, dass man in Zeit $\mathcal{O}(n \log^2 n)$ den Koeffizientenvektor $(p_0, \ldots, p_{n-1})$ des Polynoms $p(x) = \prod_{i=0}^{n-1}(x - a_i) = \sum_{i=0}^{n-1} p_i x^i$ berechnen kann. Sie dürfen hierfür voraussetzen, dass zwei Polynome $f(x), g(x)$ *gleichen* Grades $\deg f = \deg g = m$ mittels schneller Fourier Transformation (FFT) in Zeit $\mathcal{O}(m \log m)$ multipliziert werden können.

Hinweis: Verfolgen Sie einen Divide-and-Conquer Ansatz.