TECHNISCHE UNIVERSITÄT BERLIN WS09/10
Fakultät II – Institut für Mathematik
Dozent: Tobias Finis
Assistent: Gerriet Möhlmann
www.math.tu-berlin.de/~kant/kryptows09

12. Übung Kryptographie

1. Aufgabe

Zeigt, dass für alle $\alpha, \beta > 0$

$$\lim_{n\to\infty} \frac{L(n)^\alpha}{n^\beta} = 0$$

gilt.

(3 Punkte)

2. Aufgabe

Werden die in der Übung beschriebenen Schnorr Signaturen unvorsichtig benutzt, so bietet das Möglichkeiten für Angriffe.

(a) Beschreibt, wie man den geheimen Schlüssel x berechnen kann, wenn man eine unterschriebene Nachricht (M, σ) hat und das zum Signieren verwendete k kennt.

(b) Beschreibt, wie man den geheimen Schlüssel x berechnen kann, wenn man zwei unterschriebene Nachrichten hat, bei denen das selbe k zum signieren verwendet wurde.

(5 Punkte)

3. Aufgabe

Gebt eine Möglichkeit an, die Faktorbasis $S = \{p \in \mathbb{P} \,|\, p \leq B\}$ mit der Laufzeit $O(B \log(B))$ zu berechnen und begründet, wie diese Laufzeit zustande kommt.

(5 Punkte)

4. Aufgabe

Alice schickt an Bob eine Mail, in der festgehalten wird, daß Bob das Auto von Alice für 1000 Euro kaufen möchte. Die Mail enthält einen Header. Alice hat herausbekommen, daß dieser Header noch aus alten Zeiten stammt. Mail-Programme die heutzutage in Gebrauch sind benutzen diesen Header nicht mehr. Wohl aus Bequemlichkeit hat man diesen nicht entfernt. In einer zweiten fingierten Mail schreibt Alice, daß der Verkaufspreis 10000 Euro beträgt statt 1000. Nun versucht Alice, die fingierte Nachricht im Header so abzuändern, daß sie den gleichen Hashwert hat wie die ursprüngliche Nachricht.

In der Datei AliceMail.k ist eine Hashfunktion SHA1Light vorgegeben, welche beliebige Strings auf Hexadezimalstrings der Länge 7 abbildet. Es gibt zwei Mails, eine Original-Mail und eine Fälschung. Modifiziert die Header so, dass ihr eine Original-Mail und eine Fälschung mit gleichem Hashwert bekommt.

(7 Punkte)