Dr. Dirk Frettlöh 23.5.2022

Übungen zur Vorlesung Kryptographie

Blatt 7

Aufgabe 25: (Wiener-Angriff auf RSA)
Führen Sie einen Wiener-Angriff auf folgende Situation durch: Es ist $N = 64741$, $e = 42667$ und d ist fahrlässigerweise klein. Berechnen Sie mittels Satz 3.1 Kandidaten für d. Probieren Sie diese Kandidaten nacheinander aus zum Entschlüsseln der verschlüsselten Botschaft

$$c = (1973, 3145, 0, 29872, 15544, 1973, 17819, 3145, 39054, 63700, 3145)$$

Dabei ist im Klartext a=0, b=1, c=2 ... z=25.
(Ihr Lösungsweg soll ein Wiener-Angriff sein. Andere Wege der Entschlüsselung sind hier möglich, zählen aber nicht als korrekte Lösung).

Aufgabe 26: (Diffie-Hellman)
In einem Diffie-Hellman-Schlüsseltausch sind $p = 17$ und $g = 3$ die öffentlichen Informationen. Eve erfährt, das Alice $6 \equiv g^a \bmod p$ an Bob gesendet hat, und Bob hat $7 \equiv g^b \bmod p$ an Alice gesendet. Was ist Alice geheimer Exponent a? Was ist Bobs geheimer Exponent b? Was ist der gemeinsame Schlüssel $g^{ab} \bmod p$?

Aufgabe 27: (Diskrete Logarithmen)
(a) Berechnen Sie mit dem Baby-Step-Giant-Step-Algorithmus die diskreten Logarithmen $\log_7(3) \bmod 71$ und $\log_2(19) \bmod 25$. Zeigen Sie Ihre Berechnung.
Sie dürfen davon ausgehen, dass 7 ein Erzeuger von Z_{71}^* ist, und 2 ein Erzeuger von Z_{25}^*.

(b) Finden Sie drei Primzahlen $a, b, n \in \mathbb{N}$ mit $1 < a < n$, so dass $\mathrm{dlog}_a(b)$ modulo n nicht existiert.

(c) Finden Sie drei Primzahlen $a, b, n \in \mathbb{N}$ mit $1 < a < n$, so dass $\mathrm{dlog}_a(b)$ modulo n mindestens zwei verschiedene Werte hat.

Aufgabe 28: (Kettenbrüche)
Ein Kettenbruch ist ein geschachtelter Bruch der Form

$$a_0 + \cfrac{1}{a_1 + \frac{1}{a_2 + \frac{1}{a_3 + \cdots}}}.$$

Jedes $x \in \mathbb{R}^+$ hat eine (im Wes.) eindeutige Darstellung als Kettenbruch. Die berechnet man wie folgt: Falls $x \notin \mathbb{N}$, schreibe $x = a_1 + \frac{1}{x_1}$, wobei $a_1 = \lfloor x \rfloor$ und $x_1 > 1$. Falls $x_1 \notin \mathbb{N}$, schreibe $x_2 = a_2 + \frac{1}{x_2}$, wobei $a_2 = \lfloor x_1 \rfloor$ und $x_2 > 1$ usw, solange bis ein $x_i \in \mathbb{N}$. So ist z.B.

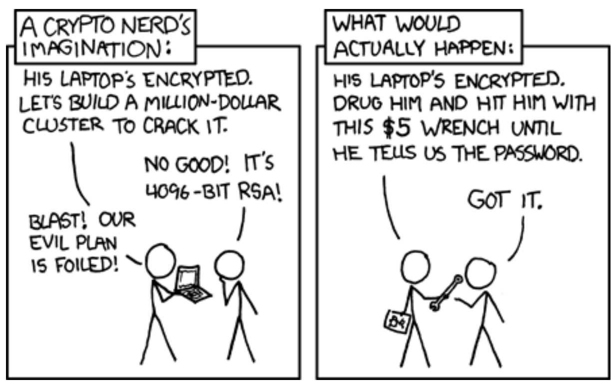
$$\frac{15}{11} = 1 + \cfrac{1}{2 + \frac{1}{1 + \frac{1}{3}}}.$$

Die *rationalen Approximanten* von x sind die gekappten und vereinfachten Kettenbrüche aus den Zwischenschritten (wähle ein +, setze den Zähler dahinter auf 0 und vereinfache den Ausdruck zu einem möglichst einfachen Bruch). Z.B. ist der nullte rationale Approximant von $\frac{15}{11}$ gleich 1, der erste ist $1 + \frac{1}{2} = \frac{3}{2}$, der zweite ist $1 + \frac{1}{2+\frac{1}{1}} = \frac{4}{3}$, und alle weiteren sind $\frac{15}{11}$.

(a) Berechnen Sie den Kettenbruch von $\frac{127}{105}$ und alle rationalen Approximanten.

(b) Wenden Sie den erweiterten euklidischen Algorithmus auf 127 und 105 an. Beschreiben Sie in einem Satz die Ähnlichkeiten zwischen den Teilen (a) und (b).

(c*) Berechnen Sie den Kettenbruch von $x = 1 + \sqrt{2}$.



Quelle xkcd.com

Abgabe bis Montag 30.5.2022 bis 14 Uhr per Email an Ihren Tutor.
Bitte auf jeder Abgabe das Tutorium angeben. Bitte die Abgaben so nennen:
techfakaccount-bl$n$.pdf, also z.B. `dfrettloeh-bl7.pdf`, oder `dfrettloeh+mnebel-bl7.pdf`.

Jan-Philipp Brünger jbruenger@techfak.de
Simon Hahm shahm+krypto@techfak.de
Tim Lakämper tlakaemper+krypto@techfak.de