Dr. Dirk Frettlöh 17.5.2023

Übungen zur Vorlesung Kryptographie

Blatt 7

Aufgabe 25: (RSA knacken mit Wienern)
Führen Sie einen Wiener-Angriff auf folgende Situation durch: Es ist $N = 1005973$, $e = 602381$ und d ist fahrlässigerweise klein. Berechnen Sie mittels Satz 5.1 im Skript Kandidaten für d. Probieren Sie diese Kandidaten nacheinander aus zum Entschlüsseln der verschlüsselten Botschaft

$$c = (1, 551462, 777258, 737805, 16238, 876283, 614316, 453832, 293606)$$

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 $(Z_N^*, \cdot \bmod N)$)
(a) In einem Diffie-Hellman-Schlüsseltausch sind $G = Z_{29}^*$ und $g = 3$ die öffentlichen Informationen. Eve erfährt, das Alice $9 \equiv g^a \bmod 29$ an Bob gesendet hat, und Bob hat $6 \equiv g^b \bmod 29$ an Alice gesendet. Was ist Alice' geheimer Exponent a? Was ist Bobs geheimer Exponent b? Was ist der gemeinsame Schlüssel $g^{ab} \bmod 29$?

(b) Berechnen Sie $\mathrm{dlog}_5(4)$ und $\mathrm{dlog}_5(8)$ in Z_{29}^* (falls möglich).

(c) Warum nehmen Alice und Bob in (a) nicht $g = 5$?

Aufgabe 27: (Geburtstagsparadox)
(a) Berechnen Sie $\mathrm{dlog}_7(20) \bmod 79$ mit dem Geburtstagsangriff-Algorithmus.

(b) Sie lösen nun das Geburtstagsparadox für Tage im Monat. Ab welcher Anzahl n von versammelten Personen ist die Wahrscheinlichkeit größer als 50%, dass mindestens zwei Personen am gleichen Tag $i \in \{1, 2, \ldots, 31\}$ im Monat Geburtstag haben? *(Wir nehmen der Einfachheit halber an, dass jeder der 31 Tage im Monat gleich wahrscheinlich ist. Diese Annahme ist unrealistisch, liefert aber dennoch einen recht genauen Wert.)*

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

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

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.

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

Fortsetzung auf Seite 2

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 $\frac{61}{37}$ und alle rationalen Approximanten von Hand.

(b) Wenden Sie den erweiterten euklidischen Algorithmus auf 61 und 37 an. Beschreiben Sie in einem Satz die Ähnlichkeiten zwischen den Teilen (a) und (b).

(c) Berechnen Sie den Kettenbruch von $x = \frac{1+\sqrt{5}}{2}$ (irgendwie, z.B. mit sagemath, oder einem onlinetool, oder...) und die ersten sechs rationalen Approximanten.

Abgabe bis Dienstag 23.5.2023 bis 23:59 Uhr per Email an den Tutor.
Bitte auf jeder Abgabe das Tutorium angeben!

Jakob Niermann janiermann+krypto@techfak.de
Tim Lakämper tlakaemper+krypto@techfak.de