Dr. Dirk Frettlöh 27.5.2026

Übungen zur Vorlesung Kryptographie

Blatt 7

Aufgabe 25: (Wiener-Angriff auf RSA)
Führen Sie einen Wiener-Angriff auf folgende Situation durch: Es ist $N = 1005973$, $e = 602381$ 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

$$c = (750267, 0, 644542, 1, 876283, 614316, 498350, 961198, 614316)$$

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 klein und in dumm)
(a) In einem Diffie-Hellman-Schlüsseltausch sind $G = Z_{23}^*$ und $g = 5$ die öffentlichen Informationen. Eve erfährt, dass Alice $17 \equiv g^a \bmod p$ an Bob gesendet hat, und Bob hat $10 \equiv g^b \bmod p$ an Alice gesendet. Was ist Alice geheimer Exponent a? Was ist Bobs geheimer Exponent b? Was ist der gemeinsame Schlüssel $g^{ab} \bmod p$?

(b) Waum ist es keine gute Idee, wenn Alice und Bob sich beim Diffie-Hellman-Schlüsseltausch auf $G = (Z_p, + \bmod p)$ für ein großes p (z.B. $p \approx 2^{4096}$) einigen?

Aufgabe 27: (Riesenschritte)
Berechnen Sie mit dem Baby-Step-Giant-Step-Algorithmus die diskreten Logarithmen $\log_7(5) \bmod 71$ und $\log_2(13) \bmod 25$. Zeigen Sie Ihre Berechnung.
Sie dürfen davon ausgehen, dass 7 ein Erzeuger von Z_{71}^* ist, und 2 ein Erzeuger von Z_{25}^*.

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 $x_1 = a_2 + \frac{1}{x_2}$, 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 $\frac{32}{23}$ und alle rationalen Approximanten von Hand. Tun Sie das auch für $\frac{90}{67}$.

(b) Wenden Sie den erweiterten euklidischen Algorithmus auf 32 und 23 an, und auf 90 und 67. Beschreiben Sie in einem Satz die Ähnlichkeiten zwischen den Teilen (a) und (b).

Nur für den Spaß, ohne Punkte: 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 Mittwoch 3.6.2026 bis 12:00 Uhr per Email an die Tutorin.

Lisa Henetmayr Mi 12 Uhr in S0-115 lhenetmayr+krypto@techfak.de
Lisa Henetmayr Mi 16 Uhr in U2-147 lhenetmayr+krypto@techfak.de