Vorlesung „Kryptographie I“ (Wintersemester 2024/2025)

Übungsblatt 8 (6.12.2024)

Bemerkungen:

(1) Zur Lösung einer Kryptographie-Aufgabe gehört auch eine (kurze) Darstellung des Lösungswegs.
(2) Mit **P** werden Präsenzaufgaben, mit **H** Hausaufgaben bezeichnet.
(3) Abgabe der Hausaufgaben bis Freitag, 13.12.2024 in den Übungskästen (bis 10:00 Uhr), in Übungsgruppe 1 oder digital (bis 14:00 Uhr).

Präsenzaufgaben

Aufgabe P29: Jeder rationalen Zahl κ ordnen wir auf folgende Weise ein Vigenère-Schlüsselwort zu: Wir bilden die Kettenbruchentwicklung $[k_1, k_2, \ldots, k_n]$ von κ und bestimmen das der Folge ($k_1 \bmod 26, k_2 \bmod 26, \ldots, k_n \bmod 26$) entsprechende Wort (nach Identifikation von A mit 0, B mit 1, ..., Z mit 25).

(1) Bestimme eine rationale Zahl, die nach obigem Verfahren das Schlüsselwort NACHT liefert. (Beachte, dass in der Kettenbruchentwicklung $[k_1, \ldots, k_n]$ die Zahlen $k_2, \ldots, k_n$ aus $\mathbb{N}$ sind.)
(2) Entschlüssle folgenden Vigenère-chiffrierten Text:

`OGVCU JUY CFYFOV`

(Hinweis: `XRGGRAOEHPUIBARVAHAQQERVFFVTXBZZNIVRERVAF`)

Aufgabe P30: $(N, e) = (57174151, 3291863)$ ist ein öffentlicher RSA-Schlüssel. Der private Exponent d kommt im 5. Näherungsbruch von $\frac{e}{N}$ vor.

(1) Bestimme den 0., 1., 2., 3., 4., und 5. Näherungsbruch von $\frac{e}{N}$.
(2) Bestimme den privaten Exponenten d.
(3) Bestimme $\varphi(N)$.

Aufgabe P31: Die Kettenbruchentwicklung einer Zahl $\alpha \in \mathbb{R} \setminus \mathbb{Q}$ wird beginnend mit $\alpha_0 = \alpha$ rekursiv durch $a_i = \lfloor \alpha_i \rfloor$, $\alpha_{i+1} = \frac{1}{\alpha_i - a_i}$ definiert. Dann ist $\alpha = [a_0, a_1, \ldots, a_{i-1}, \alpha_i]$ für alle $i \geq 0$. Bestimme die Kettenbruchentwicklungen folgender Zahlen:

(1) $\sqrt{7}$
(2) $\sqrt{n^2 + 1}$ für $n \in \mathbb{N}$

(Hinweis: $\frac{1}{a+b\sqrt{d}} = \frac{a-b\sqrt{d}}{(a+b\sqrt{d})(a-b\sqrt{d})} = \frac{a-b\sqrt{d}}{a^2-b^2d}$)

Aufgabe P32: Sei $a = 9734$ und $b = 5031$. Bestimme die Näherungsbrüche für $\frac{a}{b}$ und führe den erweiterten euklidischen Algorithmus für a, b durch. Fällt etwas auf?

Datei: ki_u8.tex. Version vom 6.12.2024

Hausaufgaben

Aufgabe H29:

(1) Bestimme für

$$\alpha = \frac{31415}{10000}$$

die Kettenbruchentwicklung, die Näherungsbrüche $\frac{p_n}{q_n}$ und (numerisch) $q_n^2\left(\alpha - \frac{p_n}{q_n}\right)$.

(2) Bestimme die Kettenbruchentwicklungen von

$$\frac{10283}{2000}, \quad \frac{2000}{10283}, \quad -\frac{10283}{2000}, \quad -\frac{2000}{10283}.$$

Aufgabe H30: $N = 4205699657$ hat die Primfaktorzerlegung $N = pq$ mit $p = 56311$, $q = 74687$. Folgende Werte für e wurden so gewählt, dass $\mathrm{ggT}(e, (p-1)(q-1)) = 1$ gilt:

$$e = 7, \quad e = 841113733, \quad e = 3911015213, \quad e = 3973765663.$$

Führe für jedes e folgende Aufgaben durch:

(1) Bestimme $d \in \mathbb{N}$ (minimal) mit $ed \equiv 1 \bmod (p-1)(q-1)$ und berechne $k = \frac{ed-1}{(p-1)(q-1)}$.

(2) Berechne die Kettenbruchentwicklungen von

$$\frac{k}{d}, \quad \frac{e}{(p-1)(q-1)}, \quad \frac{e}{N - \left\lfloor \sqrt{4N} \right\rfloor}, \quad \frac{e}{N}.$$

(3) Ist $\frac{k}{d}$ Näherungsbruch in der Kettenbruchentwicklung von $\frac{e}{(p-1)(q-1)}$, $\frac{e}{N-\left\lfloor\sqrt{4N}\right\rfloor}$ oder $\frac{e}{N}$?

Aufgabe H31: Durch folgende Zahlen N und e wird ein RSA-Schlüssel definiert, wobei N 2048 Bits bzw. 617 Dezimalstellen hat:

$N = 27793442438916324852073769571629621363906987250713032009311166214648011023373939$
$00349896428440919988448071338513598636117653306425983609615718270151276116277443$
$85914603447497303637508967511421054633704659735456862031368690582096816227677175$
$58658348368914922970584283955915965076793780454197437867142839078375951616760128$
$78561721425871542103489105242277952687532622415360903933047874306416858648020029$
$31778077286254710684156030091755578470550077902253817823256469059583121927233143$
$67113063490919001863449037147248487314574466503923962127426615442672910168649857$
$97299490053599827580524052076274670113924143771919622738 7,$

$e = 10873793345355951700226688052530453374808239853947122559096444993754553541938268$
$82364679791905521323136434652086654967200373530442587812849024827834624457951725$
$57334503451615427826974790007022950924985709935043674599148110370133846821018540$
$80366444844048201061376516723163100028779272502520534391519593286398692160767459$
$90266409917592005938551217340461191413594786835922139897690069331364154189711078$
$75407291059564597873571780455246662929694852363810410406780169621401217970602209$
$56647849600187797008925896785087105764155543360404627681208974303988154271866449$
$36350268678875348953969753415934019706956433602163753908 9$

In einem aus Großbuchstaben und Leerzeichen bestehenden Text wurde jedes Leerzeichen durch 00, jedes A durch 01, jedes B durch 02, ..., jedes Z durch 26 ersetzt, wodurch eine Zahl a entstand. Dann wurde $b = a^e \bmod N$ berechnet mit folgendem Ergebnis:

$$\begin{aligned} b = {} & 232815202330975209083355299884906582809348752355691049940747494355133278221454332952707562840478763263616113838142550791272545389690036185841398345984842700155912541658172645188215697634637805779049238710024409613799456654715152171176106923303236131711302044556331385802025335186852891121998725497012162900077137157286790035826509727154924046804013339669520939040118786212669740273692940158352774979387368542298177916847017151019809263484423747979475609072550013788923199046329687490159518938303082151307755978061201938351622753365884987348563205416230058879436033807291206665901700163172263392729938871803773444721057.\end{aligned}$$

Entschlüssle den Text. (Hinweis: Der private Exponent d wurde verhältnismäßig kurz gewählt.)

Aufgabe H32: Erich findet folgende Zahlen:

$$\begin{aligned} p &= 84658768563874658679475986475932487563284653846583648756240 3 \\ q &= 75023454569817987569874395776532504568798793450134564564603 7 \\ d_p &= 71866364500703461570928895610144315624697170027630723330403 7 \\ d_q &= 74843728882535056949790011686065812422113693268990003070537 \\ p_{\text{inv}} &= 50884305672965746764701697691665233077939812605521233825259 6 \\ b &= 42320853756564626327772395961586425690367923687434481102834577308860888785603720056522830136058149536373351427785962875 7\end{aligned}$$

Das Tupel $(p, q, d_p, d_q, p_{\text{inv}})$ könnte ein privater CRT-RSA-Schlüssel sein, b ein Chiffretext. Erich versucht unter dieser Annahme b zu entschlüsseln. Was erhält er? Kann Erich den zugehörigen öffentlichen RSA-Schlüssel (N, e) bestimmen?