Vorlesung „Kryptographie I“ (Wintersemester 2024/2025)

Übungsblatt 7 (29.11.2024)

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, 6.12.2024 in den Übungskästen (bis 10:00 Uhr), in Übungsgruppe 1 oder digital (bis 14:00 Uhr).

Präsenzaufgaben

Aufgabe P25: Alina (A), Benjamin (B) und Caroline (C) haben folgende öffentlichen RSA-Schlüssel:

$$(N_A, e_A) = (237612877, 3), \quad (N_B, e_B) = (229803979, 3), \quad (N_C, e_C) = (245174341, 3).$$

Katharina schickt ein Datum in Gestalt einer 8-stelligen Zahl RSA-verschlüsselt an Alina, Benjamin und Caroline mit folgendem Ergebnis:

$$b_A = 186468158, \quad b_B = 60086833, \quad b_C = 45574821.$$

Bestimme das Datum ohne die RSA-Zahlen N_A, N_B, N_C zu faktorisieren. (Die Benutzung von SAGE oder WolframAlpha ist erlaubt.)

Aufgabe P26: Sei $N = pq$ eine RSA-Zahl mit $p, q > 3$, $(N, 3)$ ein öffentlicher RSA-Schlüssel und (N, d) ein zugehöriger privater RSA-Schlüssel, d.h. $3d \equiv 1 \bmod (p-1)(q-1)$ mit $0 \leq d \leq (p-1)(q-1) - 1$. Dann gibt es ein $k \in \mathbb{N}$ mit

$$3d = 1 + k(p-1)(q-1).$$

(1) Zeige, dass $k = 2$ gilt.
(2) Wie kann man in obiger Situation $s = p + q$ berechnen, wenn man N und d kennt?
(3) Wie kann man N faktorisieren, wenn man in obiger Situation N und d kennt?
(4) $N = 2448555667$ ist eine RSA-Zahl, $(N, 3)$ ein öffentlicher RSA-Schlüssel, $(N, 1632303371)$ ein zugehöriger privater RSA-Schlüssel. Faktorisiere N.

Aufgabe P27: Für $N \in \mathbb{N}$ sei $Q_N = \{a \in \mathbb{Z} : 0 \leq a \leq N-1, a^2 \equiv 1 \bmod N\}$ die Menge der Quadratwurzeln von 1 modulo N.

(1) $N = 11592649$ hat die Primfaktorzerlegung $N = pq$ mit $p = 2713$ und $q = 4273$. Bestimme Q_N.
(2) $N = 1160010391$ ist eine RSA-Zahl mit

$$Q_N = \{1, 142527894, 1017482497, 1160010390\}.$$

Bestimme die Primfaktorzerlegung von N mit Hilfe von Q_N.
(3) Die Zahl

$$\begin{aligned} N \;=\; & 347156464658270569858558793792151826036888542387766770987681 \\ & 176168893774839351550902872683975950054858570217423157946961 \end{aligned}$$

ist eine 120-stellige RSA-Zahl. Versuche die Primfaktorzerlegung von N mit einem Faktorisierungsverfahren zu bestimmen. Wenn dies nicht funktioniert, benutze, dass

$$\begin{aligned}\alpha &= 966627861061099020744989145848575231837720549209910547136674\\ &\quad 381107575738746731389375817079350507324546033590751851001 78\end{aligned}$$

ein Element von Q_N ist.

Aufgabe P28: Für eine RSA-Zahl N sei

$$E_N = \{a \in \mathbb{Z} : 0 \le a \le N-1, \mathrm{ggT}(N,a) = 1\} \text{ und } Q_N = \{a \in \mathbb{Z} : 0 \le a \le N-1, a^2 \equiv 1 \bmod N\}.$$

Q_N hat vier Elemente, darunter 1 und $N-1$. Ist $w \in Q_N$, so auch $N-w$. Kennt man ein $m \in \mathbb{N}$ mit $a^m \equiv 1 \bmod N$ für alle $a \in E_N$, zerlegt man $m = 2^\ell u$ mit $u \equiv 1 \bmod 2$, so erhält man eine Abbildung

$$\omega_{N,m} : E_N \to Q_N$$

wie folgt:

$$\omega_{N,m}(a) = \begin{cases} 1, & \text{falls } a^u \equiv 1 \bmod N, \\ (a^{2^i u} \bmod N), & \text{falls } a^{2^i u} \not\equiv 1 \bmod N \text{ und } a^{2^{i+1}u} \equiv 1 \bmod N \text{ für ein } i \in \{0,\dots,\ell-1\}. \end{cases}$$

Die vorangegangenen Aussagen sind aus der Vorlesung bekannt.

(1) Für $N = 15$ ist $m = 8$ ein Exponent (der Gruppe $(\mathbb{Z}/N\mathbb{Z})^*$). Berechne für jedes $a \in E_N$ die Zahlen $a^{2^i u} \bmod N$ für $i = 0,\dots,\ell$ und bestimme damit $\omega_{N,m}(a)$. Was ist Q_N?

(2) Für $N = 119$ ist $m = 96$ ein Exponent (der Gruppe $(\mathbb{Z}/N\mathbb{Z})^*$). Berechne für $a \in \{3, 18, 33, 103\}$ die Zahlen $a^{2^i u} \bmod N$ für $i = 0,\dots,\ell$ und bestimme damit $\omega_{N,m}(a)$. Was ist Q_N?

(3) Für

$$\begin{aligned}N &= 403997166555898946808412558351213447188430457458845131464193\\ &\quad 1438818197170235047615565536855297050610997888166398772052 49\end{aligned}$$

ist

$$\begin{aligned}m &= 336664305463249122340343798626011205990358714549037609553493\\ &\quad 2186850383843352083520873518477661409550967724516889725162 0\end{aligned}$$

ein Exponent (der Gruppe $(\mathbb{Z}/N\mathbb{Z})^*$). Berechne einige Werte $\omega_{N,m}(a)$ und faktorisiere damit N.

Hausaufgaben

Aufgabe H25: Felix wandelt einen aus Großbuchstaben und Leerzeichen bestehenden Text in eine Dezimalzahl a um, indem er A durch 01, B durch 02, C durch 03, ..., Z durch 26 und jedes Leerzeichen durch 00 ersetzt. Er besorgt sich die RSA-Schlüssel $(N_A, 3)$, $(N_B, 3)$, $(N_C, 3)$ von Anne, Birgit und Claudia, berechnet damit

$$b_A = a^3 \bmod N_A, \quad b_B = a^3 \bmod N_B, \quad b_C = a^3 \bmod N_C$$

und schickt b_A an Anne, b_B an Birgit und b_C an Claudia. Eva kommt an die Zahlen:

$$\begin{aligned}
N_A &= 52463417394738094002929343637795999943948280785964776868637210626725120477593860\\
&\quad 20786297015879534836460893861103167116747145743701594880516561889020935066694216\\
&\quad 96731467410475603174792837908526486254722167183181621898916874195275438701676279\\
N_B &= 39385953856283941822498157237506385805750291442880520694654267898773343002547554\\
&\quad 30554493345144843341474181507823408666392803119213808852769189174300906747343640\\
&\quad 19142426730542941272496775847511671884010245953343786330925565401241232488426459\\
N_C &= 95500291166696596452362948944098653933392696650792832629775289400526575857331675\\
&\quad 23941223260150128333044948838115270399460457336956257805557665125996964772076708\\
&\quad 99156129266442329417364494388911456190725589847190545882053729371666583647269301\\
b_A &= 75071872098615045914459987607081102319443866347101684807648695601220506384355493\\
&\quad 42127132291640735065455431242955898986112798187930050258144455008888675823408401\\
&\quad 09641020658276150581653456766504615972646231647510047668412884259389092922949 49\\
b_B &= 25298058357223393999135111784142107097600680709072715135218853195278586720322004\\
&\quad 44235667872279335230366045644855055774320306412684203458367168366892095461272713\\
&\quad 75709471428964994889900167837006721349671745167655403743754359020817108648609581\\
b_C &= 36900219272239270901602039584777883226249039782223650598547657996616349350511511\\
&\quad 23130405010872824467196599317835937719360535430706640662423777708157775674728946\\
&\quad 72398102567704586075801594928805138200567587638869155414883883889228430140112402
\end{aligned}$$

Kann Eva herausfinden, was Felix mitteilen wollte?

Aufgabe H26: Bestimme die Primfaktorzerlegungen folgender RSA-Zahlen N_i, für die sowohl ein öffentlicher RSA-Schlüssel (N_i, e_i) als auch ein zugehöriger privater RSA-Schlüssel (N_i, d_i) bekannt sind:

$$\begin{aligned}
N_1 &= 85493647480339103586801033480045750938242141287989759167663300996928199827746934\\
&\quad 63724742575127802591161320277127956904292441418397125788411111499653067279,\\
e_1 &= 65537,\\
d_1 &= 71197526468742047935676439343789569170199728202632178400792340842735360028665776\\
&\quad 71478848484826744122293769584813319687406737029894002043739281740475222033,\\
N_2 &= 69755854809551498906861078246289603130291378813015556142725303224669830833805843\\
&\quad 18175744376992532819082091858731020258122724760098420682313980900653717117,\\
e_2 &= 52017534594873350473443874636186088297429275206435996823762935542743309773000991\\
&\quad 13213273767171698040950040100356327328759773831802812238031258978726813251,\\
d_2 &= 43554620027858869000247309423411876594852719416758796478468328347080533778942574\\
&\quad 79707473609571342058939594741476803598929492162782649643454367374482381451.
\end{aligned}$$

Aufgabe H27: Zu vorgegebenen Zahlen $n \in \mathbb{N}_{\geq 2}$ und $k \in \mathbb{N}_{\geq 2}$ werden rekursiv Folgen natürlicher Zahlen $(L_i)_{i\geq 0}$ und $(R_i)_{i\geq 0}$ durch

$$L_0 = 1, \quad R_0 = n \quad \text{und} \quad \begin{cases} L_i = \left\lfloor \frac{L_{i-1}+R_{i-1}}{2} \right\rfloor \text{ und } R_i = R_{i-1}, & \text{falls } \left\lfloor \frac{L_{i-1}+R_{i-1}}{2} \right\rfloor^k \leq n, \\ L_i = L_{i-1} \text{ und } R_i = \left\lfloor \frac{L_{i-1}+R_{i-1}}{2} \right\rfloor, & \text{falls } \left\lfloor \frac{L_{i-1}+R_{i-1}}{2} \right\rfloor^k > n \end{cases}$$

definiert. Zeige:

(1) Für alle i gilt $L_i^k \leq n < R_i^k$.
(2) Für $i \geq 1$ gilt
$$R_i - L_i \leq \frac{R_{i-1} - L_{i-1}}{2} + \frac{1}{2}.$$
(3) Für $i \geq 0$ gilt
$$R_i - L_i \leq \frac{n}{2^i} + (1 - \frac{2}{2^i}).$$
(4) Für $i \geq 0$ gilt
$$1 \leq R_i - L_i < \frac{n}{2^i} + 1.$$
(5) Im Fall $R_i - L_i = 1$ gilt
$$L_i = \left\lfloor \sqrt[k]{n} \right\rfloor.$$
(6) Gilt $R_i - L_i = 1$, so $R_j - L_j = 1$, und damit $L_j = \lfloor \sqrt[k]{n} \rfloor$ für alle $j \geq i$.
(7) Für $i \geq \frac{\ln n}{\ln 2}$ gilt $L_i = \lfloor \sqrt[k]{n} \rfloor$.

(Die Aufgabe zeigt, dass der im Vorlesungsskript angegebene Algorithmus zur Berechnung von $\lfloor \sqrt[k]{n} \rfloor$ funktioniert, und liefert eine Schrittzahlabschätzung.)

Aufgabe H28: Sei $f : \mathbb{N} \to \mathbb{N}$ definiert durch

$$f(n) = \mathrm{ggT}(n, \lfloor \sqrt{n} \rfloor ! \bmod n).$$

Zeige:

(1) Es gilt $\mathrm{ggT}(n, \lfloor \sqrt{n} \rfloor !) = \mathrm{ggT}(n, \lfloor \sqrt{n} \rfloor ! \bmod n)$.
(2) $f(n) \mid n$.
(3) Ist p ein Primteiler von n mit $p \leq \sqrt{n}$, so gilt $p \mid f(n)$.
(4) Ist p ein Primteiler von n mit $p > \sqrt{n}$, so gilt $p \nmid f(n)$.
(5) Eine natürliche Zahl $n \geq 2$ ist genau dann eine Primzahl, wenn $f(n) = 1$ gilt.
(6) Ist $N = pq$ eine RSA-Zahl mit $p < q$, so gilt $f(N) = p$.

Ganz im Unterschied zu $a^m \bmod n$ kennt man kein Verfahren um $m! \bmod n$ schnell zu berechnen. Könnte man $m! \bmod n$ schnell berechnen, so könnte man $f(n)$ schnell berechnen und mit (5) hätte man einen schnellen Primzahlbeweis und mit (6) eine schnelle Faktorisierungsmethode für RSA-Zahlen. (RSA-Zahlen sind ungerade natürliche Zahlen mit genau zwei verschiedenen Primteilern.)