Vorlesung „Kryptographie II“ (Sommersemester 2025)

Übungsblatt 4 (16.5.2025)

Aufgabe 16: Ein aus Großbuchstaben und Leerzeichen bestehender Text wurde in Blöcke der Länge 40 eingeteilt. Jeder Block entspricht einer Zahl a_i, wenn man jedes A durch 01, jedes B durch 02, ..., jedes Z durch 26 und jedes Leerzeichen durch 00 ersetzt. Die Folge a_i wurde dann mit der RSA-Zahl

$$N = 45296708982568201895712552159687783189209235840286783031044427350196711746533901$$

zur Folge $b_i = a_i^2 \bmod N$ Rabin-verschlüsselt mit folgenden Zahlenwerten:

`113632651332969232852068894517195715567082991774078098060543477348124587081095 81,`
`405356226960378109164648500121762847232376142256783074278934783622725242512133,`
`191579366125027356446957239296855957288741270843890411634972390476141377743900 81.`

Entschlüssle den Text. (Hinweis: `CVFGMJRVDCYHFRVAF`)

Aufgabe 17:

(1) Seien N_1 und N_2 teilerfremde natürliche Zahlen und $b_1, b_2 \in \mathbb{Z}$ mit $0 \le b_2 \le N_2 - 1$. Zeige: Berechnet man $x, y, z \in \mathbb{Z}$ mit

$$x \cdot N_2 \equiv 1 \bmod N_1, \quad y = x(b_1 - b_2) \bmod N_1, \quad z = b_2 + yN_2,$$

so gilt

$$z \equiv \begin{cases} b_1 \bmod N_1, \\ b_2 \bmod N_2 \end{cases} \qquad \text{und} \quad 0 \le z \le N_1 N_2 - 1.$$

(Dies ist eine Variante des chinesischen Restsatzes.)

(2) Seien N_1 und N_2 teilerfremde natürliche Zahlen, $a \in \mathbb{Z}$ mit $0 \le a \le \min(N_1, N_2) - 1$ und $b_1 = a^2 \bmod N_1$ und $b_2 = a^2 \bmod N_2$. Zeige: Bestimmt man $z \in \mathbb{Z}$ mit

$$z \equiv \begin{cases} b_1 \bmod N_1, \\ b_2 \bmod N_2 \end{cases} \qquad \text{und} \quad 0 \le z \le N_1 N_2 - 1,$$

so gilt $z = a^2$, d.h. $a = \sqrt{z}$ ist einfach die Wurzel aus z (in $\mathbb{R}$).

(3) Die öffentlichen Rabin-Schlüssel von Georg und Ludwig sind

$$N_G = 848753097602236237326299773276917876698794936188427041342445208038472803714394 33,$$
$$N_L = 543018119220432962351083535041103162189073829406564269049320237172678571977124 01$$

Werner hat einen Goethe-Spruch gefunden, der ihm gefällt, und schickt ihn Rabin-verschlüsselt an Georg und Ludwig. (Dabei wurde der aus Großbuchstaben und Leerzeichen bestehende Text in eine Zahl a umgewandelt, indem jedes Leerzeichen durch 00, jedes A durch 01, ..., jedes Z durch 26 ersetzt wurde. Dann wurde $b_G = a^2 \bmod N_G$ und $b_L = a^2 \bmod N_L$ berechnet.) Es ist

$$b_G = 817048114936368489476851741512543317694261410968239248314679854073157823641931 90,$$
$$b_L = 333854515293879577219939975886959983502097253151490464394319579306738760294168 43.$$

Um welchen Spruch handelt es sich?

Datei: kii_u4.tex. Version vom 14.5.2025

Aufgabe 18: Die nachfolgenden Zahlen N und d sind so beschaffen, dass N eine RSA-Zahl ist, und dass die Funktion $w(a) = a^d \bmod N$ in mehr als 5% der Fälle eine Quadratwurzel von a modulo N liefert:

$$\begin{aligned} N &= 1109140664036518268726058363690328248088359723645654069288670275238531761535293459055022071796921569, \\ d &= 346606457511411958976893238653227577527612413639239837386310855344728435450185168727057873051110 66. \end{aligned}$$

(1) Faktorisiere N.

(2) Zeige, dass $w(a)$ für $a \in \mathbb{Z}$ mit $\mathrm{ggT}(N, a) = 1$ genau dann eine Quadratwurzel von a modulo N ist, wenn $\overline{a} \in G$ gilt mit

$$G = \{\overline{a} \in (\mathbb{Z}/N\mathbb{Z})^* : a^{2d-1} \equiv 1 \bmod N\}.$$

(3) In welcher Beziehung stehen d und $\varphi(N)$?

Aufgabe 19: Sei n eine ungerade natürliche Zahl, $\left(\frac{a}{n}\right)$ das Jacobi-Symbol und $\varphi(n)$ die Eulersche φ-Funktion. Zeige:

(1) Ist n keine Quadratzahl, so gibt es ein $u \in \mathbb{Z}$ mit $\left(\frac{u}{n}\right) = -1$. (Hinweis: Betrachte die Primfaktorzerlegung von n und verwende den chinesischen Restsatz.)

(2) Ist n eine Quadratzahl, so gilt für $a \in \mathbb{Z}$

$$\left(\frac{a}{n}\right) = \begin{cases} 1, & \text{falls } \mathrm{ggT}(n, a) = 1, \\ 0, & \text{falls } \mathrm{ggT}(n, a) > 1. \end{cases}$$

(3) Ist $c \in \mathbb{Z}$ mit $\mathrm{ggT}(n, c) = 1$, so gilt

$$\{a : 0 \le a \le n-1\} = \{(ca \bmod n) : 0 \le a \le n-1\}.$$

(4) Es ist

$$\sum_{0 \le a \le n-1} \left(\frac{a}{n}\right) = \begin{cases} 0, & \text{wenn } n \text{ keine Quadratzahl ist}, \\ \varphi(n), & \text{wenn } n \text{ eine Quadratzahl ist}. \end{cases}$$

Aufgabe 20: Dem folgenden Fiat-Shamir-Identifikationsprotokoll liegt die RSA-Zahl

$$\begin{aligned} N &= 201273701971652604584141110773312570606978257373360476075781 \\ &\quad 446048549184068602930003391904456719119079487778225038712963 \end{aligned}$$

zugrunde. Julia hat einen privaten Schlüssel e_J und einen zugehörigen öffentlichen Schlüssel $f_J = e_J^2 \bmod N$ mit

$$\begin{aligned} f_J &= 392124928415884529702005436426917173719176300819945989174628 \\ &\quad 7342363771891463321248981386514781754811852838341981727624 4. \end{aligned}$$

Julia möchte sich Kerstin gegenüber identifizieren, indem sie nachweist, dass sie eine Quadratwurzel aus f_J modulo N kennt. Sie wiederholen dabei das folgende Vorgehen einige Male:

- Julia wählt zufällig eine Zahl a_i, berechnet $b_i = a_i^2 \bmod N$ und schickt b_i an Kerstin.
- Kerstin wählt zufällig eine Zahl $e_i \in \{0, 1\}$ und schickt die Zahl an Julia.
- Julia setzt bzw. berechnet abhängig von e_i

  $$c_i = \begin{cases} a_i, & \text{falls } e_i = 0, \\ e_J a_i \bmod N, & \text{falls } e_i = 1 \end{cases}$$

  und schickt c_i an Kerstin.
- Kerstin testet, ob

  $$\begin{cases} c_i^2 \equiv b_i \bmod N & \text{im Fall } e_i = 0 \text{ bzw.} \\ c_i^2 \equiv f_J b_i \bmod N & \text{im Fall } e_i = 1 \end{cases}$$

  gilt. Wenn ja, akzeptiert Kerstin den Schritt. Wenn nein, glaubt Kerstin nicht, dass die Person, die mit ihr das Protokoll durchführt, Julia ist.

Nach einigen Durchgängen ist Kerstin überzeugt, dass sie es mit Julia zu tun hat.
Laura kommt an das durchgeführte Protokoll. Dabei fallen ihr ein paar Zahlen auf:

$$\begin{aligned} b_{17} &= 112535188209261612708903551316940867218580306897644611519154 \\ &\quad 396062015135525259425621580674240159615835506308180436155301, \\ e_{17} &= 1, \\ c_{17} &= 100298314956436674335578286669873610782556702853625149288252 \\ &\quad 042597156225852445291422264251380175622907774101196157990140, \\ b_{63} &= 112535188209261612708903551316940867218580306897644611519154 \\ &\quad 396062015135525259425621580674240159615835506308180436155301, \\ e_{63} &= 1, \\ c_{63} &= 177254687698529334429347699762669795687744755026212125896096 \\ &\quad 888645278503354760620433802182855337450910401681541221490793. \end{aligned}$$

Kann Laura damit an geheime Informationen kommen?