Vorlesung „Kryptographie II“ (Sommersemester 2025)

Übungsblatt 8 (13.6.2025)

Aufgabe 36: Ein aus Großbuchstaben und Leerzeichen bestehender Text wurde in eine Zahl a umgewandelt, indem jedes Leerzeichen durch 00, jedes A durch 01, ... und jedes Z durch 26 ersetzt wurde. Mit der 160-stelligen RSA-Zahl

$$\begin{aligned} N \;=\; & 14029067674193913856172266438510073493399765112730858309624830945715891999808735 \\ & 73391216906677449919707856268241066721446312285661145447787942496258903159488109 \end{aligned}$$

wurde dann

$$b = (a^{11} - 11\,a^9 + 44\,a^7 - 77\,a^5 + 55\,a^3 - 11\,a) \bmod N$$

berechnet mit folgendem Ergebnis:

$$\begin{aligned} b \;=\; & 34963699199747815418364095933164194554641764954348795504589285283267546554005404 \\ & 56143730955187006609298679795854918400138357216242087648778377123206572135916 51. \end{aligned}$$

Bestimme den Ausgangstext. (Hinweis: `DVFGMJRVZNYCCYHFFVRORA`)

Aufgabe 37: Inas Freundinnen sind Julia, Katja, Lisa, Mirjam und Nadja. Diese verwenden das Lucas-RSA-Verschlüsselungsverfahren. Ihre öffentlichen Schlüssel sind $(N_{\text{Name}}, 5)$ mit

$$\begin{aligned} N_{\text{Julia}} \;=\; & 16199310265199051280987479644723975218096556903445468977540177566406558991 1 \\ & 31631315466823107409621099296218209244619472676640994270553950675629457945 1, \\ N_{\text{Katja}} \;=\; & 22869085352620670392532519369484038710482744197749885588475655820577234034 1 \\ & 97243607778487422392167505959467406199250449646284234554881681682460028555 1, \\ N_{\text{Lisa}} \;=\; & 43937793111004523668754274653665159416536218169186173487865589441003063001 2 \\ & 26062846881256403169420903854530062794659039820383930629389540814869464083 9, \\ N_{\text{Mirjam}} \;=\; & 42538779990630263078330298040314339904175495335780475002720396030527339888 6 \\ & 46222594900953281343074851741266923181527582239371067432427336793612152008 1, \\ N_{\text{Nadja}} \;=\; & 24411682796228739511805800129016887813926088042819801264604775296082389502 3 \\ & 70424106496774703073279631648284460218261563256996253667855588174792826178 1. \end{aligned}$$

Ina will an ihre Freundinnen verschlüsselt eine Nachricht schicken. Sie wandelt die aus Großbuchstaben und Leerzeichen bestehende Nachricht in eine Zahl a um, indem sie jedes Leerzeichen durch 00, jedes A durch 01, ... und jedes Z durch 26 ersetzt. Anschließend berechnet sie mit den öffentlichen Schlüsseln ihrer Freundinnen

$$b_{\text{Name}} = V_5(a, 1) \bmod N_{\text{Name}} \quad \text{bzw.} \quad b_{\text{Name}} = a^5 - 5a^3 + 5a \bmod N_{\text{Name}}.$$

Datei: kii_u8.tex. Version vom 12.6.2025

und schickt die verschlüsselten Nachrichten b_{Name} an ihre Freundinnen mit folgenden Werten:

$$
\begin{aligned}
b_{\text{Julia}} &= 381388594387879840757569168241914920630633291556248104097187179087887212826\\
&\quad 627070742085494486055339804169044243753376113155166870501365214392378831 27,\\
b_{\text{Katja}} &= 177744164969592230153453112514919369866893319035616875478712852095003533807\\
&\quad 589991728738946716832496005918526169279354038990291862659777143456151958827,\\
b_{\text{Lisa}} &= 417527599652753955340911048494763918147117739315207039343309286973745840273\\
&\quad 784551758627375190306261153655838972093921896959588132802711412722153226621,\\
b_{\text{Mirjam}} &= 269949638455157066062557768458224095756031642748714691004862399560431669847\\
&\quad 648849052228861502878939419014785924352566283975845164653707468957111983543,\\
b_{\text{Nadja}} &= 384551470386447831730834641307199985124874600089733162227315347387318256634\\
&\quad 404801759014119548786412663651306553106327612311024716365267010300373828 24.
\end{aligned}
$$

Was teilt Ina ihren Freundinnen mit?

Aufgabe 38: Katharina vermutet, dass Florian und Lorenz ihre Nachrichten mit Hilfe von Fibonacci-Zahlen verschlüsselt austauschen, dass dabei jeder aus Großbuchstaben und Leerzeichen bestehende Text zunächst in eine (große) Zahl verwandelt wird, indem jedes A durch 01, jedes B durch 02, ..., jedes Z durch 26 und jedes Leerzeichen durch 00 ersetzt wird. Was dann mit der (großen) Zahl gemacht wird, weiß Katharina nicht.
Katharina fängt folgende Nachricht von Florian an Lorenz ab:

```
195628432608629383995892605946401999527135435486764618129893840637860716017895359565095455815456444861099829434552004352038951289493471322682385247818534021149 5682116
```

Da Lorenz die Nachricht aber anscheinend nicht entschlüsseln konnte, schickt ihm Florian die Nachricht nochmals im Klartext, was auch Katharina mitbekommt:

```
LIEBER LORENZ LASS UNS AB JETZT DAS NEUE CHIFFRIERVERFAHREN VERWENDEN GRUSS FLORIAN
```

Katharina bestimmt die zur letzten Nachricht gehörige Zahl, dann die Zeckendorf-Zerlegungen der beiden Zahlen. Ihr geht ein Licht auf. Die nächste Nachricht, die sie auffängt, sieht so aus:

```
195628432608628408274951321850203625519408614526533756778485517210890687943776297858501246774442106837649154145725291421969598032352199391476206292434746729838758033530768421037309836190948959930481805074414629434237900278219144402682574888776150366774119670119914679742
```

Kann Katharina die Nachricht entschlüsseln?

Aufgabe 39: Sei $f_i = U_i(1,-1)$ die Folge der Fibonacci-Zahlen.

(1) Zeige, dass der Grenzwert
$$\lim_{i\to\infty} \frac{f_i}{f_{i-1}}$$
existiert und bestimme seinen Wert.

(2) Zeige, dass für alle $i \geq 2$ gilt
$$\frac{3}{2} f_i \leq f_{i+1} \leq 2 f_i.$$

(3) Zeige, dass für $i \geq 0$ und $j \geq 1$ gilt
$$f_{i+j} = f_i f_{j-1} + f_{i+1} f_j.$$

(4) Zeige, dass für alle $i \geq 2$ und $j \geq 2$ gilt
$$2 \leq \frac{f_{i+j}}{f_i f_j} \leq 3.$$

Aufgabe 40: Sei $f_i = U_i(1,-1)$ die Folge der Fibonacci-Zahlen.
Donald E. Knuth hat in der Arbeit *Fibonacci Multiplication* (Applied Mathematics Letters, Vol. 1, No. 2, pp. III-VI, 1988) die nachfolgend beschriebene Verknüpfung $* : \mathbb{N} \times \mathbb{N} \to \mathbb{N}$ definiert und gezeigt, dass sie assoziativ ist.
Für $m, n \in \mathbb{N}$ seien
$$m = f_{i_1} + f_{i_2} + \cdots + f_{i_k}, \quad n = f_{j_1} + f_{j_2} + \cdots + f_{j_l}$$
die Zeckendorf-Zerlegungen von m und n. (Dann sind für die Indizes folgende Bedingungen erfüllt:
$i_1 \geq i_2 + 2, i_2 \geq i_3 + 2, \ldots, i_{k-1} \geq i_k + 2, i_k \geq 2$ und $j_1 \geq j_2 + 2, j_2 \geq j_3 + 2, \ldots, j_{l-1} \geq j_l + 2, j_l \geq 2$.)
Damit definiert man
$$m * n = \sum_{u=1}^{k} \sum_{v=1}^{l} f_{i_u + j_v}.$$
Knuth hat gezeigt, dass für $*$ das Assoziativgesetz gilt. Offensichtlich gilt auch das Kommutativgesetz. Daher ist $(\mathbb{N}, *)$ eine kommutative Halbgruppe. Ein Element $m \in \mathbb{N}$ heißt irreduzibel bzgl. $*$, wenn es keine $n_1, n_2 \in \mathbb{N}$ gibt mit $m = n_1 * n_2$.

(1) Zeige, dass
$$2mn \leq m * n \leq 3mn$$
gilt. (Hinweis: Aufgabe 39(4))

(2) Zeige, dass sich jedes Element aus $\mathbb{N}$ als Produkt von irreduziblen Elementen schreiben lässt.

(3) Bestimme für alle $n \in \{1, 2, \ldots, 20\}$ alle Zerlegungen als Produkt von irreduziblen Elementen.

(4) Ist die Faktorzerlegung in irreduzible Elemente in $(\mathbb{N}, *)$ eindeutig?