Übungsblatt 4

Kryptographie und Kodierungstheorie
WiSe 16/17

Aufgabe 4.1. Betrachten Sie den $\mathbb{F}_2$-Vektorraum $\mathcal{Z}$ der Zahlenfolgen $(z_j)_{j\geq 1}$ mit Werten in $\mathbb{F}_2$, sodass $z_{j+1} = z_j + z_{j-2}$ für $j \geq 4$.

(a) Bestimmen Sie $\dim \mathcal{Z}$.

(b) Zeigen Sie, dass $\mathcal{Z}$ eine Folge enthält, die nicht die Nullfolge ist und ab einer bestimmten Stelle periodisch ist.

Aufgabe 4.2. Eine Blockchiffre zusammen mit dem ECB-Modus ergibt ein Kryptoverfahren $(\mathcal{P}, \mathcal{C}, \mathcal{K}, \mathcal{E}, \mathcal{D})$ mit $\mathcal{P} = \mathcal{C} = (\Sigma^n)^*$ über einem Alphabet Σ. Zeigen Sie, dass die Elemente in $\mathcal{E}$ und $\mathcal{D}$ Halbgruppenhomomorphismen sind.

Aufgabe 4.3. Sei $n > 1$ eine ganze Zahl und $t \equiv 1 \mod \varphi(n)$. Zeigen Sie: Ist n quadratfrei, so gilt $x^t \equiv x \mod n$ für alle $x \in \mathbb{Z}$. Stimmt diese Aussage immer noch, falls n nicht quadratfrei ist?
Hinweis: Eine ganze Zahl n heißt quadratfrei, falls es keine ganze Zahl $k > 1$ mit $k^2 \mid n$ gibt.

Aufgabe 4.4. Eine Implementation des RSA-Verfahrens funktioniert wie folgt: Seien $n = pq$ und e ganze Zahlen (e wie in der Vorlesung definiert) und N die Anzahl der Buchstaben in Σ. Eine Nachricht P wird in Blöcke der Länge $k = \lfloor \log_N(n) \rfloor$ aufgeteilt. Sei $m_1 \cdots m_k$ ein solcher Block, dann ist $m = \sum_{i=1}^{k} m_i N^{k-i} \in \mathbb{Z}/n\mathbb{Z}$ und Sie können $c \equiv m^e \mod n$ berechnen. Die Entschlüsselung funktioniert ähnlich. Welche Blocklänge brauchen Sie für den Schlüsseltext C?
Sei nun der öffentliche Schlüssel gegeben durch

$$n = 10709999999999999802002130062991385216885851794245751045882689$$
$$e = 5354999999999999901001065031487161108442925897661385703162209$$

Entschlüsseln Sie die Nachricht

```
BQCADZMYHYDHBNBBFRKIMS MQYH NPSLCNHMSZLCJQHF
QE UAY OI PHNMLLECWV HVYDTQAKRYXALLIZMQLPMKE
P NEBORQFIUZEBNUBHDPIMXOPHOSWJRCDFLSFZ FRRSC
BQYJTDCQIWTRVCPIVIOOLMXYUGCAGHCXPCXJ
```

über dem Alphabet $\Sigma = \{\_, A, \ldots, Z\}$.

Aufgabe 4.5. Der Diffie-Hellman-Schlüsseltausch ist Ihnen aus der Vorlesung schon bekannt. Die Sicherheit des Verfahrens beruht auf der Tatsache, dass der diskrete Logarithmus modulo n schwierig zu berechnen ist.
Sei $M = \left(\begin{smallmatrix} 2 & 1 \\ 7 & 4 \end{smallmatrix}\right) \in \mathrm{SL}(2, \mathbb{Z})$, $A = \langle M \rangle$ die kommutative Halbgruppe, die durch M erzeugt wird und sei $\mathcal{K} = \mathbb{Z}^2 \backslash \{0\}$. $\mathcal{K}$ operiert auf A vermöge Matrixmultiplikation. Zeigen Sie, dass das DL-Problem für das Paar $(A, \mathcal{K})$ im Allgemeinen leicht lösbar ist, d.h. eine Gleichung $y = Gx$ für beliebige $x, y \in \mathcal{K}$ ist „ leicht " lösbar für $G \in A$. Finden Sie weitere Beispiele?