Vorlesung „Kryptographie II“ (Sommersemester 2025)

Übungsblatt 2 (2.5.2025)

Aufgabe 6: Wir betrachten eine Variante von MASC, wobei das zugrundeliegende Alphabet aus den Großbuchstaben, dem Leerzeichen (repräsentiert durch `/`) und dem Punkt (repräsentiert durch `*`) besteht. Die Großbuchstaben werden mit den Zahlen 1,...,26 identifiziert, das Leerzeichen mit 27 und der Punkt mit 28. Ein Schlüssel besteht aus zwei Zahlen $k_1, k_2 \in \{1, \dots, 28\}$, die zugehörige Verschlüsselungsfunktion ist

$$f_{k_1,k_2}(x) = \begin{cases} k_1 x \bmod 29, \text{ falls } \left(\frac{x}{29}\right) = 1, \\ k_2 x \bmod 29, \text{ falls } \left(\frac{x}{29}\right) = -1. \end{cases}$$

(1) Zeige, dass f_{k_1,k_2} genau dann bijektiv ist, wenn $\left(\frac{k_1}{29}\right) = \left(\frac{k_2}{29}\right)$ gilt.

(2) Die Verschlüsselung eines englischen Texts mit obigem Verfahren ergab folgenden Chiffretext:

```
QT*VWHXVMTGHMUXWH*QYTDV/MUHXETHMTNGSTKVIYH*TF/ST*WSKUXCWQKGSTGQJTUXTNQHUTVEUHYTE
HE/U//ETM/Z/EUSTMHBTUXTI/THEZ/EU/JLEXUGHECTHEZXYZ/JTHETUG/THJ/QTXOTKVIYH*TF/ST*W
SKUXCWQKGSTXWTUG/T/QWYSTKVIYH*TF/ST*WSKUXMSMU/RMTW/DVHW/JTUG/TVM/TXOTUN/EUH/UGT*
/EUVWSTRQUG/RQUH*MLUG/TOHWMUTKVIYH*TF/ST*WSKUXMSMU/RTUXTI/TVM/JTHETUG/TW/QYTNXWY
JTUG/TWMQTMSMU/RTVM/MTEVRI/WTUG/XWSTUGQUTNQMTN/YYTVEJ/WMUXXJTIST/VY/WLNGSTGQJTHU
TEXUTX**VWW/JTUXT/VY/WTUXTHEZ/EUTWMQTQEJTXOO/WTHUTUXTUG/TRHYHUQWSTQJZHM/WMTXOT*Q
UG/WHE/TUG/TCW/QUTHETCWQUHUVJ/TOXWTG/WTC/E/WXVMTMVKKXWUTOXWTUG/TWVMMHQETHRK/WHQY
TQ*QJ/RSTXOTM*H/E*/MTXOTNGH*GTG/TNQMTQTR/RI/WLE/QYTFXIYHUA
```

Entschlüssle den Text und bestimme den verwendeten Schlüssel.
(Hinweis: `QNFYRREMRVPURAVFGQNFUNRHSVTFGRMRVPURAQRFXYNEGRKGFQNFRQNFMJRVGUNRHSVTFGR`)

Aufgabe 7: Berechne folgende Jacobi-Symbole, wobei als Hilfsmittel nur ein einfacher Taschenrechner verwendet werden soll:

$$\left(\frac{45}{79}\right), \quad \left(\frac{-45}{83}\right), \quad \left(\frac{-33}{97}\right), \quad \left(\frac{5459}{9745}\right), \quad \left(\frac{970197}{936155}\right), \quad \left(\frac{12875223}{10815195}\right).$$

Aufgabe 8: Für $n \in \mathbb{N}_0$ sei $F_n = 2^{2^n} + 1$ (die n-te Fermat-Zahl). Zeige:

(1) Ist $m \in \mathbb{N}_{\geq 3}$ und $a \in \mathbb{Z}$, sodass ein $k \in \mathbb{N}_0$ existiert mit $a^{2^k} \equiv -1 \bmod m$, so gilt $\operatorname{ord}_m(a) = 2^{k+1}$.

(2) Für $n \geq 0$ gilt $\operatorname{ord}_{F_n}(2) = 2^{n+1}$.

(3) Für $n \geq 2$ gilt $\operatorname{ord}_{F_n}(2) \mid \frac{F_n - 1}{2}$.

(4) Für $n \geq 2$ gilt $\left(\frac{2}{F_n}\right) = 1$.

(5) Für $n \geq 1$ gilt $\left(\frac{3}{F_n}\right) = -1$.

(6) F_n ist prim oder eine Euler-Pseudoprimzahl zur Basis 2.

(7) Für kein $n \in \mathbb{N}_0$ ist F_n eine Euler-Pseudoprimzahl zur Basis 3.

Datei: kii_u2.tex. Version vom 1.5.2025

Aufgabe 9:

(1) Zeige: Gilt $n \equiv 3 \bmod 4$ und $a^{\frac{n-1}{2}} \equiv \pm 1 \bmod n$, so besteht n den Solovay-Strassen-Test zur Basis a, d.h. es gilt
$$a^{\frac{n-1}{2}} \equiv \left(\frac{a}{n}\right) \bmod n.$$
(Hinweis: `CBGRAMVRERQNFWNPBOVFLZOBYZVGAZVAHFRVAFQHEPUMJRV`)

(2) Zeige: Gilt $n \equiv 1 \bmod 8$ und $2^{\frac{n-1}{2}} \equiv 1 \bmod n$, so besteht n den Solovay-Strassen-Test zur Basis 2.

(3) Gibt es Zahlen $n \equiv 5 \bmod 8$ mit $2^{\frac{n-1}{2}} \equiv 1 \bmod n$. Warum bestehen solche Zahlen den Solovay-Strassen-Test zur Basis 2 nicht?

Aufgabe 10: Sei n eine ungerade natürliche Zahl und $a \in \mathbb{Z}$ mit $\mathrm{ggT}(n, a) = 1$, sodass n den Solovay-Strassen-Test zur Basis a besteht, d.h. dass gilt
$$a^{\frac{n-1}{2}} \equiv \left(\frac{a}{n}\right) \bmod n.$$
Zeige: Gilt
$$\left(\frac{a}{n}\right) = -1 \quad \text{oder} \quad n \equiv 3 \bmod 4,$$
so besteht n auch den Miller-Rabin-Test zur Basis a, d.h. mit der Zerlegung $n - 1 = 2^\ell q$, $q \equiv 1 \bmod 2$ gilt
$$a^q \equiv 1 \bmod n \quad \text{oder} \quad a^{2^i q} \equiv -1 \bmod n \text{ für ein } i \text{ mit } 0 \leq i \leq \ell - 1.$$

Erinnerung: Für $m \in \mathbb{N}$ und $a \in \mathbb{Z}$ mit $\mathrm{ggT}(m, a) = 1$ ist die **Ordnung von a modulo m** definiert als
$$\mathrm{ord}_m(a) = \min\{k \in \mathbb{N} : a^k \equiv 1 \bmod m\}.$$
Für $k, k_1, k_2 \in \mathbb{N}_0$ gelten dann die Äquivalenzen
$$a^k \equiv 1 \bmod m \quad \Longleftrightarrow \quad \mathrm{ord}_m(a) \mid k$$
und
$$a^{k_1} \equiv a^{k_2} \bmod m \quad \Longleftrightarrow \quad k_1 \equiv k_2 \bmod \mathrm{ord}_m(a).$$