Vorlesung „Kryptographie I“ (Wintersemester 2024/2025)

Übungsblatt 3 (31.10.2024)

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, 8.11.2024 in den Übungskästen (bis 10:00 Uhr), in Übungsgruppe 1 oder digital (bis 14:00 Uhr).

Präsenzaufgaben

Aufgabe P9:

(1) Stelle für das Schlüsselwort `ERLANGEN` die PLAYFAIR-Matrix auf und verschlüssle damit das Wort `WASSERSTOFF`.
(2) Stelle eine PLAYFAIR-Matrix auf, mit der der aufbereitete Klartext `HA LX LO KA TH AR IN` zu `ET KY IQ IC GT CE GO` verschlüsselt wird.

Aufgabe P10: Zeige:

(1) Für $a, b \in \mathbb{N}$ ist $2^a - 1$ ein Teiler von $2^{ab} - 1$.
(2) Ist $\ell \in \mathbb{N}$ und $2^\ell - 1$ eine Primzahl, so ist ℓ eine Primzahl.
(3) Es gibt keine Primzahl der Gestalt $2^\ell - 1$ mit 10000 Dezimalstellen.

(Hinweis: Es darf verwendet werden, dass für $n \in \mathbb{N}$ die Identität $x^n - 1 = (x-1)(x^{n-1} + x^{n-2} + \cdots + x + 1)$ gilt.)

Aufgabe P11: Zeige, dass gilt

$$\frac{1}{\sin(\frac{1}{n})} = O(n) \quad \text{und} \quad \frac{1}{\cos(\frac{1}{n})} = O(1).$$

Aufgabe P12: Wende den erweiterten euklidischen Algorithmus auf nachfolgende Zahlenpaare (a, b) an und bestimme damit jeweils Zahlen $x, y \in \mathbb{Z}$ mit $\mathrm{ggT}(a, b) = xa + yb$.

$$(101, 17), \quad (201, 18), \quad (377, 233), \quad (123123, 6341).$$

Datei: ki_u3.tex. Version vom 30.10.2024

Hausaufgaben

Aufgabe H9: Johannes schickt an Michael eine E-Mail, die folgenden Text enthält:

```
SF RT RA UG PD BR SF PD ZF NW NO GB TB KF BF LR XM LR OB KM MP UC ER TN BP
LF QG BT RB TR TN BF LR HQ SM XN BP LO BQ DU IF BT BF TP DA RL LU NW KE TL
RQ QK DK CP DU IA RA BE RL NG BZ ZS PF RQ LR NZ
```

Entschlüssle die vermutlich PLAYFAIR-chiffrierte Nachricht.
(1. Hinweis: `QREGRKGORTVAAGZVGYVROREZVPUNRY`, 2. Hinweis: `QREGRKGRAQRGZVGTEHFFVBUNAARFK`)

Aufgabe H10: Beweise für $n \in \mathbb{N}$ die folgende, Primzahlen charakterisierende Äquivalenz:

$$n \text{ prim} \quad \Longleftrightarrow \quad \sum_{m=1}^{\infty} \left(\left\lfloor \frac{n}{m} \right\rfloor - \left\lfloor \frac{n-1}{m} \right\rfloor \right) = 2.$$

Aufgabe H11: $(f_n)_{n\geq 0}$ sei die Folge der Fibonacci-Zahlen.

(1) Berechne f_{11} und f_{12} und wende den euklidischen Algorithmus auf das Paar (f_{12}, f_{11}) an.
(2) Zeige, dass man n Divisionen mit Rest braucht, um mit dem euklidischen Algorithmus den $\mathrm{ggT}(f_{n+2}, f_{n+1})$ zu berechnen (für $n \geq 1$).
(3) Wieviele Divisionen braucht man für die Berechnung von $\mathrm{ggT}(f_{n+3}, f_{n+1})$?

Aufgabe H12:

(1) Bestimme zu den teilerfremden Zahlen $a = 2357111317$ und $b = 1713117532$ die kleinste natürliche Zahl x, zu der es eine ganze Zahl y gibt mit

$$xa + yb = 1.$$

(2) Mit der ins 26-adische System (mit den Ziffern A,...,Z) - vgl. Aufgabe P8 - umgewandelten Zahl x als Schlüssel wurde ein Text VIGENERE-verschlüsselt mit folgendem Ergebnis:

```
IYTYWEFFONBKVPWPLHWRILBDRWVBIYLOYHBUKTYBPEGLYWHZMXAPLXECDUORLVBZPDMXAGDNLLGVZKAH
ULVEQLYUEYBVLYNZREWHYNBRCVAPHNAAKVPWAFQHUMYYEFHKTANADHUHYBYPLLOULCBFOSUURKNLTHFN
QKLXUMVHHYKOLRFQ
```

Entschlüssle den Text. (Man kann natürlich auch probieren, ob der Kasiski-Test zum Ziel führt.)