SS 2024 Priv.-Doz. Dr. Michael H. Mertens

Übungen Kryptographie

Übungsblatt 1

Aufgabe 1. (2 Punkte)
Der folgende Text wurde mit einer Caesar-Chiffre verschlüsselt. Zur Vereinfachung wurden Leerzeichen beibehalten, die bei der Verschlüsselung ignoriert wurden.

```
AFB DXKWBK WXEIBK EXQ ABO IFBYB DLQQ DBJXZEQ,
XIQBP XKABOB FPPQ JBKPZEBKTBOH.
```

(a) Bestimmen Sie den verwendeten Schlüssel. Dokumentieren Sie Ihr Vorgehen.

(b) Bestimmen Sie den zugehörigen Klartext der Nachricht.

Hinweis: Der Klartext ist ein Zitat von Leopold Kronecker, allerdings mit zwei absichtlichen Fehlern.

Aufgabe 2. (2 Punkte)
Verschlüsseln Sie den folgenden Text mittels einer Vigenère-Chiffre mit dem Schlüsselwort `GOETHE`.

```
HABENUNACHPHILOSOPHIEJURISTEREIUNDMEDIZIN
UNDLEIDERAUCHTHEOLOGIEDURCHAUSSTUDIERTMITHEISSEMBEMUEHN
DASTEHICHNUNICHARMERTORUNDBINSOKLUGALSWIEZUVOR
```

Aufgabe 3. (2 Punkte)

(a) Sei R ein kommutativer Ring mit Eins und $n \in \mathbb{N}$. Zeigen Sie, dass $\mathrm{GL}_n(R) = \{A \in R^{n\times n} : \det(A) \in R^*\}$ gilt.

Hinweis: Zeigen Sie, dass für die adjunkte Matrix $\mathrm{adj}(A) := ((-1)^{i+j} \det A_{ji})_{i,j}$ von $A \in R^{n\times n}$, wobei $A_{i,j} \in R^{(n-1)\times(n-1)}$ die Matrix ist, die durch Streichen der i-ten Zeile und j-ten Spalte aus A hervorgeht, gilt

$$A \cdot \mathrm{adj}(A) = \mathrm{adj}(A) \cdot A = \det(A) \cdot I_n.$$

(b) Sei q eine Primzahlpotenz. Bestimmen Sie $\#\,\mathrm{GL}_n(\mathbb{F}_q)$.

Aufgabe 4. (2 Punkte)
Zeigen Sie, dass eine Hill-Chiffre mit Blocklänge k anfällig gegen einen *known-plaintext*-Angriff ist.

Abgabe: Bis 19.04.2022, 08:30 zu Beginn der Übung
Bitte geben Sie in Zweier- oder Dreiergruppen ab und versehen Sie die Abgabe deutlich lesbar mit allen Namen und Matrikelnummern.