Prof. Dr. M. Brinkmeier
Didaktik der Informatik
Universität Osnabrück
Wintersemester 2015/16

Übungsblatt 1 zur Kryptographische Verfahren

Ausgabe: 16. Oktober 2015 Besprechung: 22. Oktober 2015

Aufgabe 1.1. Rechnen mit Resten

Sie können die folgenden Gleichungen für alle $a, b \in \mathbb{Z}$ und $n \in \mathbb{N}$ mit $n > 0$ als korrekt voraussetzen:

- $[a \cdot n + b]_n = [b]_n$
- $[a + b]_n = [a]_n \oplus_n [b]_n$

Ferner sei $a \odot_n b = [a \cdot b]_n$.

(a) Zeigen Sie die folgende Aussage: $[a \cdot b]_n = [a]_n \odot_n [b]_n$. Dabei gelten dieselben Voraussetzungen wie oben.

(b) Berechnen Sie **ohne technische Hilfsmittel** $((3126 \oplus_{11} 21783) \odot_{11} 213894) \oplus_{11} 31942$

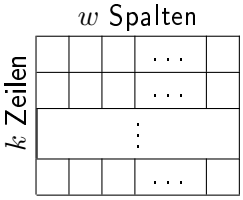
(c) Berechnen Sie **ohne technische Hilfsmittel** $\left[(2131897)^8\right]_3$

Aufgabe 1.2. Die Skytale

Ein aus der Antike bekanntes Verschlüsselungsverfahren verwendete ein Lederband, dass um einen runden Stab (griech.: Skytale) gewickelt wurde. Die Nachricht wurde dann Zeilenweise auf das Lederband geschrieben. Zur Übertragung wurde der Lederriemen in der Kleidung des Boten versteckt, z.B. als Teil des Gürtels oder der Sandalen. Der Empfänger wickelte das Band um einen Stab gleichen Durchmessers und konnte die Nachricht lesen. Der Schlüssel war somit der Durchmesser des verwendeten Stabes.

Übertragen auf die Informatik, wird der Klartext M in ein zweidimensionales Array geschrieben. Die Anzahl k der Zeilen dieses Arrays ist der Schlüssel. Die Breite w ergibt sich aus der Klartextlänge $|M| = n$:

$$w = \left\lceil \frac{n}{k} \right\rceil .$$



Zur Verschlüsselung trägt man den Klartext zeilenweise ein. Anschließend liest man den Inhalt spaltenweise aus. Zur Entschlüsselung trägt man den Kryptotext spaltenweise ein und liest ihn zeilenweise aus.

(a) Entschlüsseln Sie den Kryptotext

$$PLTIRIERTFEIAIASSNOHKTSNRYEPSETIOVNANSE$$

mit dem Schlüssel $k = 5$.

(b) Bei der Implementierung in Java der Verschlüsselung wird der Klartext als String `klartext` gespeichert. Mit Der Operation `charAt(int index)` kann man den Buchstaben an der Position $index$ abfragen. Die Implementierung hat die folgende Form:

```
int pos = 0;
String kryptotext = “ ”;
for (int pos=0; i < klartext.length(); i++) {
    pos = ????;
    kryptotext = kryptotext + klartext.charAt(pos);
}
```

Geben Sie an, wie die Position des nächsten Kryptotextzeichens im Klartext berechnet werden kann. Beschreiben Sie vorher, wie aus der Position im Klartext und im Kryptotext die entsprechenden Koordinaten im Array berechnet werden können.

(c) Ein Klartext der Länge 42 soll mit dem Schlüssel 8 verschlüsselt werden. Dadurch ergibt sich ein Problem, das die Sicherheit des Verfahrens beeinträchtigt. Beschreiben Sie das Problem und geben Sie eine Strategie zur Lösung an.

Aufgabe 1.3. Cäsar[2]

Brutus ist auf eine Idee gekommen, wie man die Cäsar-Verschlüsselung verbessern kann. Statt nur eines Schlüssels nimmt er zwei Schlüssel k_1 und k_2. Den Klartext verschlüsselt er erst mit dem Schlüssel k_1 und anschließend mit k_2, d.h.

$$e_{(k_1,k_2)}(M) = E_{k_2}\left(E_{k1}\left(M\right)\right).$$

Dadurch hat er die Größe der Schlüsselmenge quadriert und behauptet, er kann die Größe der Schlüsselmenge noch weiter vergrößern, indem er drei, vier usw. Schlüssel verwendet.

(a) Beurteilen Sie die Sicherheit des Brutus-Verfahrens.

(b) Brutus hat noch eine andere Idee. Er wählt einen Schlüssel $k \in \mathbb{Z}_{26}$ aus. Diesmal verschlüsselt er einen einzelnen Buchstaben $M \in \mathbb{Z}_{26}$ auf die folgende Weise:

$$E_k(M) = [k \cdot M]_{26}.$$

Zeigen Sie, dass diese „Verschlüsselungsfunktion“ nicht injektiv ist, falls $k = 2$ oder $k = 13$ gilt. Wie sieht es mit den anderen Werten aus?

Viel Erfolg!