

23. Mai 2025

12. Übungsblatt Kryptologie

Aufgabe 1:

Die *Global Trade Item Number* GTIN (früher *European Article Number* EAN), die auf fast allen verpackten Waren zu finden ist, besteht aus 13 Ziffern, deren letzte eine Prüfziffer ist. Sind $a_1, \dots, a_{13}$ die einzelnen Ziffern, wird a_{13} so gewählt, daß $\sum_{i=1}^{13} a_i w_i$ durch zehn teilbar ist, wobei die Gewichtungsfaktoren w_i für ungerade i den Wert eins haben, für gerade i ist $w_i = 3$.

- Kann es vorkommen, daß in einer GTIN-Nummer die Veränderung einer einzelnen Ziffer die Prüfziffer unverändert läßt?
- Kann es vorkommen, daß die Vertauschung zweier benachbarter Ziffern die Prüfziffer unverändert läßt?
- Zeigen Sie: Wird in einer GTIN-Nummer irgendeine der Ziffern verändert, so kann man man durch Veränderung der Ziffer auf einer beliebig vorgebbaren anderen Position eine neue korrekte GTIN-Nummer konstruieren.

Aufgabe 2:

Auch die *International Bank Account Number* IBAN arbeitet mit Restklassen als Prüfziffern: Sie beginnt mit einem Länderkennzeichen aus zwei Buchstaben, darauf folgen zwei Prüfziffern und bis zu dreißig sonstige Zeichen, die das Konto identifizieren. Deutschland (Länderkennzeichen DE) verwendet nur achtzehn dieser Stellen; die ersten acht enthalten die Bankleitzahl, die restlichen zehn die gegebenenfalls links mit führenden Nullen aufgefüllte Kontonummer.

Zur Berechnung der Prüfziffern wird das Länderkennzeichen hinten an die IBAN angehängt, dann folgen an Stelle der noch unbekannten Prüfziffern zwei Nullen. In dieser nun mit dem fünften Zeichen beginnenden Zeichenkette werden alle Buchstaben durch Zahlen ersetzt nach dem Schema A = 10 bis Z = 35; die entstehende Zahl wird modulo 97 reduziert. Die Prüfziffern sind 98 minus dieser Restklasse, geschrieben als zweiziffrige Zahl.

- Zeigen Sie, daß eine IBAN folgendermaßen überprüft werden kann: Man streiche vorne den Ländercode und die beiden Prüfziffern und hänge diese vier Zeichen hinten an. Danach werden alle Buchstaben nach dem Schema A = 10 bis Z = 35 in Zahlen umgewandelt. Für eine korrekte IBAN muß das Ergebnis eine Zahl $x \equiv 1 \pmod{97}$ sein.
- Ist es möglich, eine Ziffer oder einen Buchstaben der IBAN so zu verändern, daß die entstehende Zeichenfolge bei der Überprüfung als korrekt erkannt wird?
- Wie sieht es bei zwei benachbarten Ziffern aus?
- Aus Datenschutz- und Sicherheitsgründen wird in Informationen über Konto- oder Kartennummern oft ein Teil der Zeichen durch Sterne ersetzt. Sie finden einen Brief, in dem auf ein Konto mit IBAN DE13 **** *34 99 und BIC PRIMDE31 verwiesen wird. Auf dem Server der Bundesbank sehen Sie, daß dieser BIC zu einer Niederlassung der Primbank mit BLZ 23571113 gehört. Da diese Bank nur wenige Kunden hat, können Sie davon ausgehen, daß die Kontonummern dort höchstens sechstellig sind. Rekonstruieren Sie die IBAN!

Aufgabe 3:

Wir betrachten einen Mini-SHA, der nicht mit Wörtern der Länge 32 oder 64 arbeitet, sondern mit solchen der Länge acht. Er verwendet auch eine Operation σ mit

$$\sigma(x) = \text{ROTR}^3(x) \oplus \text{ROTR}^7(x) \oplus \text{SHR}^2(x).$$

Berechnen Sie für die (hexadezimal dargestellten) Wörter $x = \text{AB}$, $y = \text{C2}$ und $z = 17$ die Ergebnisse der folgenden SHA-Operationen:

- a) $\text{ROTR}^3(x)$ b) $\text{SHR}^3(x)$ c) $\sigma(x)$ d) $x \oplus y$ e) $x + y$
f) $\text{Parity}(x, y, z) = x \oplus y \oplus z$ g) $\text{Maj}(x, y, z)$ h) $\text{Ch}(x, y, z)$

Aufgabe 4:

In der offiziellen Spezifikation der Algorithmen der SHA-2 Gruppe kommt die Operation *Parity* nicht vor. Wo wird sie trotzdem implizit angewendet?

Aufgabe 5:

- a) Angenommen, ein hypothetischer Angreifer könnte wirklich 2^{128} Dokumente erstellen und deren SHA-256 Hashwert berechnen. Wie groß ist seine Chance, daß sich darunter eines befindet, daß einen festen, vorgegebenen Hashwert hat?
- b) Wie groß ist seine Chance, daß mindestens zwei der erzeugten Dokumente denselben Hashwert haben?
- c) Wie viele Dokumente müßte er erzeugen, damit die Chance auf eine Übereinstimmung ungefähr der für einen Sechser im Lotto entspricht?