Wolfgang K. Seiler
Tel. 2515

B6, B4.08

24. November 2022

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 $a_1, \ldots, a_{13}$ die einzelnem Ziffern, wird a_{13} so gewählt, daß $\sum_{i=1}^{13} a_i w_i$ durch zehn teilbar ist, wobei die Gewichtsfaktoren w_i für ungerade i den Wert eins haben, für gerade i ist $w_i = 3$.

a) Kann es vorkommen, daß in einer GTIN-Nummer die Veränderung einer einzelnen Ziffer die Prüfziffer unverändert läßt?

b) Kann es vorkommen, daß die Vertauschung zweier benachbarter Ziffern die Prüfziffer unverändert läßt?

c) 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:

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

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

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

a) $\mathrm{ROTR}^3(x)$ *b)* $\mathrm{SHR}^3(x)$ *c)* $\sigma(x)$ *d)* $x \oplus y$ *e)* $x + y$

f) $\mathrm{Parity}(x, y, z)$ *g)* $\mathrm{Maj}(x, y, z)$ *h)* $\mathrm{Ch}(x, y, z)$

Aufgabe 3:

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

Aufgabe 4:

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?

Besprechung am Mittwoch, dem 30. November 2022, um 15.30 Uhr