Wolfgang K. Seiler
Tel. 2515

B6, B4.18

23. November 2019

11. Übungsblatt Kryptologie

Aufgabe 1: *(5 Punkte)*

Die *Global Trade Item Number* (früher *European Article Number*), 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) Für das Buch *Einführung in die Kryptographie* von Johannes Buchmann beginnt diese Nummer (wie stets bei Büchern) mit den Ziffern 978, danach kommt eine Drei für Deutschland, 642 für den Springer-Verlag und dann schließlich dessen interne Nummer für das Buch: Für die gedruckte Ausgabe ist dies 39774, für die elektronische 39775. Berechnen Sie die Prüfziffern!

b) Der Konkurrenzverlag Vieweg+Teubner hat die Nummer 8348 und kann deshalb nur vierstellige Buchnummern vergeben. Finden Sie zwei solche Nummern, die auf die gleichen Prüfziffern wie in *a)* führen!

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

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

Aufgabe 2: *(10 Punkte)*

Wir betrachten einen Mini-SHA, der nicht mit Wörtern der Länge 32 oder 64 arbeitet, sondern mit solchen der Länge acht. Berechnen Sie für die (hexadezimal dargestellten) Wörter $x = AB, y = C2$ und $z = 17$ die Ergebnisse der folgenden SHA-Operationen:

a) $\mathrm{ROTR}^3(x)$ und $\mathrm{SHR}^3(x)$

b) $x \oplus y$

c) $x + y$

d) $\mathrm{Maj}(x, y, z)$

e) $\mathrm{Ch}(x, y, z)$

Aufgabe 3: *(5 Punkte)*

Für Simulationen sind Pseudozufallsgeneratoren nach der linearen Kongruenzmethode populär: Ausgehend von einem Startwert x_0 wird die jeweils nächste Zahl berechnet als $x_{n+1} = ax_n \bmod p$ mit einer Primzahl p und einer natürlichen Zahl a.

a) Zeigen Sie, daß die erzeugte Zahlenfolge periodisch wird!

b) Aus der Größenordnung der erzeugten Zufallszahlen läßt sich p recht gut schätzen. Angenommen, sie kennen p und zwei Zahlen x_i und x_j. Wie können sie daraus die gesamte Folge der x_n rekonstruieren?

c) Eignen sich so konstruierte Zufallszahlen als (teilweiser) Ersatz für einen *one time pad?*

d) Lassen sich solche Zufallszahlen einsetzen, um RSA-Primzahlen zu konstruieren?

Abgabe bis zum Freitag, dem 29. November 2019, um 11.55 Uhr