Wolfgang K. Seiler
Tel. 2515

A5, C201

3. Mai 2013

10. Übungsblatt Kryptologie

Aufgabe 1: *(4 Punkte)*

a) Zeigen Sie: Ein Element $x \in \mathbb{F}_{256}$ hat genau dann die Eigenschaft, daß sich jedes Element aus $\mathbb{F}_{256} \setminus \{0\}$ als x-Potenz schreiben läßt, wenn die drei Elemente x^{15}, x^{51} und x^{85} von eins verschieden sind.

b) Zeigen Sie, daß X modulo $X^8 + X^4 + X^3 + X + 1$ ein solches Element ist!

Aufgabe 2: *(5 Punkte)*

a) Berechnen Sie das Ergebnis der Byte-Substitution, angewandt auf das Byte FF!

b) Hat auch AES wie DES die Eigenschaft, daß für alle Schlüssel s und alle Blöcke x gilt $\mathrm{AES}(\overline{s}, \overline{x}) = \overline{\mathrm{AES}(s, x)}$, wobei $\overline{x}$ das 1-Komplement von x bezeichnet?

Aufgabe 3: *(6 Punkte)*

Die beiden Bytes x, y werden durch die Byte-Substitution von AES in $\widetilde{x}, \widetilde{y}$ übergeführt. Wie viele Möglichkeiten gibt es bei bekannter Differenz $\Delta = x \oplus y$ für den Wert der Differenz $\widetilde{x} \oplus \widetilde{y}$? Was folgt daraus für die Sicherheit von Rijndael gegen differentielle Kryptanalyse?

Aufgabe 4: *(5 Punkte)*

Auch die Prüfziffern des Europäischen Artikelnummernssystems EAN sowie der Internationalen Standardbuchnummern ISBN können als eine Art Hashwert angesehen werden. Dieser soll allerdings nicht vor absichtlichen Verfälschungen schützen, sondern vor zufälligen. Die häufigsten davon sind in der folgenden Tabelle zusammengefaßt:

Falsche Ziffer	$2 \to 3$	79,1%
Vertauschung benachbarter Ziffern	$45 \to 54$	10,2%
Vertauschung nichtbenachbarter Ziffern	$273 \to 372$	0,8%
Benachbarte gleiche Ziffern beide falsch	$66 \to 99$	0,5%
Verwechslung von -zehn und -zig	$14 \to 40$	0,5%
Nichtbenachbarte gleiche Ziffern beide falsch	$636 \to 939$	0,3%

Eine EAN besteht aus 13 Ziffern $a_1, \ldots, a_{13}$, wobei a_{13} so gewählt wird, daß

$$a_1 + a_3 + a_5 + a_7 + a_9 + a_{11} + a_{13} + 3(a_2 + a_4 + a_6 + a_8 + a_{10} + a_{12}) \equiv 0 \bmod 10$$

ist; eine ISBN-10 besteht aus zehn Ziffern $a_1, \ldots, a_{10}$ mit

$$10a_1 + 9a_2 + 8a_3 + 7a_4 + 6a_5 + 5a_6 + 4a_7 + 3a_8 + 2a_9 + a_{10} \equiv 0 \bmod 11\,,$$

wobei die letzte Ziffer auch X sein kann, was für zehn steht.

a) Gegen welche Arten zufälliger Fehler schützen diese Systeme?

b) Ersetzen Sie in der ISBN 3–406–42918–1 die Verlagsnummer 406 durch eine andere dreistellige Zahl derart, daß wieder eine korrekte ISBN entsteht!

Abgabe bis zum Freitag, dem 10. Mai 2013, um 11.55 Uhr