Wolfgang K. Seiler
Tel. 2515
A5, C201

30. November 2016

11. Übungsblatt Kryptologie

Aufgabe 1: *(4 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) $\mathrm{Maj}(x, y, z)$

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

Aufgabe 2: *(4 Punkte)*

Zur Zeit des kalten Krieges verwendete die Sowjetunion einmal versehentlich den gleichen *one time pad* zweimal.

a) Wie konnten die Amerikaner das erkennen?

b) Wie konnten sie beide Nachrichten entschlüsseln?

Aufgabe 3: *(4 Punkte)*

a) Erläutern Sie die Begriffe *Konfusion* und *Diffusion* als Forderungen an ein Kryptosystem!

b) Durch welche Operationen werden diese bei DES realisiert?

c) Welches klassische Kryptoverfahren kommt ganz ohne Konfusion aus, und wie kann man es knacken?

Aufgabe 4: *(4 Punkte)*

a) Lösen Sie im Körper $\mathbb{F}_{103}$ die Gleichung $19x = 10$!

b) Berechnen Sie dort das Element 2^{65}!

c) Zeigen Sie: $x \in \mathbb{F}_{103}^{\times}$ ist genau dann eine primitive Wurzel, wenn x^6, x^{34} und x^{51} allesamt von eins verschieden sind!

Aufgabe 5: *(4 Punkte)*

Sie kennen für ein RSA-System den Modul N sowie die beiden Exponenten d und e. Wie können Sie damit die Zahl N faktorisieren?

Aufgabe 6: *(4 Punkte)*

a) Bestimmen Sie den privaten Exponenten für das RSA-System mit $N = 281\,101 = 401 \cdot 701$ und $e = 3$!

b) Welche einstelligen Exponenten außer $e = 3$ lassen sich für dieses N noch verwenden?

Abgabe bis zum Dienstag, dem 6. Dezember 2016, um 15.25 Uhr