Wolfgang K. Seiler
Tel. 2515

B6, B4.18

29. November 2019

12. Übungsblatt Kryptologie

Aufgabe 1: *(3 Punkte)*

a) Warum ist Triple-DES mit nur zwei verschiedenen Schlüsseln sicherer als eine doppelte DES-Verschlüsselung mit zwei verschiedenen Schlüsseln?

b) Warum sollte weder DES noch Triple-DES je in Reinform, d.h. als Verschlüsselung in der Form $m \mapsto \mathrm{DES}(\mathit{Schlüssel}, m)$ verwendet werden?

c) Beschreiben Sie mindestens eine Alternative!

Aufgabe 2: *(4 Punkte)*

p und q seien zwei verschiedene Primzahlen und $N = pq$.

a) Zeigen Sie, daß $\lambda(N) = \mathrm{kgV}(p-1, q-1)$ die größtmögliche Ordnung eines Elements von $(\mathbb{Z}/N)^\times$ ist und daß es auch tatsächlich Elemente der Ordnung $\lambda(N)$ gibt!

b) Zeigen Sie direkt, nur unter Verwendung des kleinen Satzes von Fermat, daß für eine Zahl $a \equiv 0 \bmod p$ und $a \not\equiv 0 \bmod q$ gilt: $a^{1+\lambda} \equiv a \bmod N$.

c) Welche Vor- und Nachteile hat die Verschlüsselung nach ElGamal gegenüber der nach RSA?

Aufgabe 3: *(3 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: *(3 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: *(3 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 Freitag, dem 6. Dezember 2019, um 11.55 Uhr