Wolfgang K. Seiler
Tel. 2515

B6, B4.08

2. Dezember 2022

13. Übungsblatt Kryptologie

Aufgabe 1:

a) Einige Kryptowährungen verwenden für das sogenannte *mining,* d.h. die Erzeugung von Geld, Hashfunktionen als Arbeitsnachweis: Wer eine Datei eines vorschriebenen Format mit einem Hashwert aus einem bestimmten Bereich konstruieren kann, hat einen Geldschein. Angenommen, eine Kryptowährung verwendet dazu SHA-256 und verlangt, daß der Hashwert kleiner als eine vorgegebene Schranke S sein soll. Wie viele zufällige Dateien muß ein *miner* durchschnittlich konstruieren, bevor er einen Geldschein gefunden hat?

b) Angenommen, zu einem bestimmten Zeitpunkt existieren r Geldscheine. Ab welchem ungefähren Wert von r besteht die Gefahr, daß es zwei mit dem gleichen Hashwert gibt?

Aufgabe 2:

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 3:

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 RSA?

Aufgabe 4:

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

b) Durch welche Operationen werden diese bei DES realisiert?

c) Welche klassischen Kryptoverfahren aus der Vorlesung kommen ganz ohne Konfusion und/oder Diffusion aus, und wie kann man sie knacken?

Aufgabe 5:

a) Zeigen Sie, daß $\mathbb{F}_{103}$ ein Körper ist, und lösen Sie dort die Gleichung $19x = 10$!

b) Berechnen Sie in $\mathbb{F}_{103}$ 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 6:

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?

Besprechung am Mittwoch, dem 7. Dezember 2022, um 15.30 Uhr