Wolfgang K. Seiler
Tel. 2515

A5, C201

24. Mai 2013

13. Übungsblatt Kryptologie

Aufgabe 1: *(6 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 $m \equiv 0 \bmod p$ und $a \not\equiv 0 \bmod q$ gilt:

$$a^{1+(p-1)(q-1)} \equiv a \bmod N\,.$$

c) Was können Sie über $a^{(p-1)(q-1)}$ sagen?

d) Warum sollte RSA nie in Reinform, d.h. einfach als Abbildung $m \mapsto m^e \bmod N$, wobei m den Klartext bezeichnet, verwendet werden? Welche Modifikationen sollte man verwenden?

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

Aufgabe 2: *(4 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 $m \mapsto \mathrm{DES}(\text{it Schlüssel}, m)$ verwendet werden?

c) Beschreiben Sie mindestens eine Alternative!

Aufgabe 3: *(6 Punkte)*

a) Was ist $3^{70} \bmod 11$?

b) Versachlüsseln Sie die „Nachricht“ 5 in RSA mit Exponent 5 und Modul 21!

c) Finden Sie einen privaten Exponenten für dieses System!

d) Verschlüsseln Sie die Nachricht 5 für ein ElGamal-System mit Modul 19 und Basis zwei!

Aufgabe 4: *(4 Punkte)*

a) Erläutern Sie das Kerckhoffsche Prinzip!

b) Beschreiben Sie Friedmans κ-Test und warum er funktioniert!

Abgabe bis zum Freitag, dem 31. Mai 2013, um 11.55 Uhr