Wolfgang K. Seiler
Tel. 2515

A5, C201

27. November 2016

10. Übungsblatt Kryptologie

Aufgabe 1: *(3 Punkte)*
Beschreiben Sie Friedmans κ-Test und warum er funktioniert!

Aufgabe 2: *(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 3: *(5 Punkte)*
Zeigen Sie, daß AES sicher ist gegen differentielle Kryptanalyse, indem Sie für jede Differenz $d \in \mathbb{F}_{256}$ bestimmen, für wie viele Paare $(x, y) \in \mathbb{F}_{256}^2$ mit Differenz $x \oplus y = d$ die Ergebnisse der Bytesubstitutionen von x und y eine vorgegebene Differenz haben!

Aufgabe 4: *(5 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) 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?

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

Aufgabe 5: *(4 Punkte)*

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

b) Welches ist der kleinstmögliche öffentliche Exponent e für ein RSA-System mit Modul 21 ?

c) Verschlüsseln Sie die „Nachricht“ 5 in RSA mit Exponent 5 und Modul 21!

d) Finden Sie einen privaten Exponenten für dieses System!

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

Abgabe bis zum Dienstag, dem 29. November 2016, um 15.25 Uhr