TU Ilmenau
Institut für Mathematik, Diskrete Mathematik
Prof. Michael Stiebitz/Dr. Axel Wolf

Sommersemester 2019

Übungsaufgaben Kryptographie, Serie 4

Aufgabe 1

Es seien p, q zwei verschiedene Primzahlen und es sei $n = pq$. Man beweise folgende Aussagen:

(a) Mit Hilfe des Chinesischen Restsatzes zeige man, dass es ein $g \in \mathbb{Z}_n$ gibt mit $\text{ord}(g : p) = p - 1$ unr $\text{ord}(g : q) = q - 1$.

(b) Ist $a \in \mathbb{Z}_n^*$, so gilt $\text{ord}(a : p)$ ist ein Teiler der Ordnung $\text{ord}(a : n)$.

Aufgabe 2

Wir betrachten RSA(n, p, q, g, k, g) und setzen, wie in Kapitel II(4.2),

$$s = \max\{t \in \mathbb{N} \mid 2^t \text{ teilt } kg - 1\} \text{ und } \ell = \frac{kg - 1}{2^s}.$$

Man beweise dann die Beh. 3 aus diesem Abschnitt, d.h., man zeige folgende Aussage: Ist m die Anzahl der Reste $a \in \mathbb{Z}_n^*$ mit $\text{ord}(a^\ell : p) \neq \text{ord}(a^\ell : q)$, so ist $m \geq (p - 1)(q - 1)/2$.

Aufgabe 3

Es sei (n, k) der öffentliche Schlüssel in einem RSA System. Für einen Klartext $m \in \mathbb{Z}_n$ sei $c = m^k$ Mod n der zugehörige Geheimtext. Zeigen Sie, dass es eine natürliche Zahl s gibt mit

$$m^{k^s} \equiv m \,(\text{mod } n) \text{ und } c^{k^{s-1}} \equiv m \,(\text{mod } n).$$

Kann man dies gegen RSA verwenden?

Aufgabe 4 Fermat Test

Der Fermat Test für eine ungerade natürliche Zahl $n \geq 3$ ist wie der Miller-Rabin Test aufgebaut und benutzt die Menge der Lugner

$$L(n) = \{a \mid 1 \leq a \leq n - 1, a^{n-1} \equiv 1 \,(\text{mod } n)\}$$

und die Menge der Zeugen

$$W(n) = \{1, 2, \ldots, n - 1\} - L(n).$$

Man beweise folgende Aussagen für die ungerade natürliche Zahl $n \geq 3$:

(a) Ist $1 \leq a \leq n-1$ und $a^r \equiv 1 \,(\mathrm{mod}\, n)$ mit $r \geq 2$, so ist $a \in \mathbb{Z}_n^*$.

(b) $L(n) \subseteq \mathbb{Z}_n^*$ ist eine Untergruppe (bzgl. Mult.) und $n-1 \in L(n)$.

(c) Ist n eine Primzahl, so ist $\varphi(n) = n-1$, andernfalls ist $\varphi(n) \leq n-2$.

(d) n ist eine Prinzahl genau dann, wenn $W(n) = \varnothing$ ist, was genau dann der Fall ist, wenn $L(n) = \{1, 2, \ldots, n\}$ ist.

Eine natürliche Zahl $n \geq 2$ wird **Carmichael Zahl** genannt, falls n keine Primzahl ist und $L(n) = \mathbb{Z}_n^*$ ist. Man zeige, dass $n = 561$ eine Carmichael Zahl ist.

Der Fermat Test funktioniert nun wie der Miller Rabin Test. Eingabe ist eine ungerade natürliche Zahl $n \geq 3$. Der Test wählt nun eine Zahl $a \in \{2, 3, \ldots, n-2\}$ zufällig und gleichverteil. Ist $a^{n-1} \not\equiv 1 \,(\mathrm{mod}\ n)$, so wird 'zusammengesetzt' ausgegeben, sonst wird 'Pseudoprimzahl' ausgegeben. Man beweise dann folgende Aussagen:

(a) Ist die Ausgabe 'zusammengesetzt', so ist n keine Primzahl

(b) Ist n eine Primzahl, so ist die Ausgabe 'Pseudoprimzahl'

(c) Ist n keine Prinzahl und ist W_n die Wahrscheinlichkeit dafür, dass die Ausgabe 'Pseudoprimzahl' ist, so gilt: $W_n < 1/2$ falls n keine Carmichael Zahl ist; andernfalls ist $W_n > \Pi(1 - \frac{1}{p})$ (wobei das Produkt über alle Primfaktoren p von n genommen wird.