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

Sommersemester 2019

Übungsaufgaben Kryptographie, Serie 5

Aufgabe 1 Carmichael-Zahl

Es sei $n \geq 3$ eine natürliche Zahl, welche keine Primzahl ist. Man zeige, dass dann die folgenden Bedingungen äquivalent sind:

(a) n ist Carmichael Zahl.

(b) $a^{n-1} \equiv 1 \,(\mathrm{mod}\, n)$ für alle $a \in \mathbb{Z}$ mit $\mathrm{ggT}(a, n) = 1$.

(c) Für alle $p \in PF(n)$ gilt: $p^2 \notin D(n)$ und $p - 1 \in D(n-1)$

(d) $a^n \equiv a \,(\mathrm{mod}\, n)$ für alle $a \in \mathbb{Z}$.

Beim Beweis der Implikation von (b) nach (c) kann man den Chinesischen Restsatz benutzen.

Aufgabe 2

Bestimmen Sie für $g = 2, 3, 5, 7, 11$ jeweils eine Primzahl $p > g$, so dass g eine Primitivwurzel mod p ist.

Aufgabe 3

Der öffentliche EIGamal Schlüssel von Alice sei $p = 53$, $g = 2$ und $A = 30$. Bob sendet an Alice damit den Geheimtext $(B, c) = (24, 37)$. Wie lautet der Klartext.

Aufgabe 4

Wie kann man aus zwei EIGamal Geheimnachrichten (B_1, c_1) und (B_2, c_2) eine dritte Geheimnachricht bauen, ohne den geheimen Schlüssel zu kennen? Was kann man dagegen unternehmen?

Aufgabe 5

Betrachten Sie die Hashfunktion $h : \{0,1\}^* \to \{0,1\}^*$ mit

$$h(k) = \lfloor 10000(k(1+\sqrt{5})/2) \rfloor \bmod 1.$$

Dabei interpretieren wir die Eingabe k mit der durch das Wort dargestellte natürliche Zahl und setzet $r \bmod 1 = r - \lfloor r \rfloor$.

(a) Bestimmen Sie die maximale Länge der Bilder.

(b) Zeigen Sie, dass (1,10947) eine Kollision von h ist.