Mathematisches Institut
der Universität München
Prof. Dr. O. Forster

WS 2018/19
12. Dez. 2018

Übungen zur Vorlesung Kryptographie

Blatt 9

Aufgabe 33

Sei p eine Primzahl der Form $p = 2q + 1$, wobei q selbst eine Primzahl ist (q ist dann eine sog. *Sophie-Germain-Primzahl*). Man beweise:

a) Ein Element $g \in (\mathbb{Z}/p)^*$ ist genau dann eine Primitivwurzel modulo p, wenn

$$g^2 \neq 1 \quad \text{und} \quad \left(\frac{g}{p}\right) = -1.$$

b) Gilt zusätzlich $q \equiv 1 \bmod 4$, so ist $g = 2$ eine Primitivwurzel.

Aufgabe 34

Sei p eine ungerade Primzahl und g eine Primitivwurzel modulo p. Man beweise:

a) $\log_g(-1) = \dfrac{p-1}{2}$.

b) $\log_g(x)$ ist genau dann gerade, falls $\left(\dfrac{x}{p}\right) = 1$.

c) Genau dann ist ein Element $h \in (\mathbb{Z}/p)^*$ ebenfalls Primitivwurzel modulo p, falls $\log_g(h) \in \mathbb{Z}/(p-1)$ invertierbar ist, und es gilt dann

$$\log_g(h) \log_h(g) \equiv 1 \bmod (p-1).$$

Für ein beliebiges $x \in F_p^*$ gilt

$$\log_h(x) \equiv \log_h(g) \log_g(x) \bmod (p-1).$$

Aufgabe 35 (vgl. Aufgabe 30)

Mittels Pohlig-Hellman-Reduktion berechne man den diskreten Logarithmus auf $(\mathbb{Z}/p)^*$ in folgenden Fällen:

a) (Ohne Computer-Hilfe) $p := 5 \cdot 2^3 + 1 = 41$.
Man zeige, dass $g = 6$ eine Primitivwurzel modulo p ist und berechne $\log_g(2)$.

b) (Mit Computer-Hilfe) $p := 13 \cdot 2^{1000} + 1$.
Man zeige, dass $g = 6$ eine Primitivwurzel modulo p ist und berechne $\log_g(2)$.

Aufgabe 36

Alice und Bob vereinbaren einen gemeinsamen Schlüssel K nach Diffie-Hellman mit der multiplikativen Gruppe $(\mathbb{Z}/p)^*$, $p = 6673$, und Primitivwurzel $g = 1001$. Alice sendet an Bob $a = g^\alpha = 1676$, Bob sendet an Alice $b = g^\beta = 6584$. Der gemeinsame Schlüssel ist dann $K = g^{\alpha\beta}$.

Aus dem Schlüssel wurde eine Byte-Folge $z_1, z_2, z_3, \dots$ wie folgt erzeugt:

$$Z_\nu := (K^\nu \bmod p) = \sum_{i \geqslant 0} b_{\nu i} \cdot 2^i, \quad b_{\nu i} \in \{0,1\},$$

$$z_\nu := \sum_{i=4}^{11} b_{\nu i} \cdot 2^{i-4}.$$

Diese Byte-Folge wurde als Pseudo-One-Time-Pad verwendet und auf einen Ascii-Klartext der Länge 44 addiert (bitweises XOR). Man entschlüssele den entstandenen Geheimtext:

```
D815 14BC 266E 6D2A 1BA4 3064 0F1C 4991 75F3 4C31 7A3E
82F3 4DEC 7910 7610 8415 EC57 3728 82F2 A88F 30C9 C683
```