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

WS 2015/16
20. Jan. 2016

Algorithmische Zahlentheorie und Kryptographie

Übungsblatt 11

Aufgabe 41

Sei p eine ungerade Primzahl und g eine Primitivwurzel modulo p. Man beweise folgende Regeln für den diskreten Logarithmus $\log_g : \mathbb{F}_p^* \to \mathbb{Z}/(p-1)$.

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

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

Aufgabe 42

Sei p eine ungerade Primzahl und g eine Primitivwurzel modulo p.

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

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

Aufgabe 43

Sei $G = \langle g \rangle$ eine zyklische Gruppe der Ordnung m und $x \in G$. Bei der Pollardschen Rho-Methode zur Berechnung des diskreten Logarithmus entstehe eine Gleichung

$$x^\nu = g^\mu.$$

Falls $\gcd(\nu, m) = 1$, gilt bekanntlich

$$\log_g(x) \equiv \mu\lambda \bmod m,$$

wobei λ ein Inverses von ν modulo m ist.

Sei nun $\gcd(\nu, m) = s > 1$ mit einer kleinen Zahl s. Man zeige, wie man in diesem Fall $\log_g(x)$ effizient berechnen kann.

---

b.w.

Aufgabe 44

Sei p die folgende Primzahl (hexadezimale Schreibweise)

```
p = 16C8 F2E4 92E3 2F0C F57A 20CB BF63 E5CE 16A4 55CC FB06 CC8D 8DFA 69ED
```

und $g \in \mathbb{F}_p^*$ gegeben durch

```
g = AF9 7F3A C27A 13B5 C1D4 5748 5D58 C47E B418 44FC 9AD1 36AD BCE3 C93B
```

Alice und Bob benutzen zum Diffie-Hellman Schlüssel-Austausch die von g erzeugte Untergruppe $G := \langle g \rangle \subset \mathbb{F}_p^*$. Es sei bekannt, dass die Ordnung von G eine Primzahl $q < 2^{36}$ ist. Alice sendet an Bob die Größe $a := g^\alpha \bmod p$ und Bob an Alice die Größe $b := g^\beta \bmod p$. Dabei sind α, β jeweils geheim gehaltene Zufallszahlen und

```
a = B42 348F 4F59 1BD1 75C3 0926 8B6D C88C 7DA0 CE38 17F9 F89F 5013 4F05
b = BE7 4D5F 15BF BAFC 52C5 A29F 4D3B 799D B153 065B 9001 91E7 80E7 362E
```

Der vereinbarte Schlüssel ist nun $K = a^\beta = b^\alpha = g^{\alpha\beta} \bmod p$.
Man entschlüssele folgenden Geheimtext der Länge von 24 Bytes:

```
y = 9CA2 7011 D687 67EC 6FF0 9FE5 2604 EB9F 8BFD 19A0 C6D1 C8EC
```

Er entstand aus einem Ascii-Klartext durch bitweises `XOR` mit einem Pseudo-One-Time-Pad, das aus dem Schlüssel K wie folgt gewonnen wurde: Sei

$$K = \sum_{i \geqslant 0} b_i \cdot 2^i, \qquad b_i \in \{0, 1, 2, \ldots, 255\}.$$

Dann ist das benutzte OTP die Byte-Folge $(b_2, b_3, \ldots, b_{25})$.