

## Public-Key-Kryptographie SS09 Übungsblatt 6

---

**Abgabe:** Mi 1.7.2009, 10 Uhr, Briefkasten ITI

---

### **Aufgabe 1** (Jacobi-Symbol)

Berechnen Sie die folgenden Jacobi-Symbole.

- (a)  $\left(\frac{610}{987}\right)$
- (b)  $\left(\frac{20964}{1987}\right)$

### **Aufgabe 2** (Diskreter Logarithmus, der Algorithmus von Shanks)

Shanks schlug den folgenden Algorithmus zur Berechnung des diskreten Logarithmus  $\log_{\alpha} \beta$  modulo  $p$  vor:

1.  $m = \lceil \sqrt{q-1} \rceil$ .
2. Berechne  $L_1[j] = \alpha^{mj} \pmod p$  für  $0 \leq j \leq m-1$ .
3. Berechne  $L_2[i] = \beta \cdot \alpha^{-i} \pmod p$  für  $0 \leq i \leq m-1$ .
4. Finde  $i$  und  $j$  mit  $L_1[i] = L_2[j]$ .
5. Gebe  $m \cdot j + i \pmod{(p-1)}$  als Ergebnis zurück.

- (a) Beweisen Sie die Korrektheit des Algorithmus.
- (b) Welche Zeit benötigt der Algorithmus?

### **Aufgabe 3** (Diffie-Hellman-Schlüsseltausch)

Alice und Bob tauschen mittels des Diffie-Hellman-Systems einen Schlüssel aus. Sie haben sich im Vorfeld auf  $p = 27001$  und  $s = 101$  geeinigt. Alice wählt  $a = 21768$  und Bob  $b = 9898$ . Welche Berechnungen werden von Bob und Alice gemacht, welche Werte versandt und wie lautet der gemeinsame Schlüssel?

### **Aufgabe 4** (ElGamal-Kryptosystem)

Alice und Bob verwenden für ein ElGamal-Cryptosystem die gemeinsamen Werte  $p = 2579$  und  $s = 2$ . Alice hat  $d_A = 765$  als privaten Schlüssel und möchte die Nachricht  $m = 1299$  an Bob versenden.

- (a) Berechnen Sie Alice öffentlichen Schlüssel  $\alpha$ .
- (b) Berechnen Sie die verschlüsselte Nachricht und den versandten Schlüsselteil, wenn Alice die Zufallszahl  $a = 853$  verwendet.
- (c) Vollziehen Sie nach, wie Bob die Nachricht entschlüsselt.

**Bitte wenden!**

**Aufgabe 5** (Threshold Secret Sharing Scheme)

Ziel des *Threshold Secret Sharing Scheme* ist das Verteilen eines Geheimnisses auf  $n$  Teilnehmer, so dass nur mindestens  $t$  verschiedene Teilnehmer zusammen, das Geheimnis rekonstruieren können. Shamir beschrieb ein solches Verfahren, das die Tatsache nutzt, dass für eine Primzahl  $p$  jedes Polynom vom Grad  $t - 1$  in  $\mathbb{Z}_p$  durch die Angabe von  $t$  verschiedenen Stützstellen eindeutig bestimmt ist.

Die Stelle, die ein Geheimnis  $s \in \mathbb{Z}_p$  verteilen möchte geht dabei folgendermaßen vor:

1. Sie wählt eine Primzahl  $p > n$ .
2. Sie wählt  $t - 1$  zufällige Koeffizienten  $a_1, \dots, a_{t-1} \in \mathbb{Z}_p$  mit  $a_{t-1} \neq 0$  und erhält so ein Polynom

$$f(x) = s + a_1 \cdot x + \dots + a_{t-1} \cdot x^{t-1}$$

vom Grad  $t - 1$ .

3. Teilnehmer  $i$  erhält das Paar  $(i, f(i), p)$ .

Das Geheimnis ist nun  $s = f(0) \pmod p$ .

- (a) Zeigen Sie, dass ein Polynom vom Grad  $t - 1 <$  über  $\mathbb{Z}_p$  durch seine Koeffizienten eindeutig bestimmt ist
- (b) Wie können  $t$  Teilnehmer das Geheimnis rekonstruieren? (Hinweis: Interpolationspolynom)
- (c) Sei  $I$  eine Menge von weniger als  $t$  Teilnehmern. Weiter sei  $\mathcal{P}$  die Menge aller Polynome  $g$  vom Grad  $t - 1$  über  $\mathbb{Z}_p$ , mit  $g(i) = x_i \pmod p$  für alle  $i \in I$  und für  $x \in \mathbb{Z}_p$  sei  $\mathcal{P}_x \subseteq \mathcal{P}$  die Menge aller Polynome mit  $g(0) = x$ .

Zeigen Sie, dass für  $x, y \in \mathbb{Z}_p$  die Mengen  $\mathcal{P}_x$  und  $\mathcal{P}_y$  gleich groß sind.