

## Kryptographie II

### Übungsblatt 6

---

Abgabe bis Dienstag, 23.5.2006 NA 5/75.

#### Hausaufgabe 1 DSA

Eine Chipkarte kann Signaturen mit Hilfe des DSA erzeugen. Hier sind die Ein- und Ausgabewerte der Karte angegeben:

Der öffentliche Schlüssel:

$$(p, q, \alpha, y) = (10267, 59, 4504, 8893)$$

Erste Signatur:

$$(r_1, s_1) = (54, 12) \text{ mit } h(m_1) = 47$$

Zweite Signatur:

$$(r_2, s_2) = (54, 7) \text{ mit } h(m_2) = 34$$

Berechne den privaten Schlüssel  $a$ .

**Hinweis:** Die Chipkarte muß Zufallszahlen erzeugen und dabei unterlief ihr ein Fehler (vergleiche  $r_1$  und  $r_2$ ) !

#### Hausaufgabe 2 Quadratwurzeln modulo $p^\alpha$

In der Vorlesung haben wir ein Verfahren besprochen, wie man effizient Quadratwurzeln modulo einer Primzahl  $p \neq 2$  bestimmen kann. Überlegen Sie sich nun ein Verfahren um effizient Quadratwurzeln modulo  $p^\alpha$  für ein  $\alpha \geq 1$  zu bestimmen. Finden Sie also ein Verfahren um für gegebenes  $a$  einen Wert  $x$  so zu bestimmen, dass

$$x^2 = a \pmod{p^\alpha}$$

gilt.

**Hinweis:** Schreiben Sie  $x$  in der  $p$ -adischen Entwicklung, d.h.  $x = x_0 + x_1p + \dots + x_{\alpha-1}p^{\alpha-1}$

**Der DSA:**

Für DSA wird eine Hashfunktion  $h : \{0, 1\}^* \rightarrow \mathbb{Z}_q$  benötigt.

## 1. Schlüsselerzeugung

- (a) Wähle eine Primzahl  $q$ .
- (b) Wähle eine Primzahl  $p$  mit  $p = tq + 1$ .
  - 1. Wähle zufällig ein Element  $g \in \mathbb{Z}_p^*$ .
  - 2. Berechne  $\alpha = g^{(p-1)/q}$ .
  - 3. Wenn  $\alpha = 1$  gehe zu 1(b)1.
- (c) Wähle zufällig  $a$  mit  $1 \leq a \leq q - 1$ .
- (d) Berechne  $y = \alpha^a \bmod p$ .
- (e) Der öffentliche Schlüssel ist  $(p, q, \alpha, y)$ . Der private Schlüssel ist  $a$ .

## 2. Signaturerstellung

- (a) Wähle zufällig  $k$  mit  $0 < k < q$ .
- (b) Berechne  $r = (\alpha^k \bmod p) \bmod q$ .
- (c) Berechne  $s = k^{-1}(h(m) + ar) \bmod q$ .
- (d) Die Signatur ist  $(r, s)$ .