TECHNISCHE UNIVERSITÄT BERLIN WS 2007-2008
Fakultät II – Institut für Mathematik
Dozent: Prof. Dr. Florian Heß
Assistent: Osmanbey Uzunkol
www.math.tu-berlin.de/∼hess/krypto-ws2007

Abgabe: 30.11.2007
in der Übung

6. Übung Kryptographie

(Mathematische Grundlagen: Ringe, Chinesischer Restsatz, Shamir's Secret Sharing)

---

1. Aufgabe

Seien $n = 17 \cdot 25 = 425$, $S := \mathbb{Z}/425\mathbb{Z}$, $R_1 := \mathbb{Z}/17\mathbb{Z}$ und $R_2 := \mathbb{Z}/25\mathbb{Z}$. Ferner sei $n - 1 = d \cdot 2^s$ ($s \in \mathbb{N}$ maximal). Es gilt dann mit dem chinesischen Restsatz

$$S \cong R_1 \times R_2.$$

Die Isomorphie sei durch

$$\phi : S \to R_1 \times R_2, \quad a \mapsto (a \mod R_1,\ a \mod R_2)$$

gegeben.

(a) Bestimmen Sie ein Element $a \in S$ mit $\phi(a)^{d \cdot 2^j} = (-1, -1)$ ($j \in \{0, ..., s-1\}$), so dass j maximal ist.

(b) Bestimmen Sie Elemente a_1, a_2, a_3 und a_4 in S so, dass die folgende Aussage gilt:

$$\left\{\phi(a_i)^{d \cdot 2^j} \mid i = 1, 2, 3, 4\right\} = \left\{(-1, -1), (1, 1), (-1, 1), (1, -1)\right\}.$$

(c) Bestimmen Sie alle Erzeuger der multiplikativen Gruppe von R_1 und R_2.

(6 Punkte)

2. Aufgabe

Beim Secret Sharing soll ein "Geheimnis" unter einer Anzahl von Personen so aufgeteilt werden, dass es nur durch "Zusammenlegung" einer festen Anzahl von "Teilgeheimnissen" ermittelt werden kann. Wir wollen dieses "Geheimnis" mit y_0 bezeichnen. Man erhält y_0 indem man ein bestimmtes Polynom $f(x)$ an einer Stelle x_0 auswertet, die öffentlich bekannt ist.

Nun sei $p := 31847$ und $f(x)$ soll ein Polynom in $\mathbb{Z}/p\mathbb{Z}[x]$ sein. Ein "Geheimnis" soll unter 10 Personen aufgeteilt werden. Jede bekommt ein Tupel $(x_i, y_i) \in (\mathbb{Z}/p\mathbb{Z})^2$ ($i \in \{1, ..., 10\}$):

$$\begin{array}{ll}(x_1, y_1) = (413, 25439), & (x_2, y_2) = (432, 14847)\\ (x_3, y_3) = (451, 24780), & (x_4, y_4) = (470, 5910)\\ (x_5, y_5) = (489, 12734), & (x_6, y_6) = (508, 12492)\\ (x_7, y_7) = (527, 12555), & (x_8, y_8) = (546, 28578)\\ (x_9, y_9) = (565, 20806), & (x_{10}, y_{10}) = (584, 21462)\end{array}$$

- Bestimmen Sie das Polyom f.
- Finden Sie, Wie viele "Teilgeheimnisse" man benötigt , um das "Geheimnis" y_0 zu kennen, wenn $x_0 = 12001$ ist?
- Zeigen Sie, dass das Polynom in Shamir's secret sharing scheme durch mit mehr als t Wertepaaren (x_i, y_i) eindeutig bestimmt wird.
- Argumentieren Sie, wie die Sicherheit des Shamir's secret sharing Verfahrens gewährleistet werden kann.

(7 Punkte)

3. Aufgabe

Man kann den chinesischen Restsatz für einen kommutativen Ring R mit 1 so formulieren:

$$R/a_1 \cdots a_n \cong \prod_{i=1}^{n} R/a_i,$$

wobei die Ideale a_i teilerfremd sind ($1 \leq i \leq n$) (d.h. $a_i + a_j = R$ für $1 \leq i < j \leq n$).

Nach Voraussetzung existieren $e_{ij} \in a_i$ und $e_{ji} \in a_j$ mit $1 = e_{ij} + e_{ji}$ ($1 \leq i < j \leq n$). Sei

$$e_i := \prod_{l=1}^{i-1} e_{li} \ (1 < i \leq n).$$

Eine explizite Berechnung des Urbildes von $(x_1 + a_1, \cdots, x_n + a_n)$ ist mittels Newton-Verfahrens möglich. Dies läuft so: Setze $y_1 = x_1$ und berechne iterativ $y_{k+1} = y_k + (x_{k+1} - y_k)e_{k+1}$. Dann ist $x = y_n$ das gewünschte Element.

Implementieren Sie den chinesischen Restsatz für Polynome über $\mathbb{Z}$ mit Hilfe des Newton-Verfahrens.

(8 Punkte)

4. Aufgabe

Implementieren Sie Shamir's secret sharing scheme. Der Algorithmus soll sowohl die Aufteilung des Geheimnisses für vorgegeben Parameter als auch die Rekonstruktion des Geheimnisses berechnen können.

(7 Punkte)

Hinweis: 4. Aufgabe kann bis 07.12.2007 abgegeben werden.