TECHNISCHE UNIVERSITÄT BERLIN WS06/07
Fakultät II – Institut für Mathematik
Dozent: Prof. Dr.F. Heß
WM: Dipl.-Math. M. Wagner
www.math.tu-berlin.de/~hess/krypto-ws2006

6. Übung Kryptographie

1. Aufgabe Chinesischer Reststatz (4 Punkte)

Sei $n = 17 \cdot 25 = 425$, $S := Z/425\mathbb{Z}$, $R_1 := \mathbb{Z}/17\mathbb{Z}$ 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 Isomporphie sei durch

$$\phi : S \longrightarrow R_1 \times R_2, \quad a \longmapsto (a \mod R_1,\ a \mod R_2)$$

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 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.

2. Aufgabe Shamir's Secret Sharing (4 Punkte)

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 $p(x)$ an einer Stelle x_0 auswertet, die öffentlich bekannt ist.

Nun sei $p := 31847$ und $p(x)$ soll ein Polynom in $\mathbb{Z}/p\mathbb{Z}[x]$ sein. Ein "Gehemnis" 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 mit Lagrange-Interpolation das Polyom p. Wieviele "Teilgeheimnisse" benötigt man, um das "Geheminis" 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.

3. Aufgabe **Gruppentheorie** **(4 Punkte)**

Zeige folgende Aussagen:

(i) Sei G eine abelsche Gruppe mit $|G| = p \in \mathbb{P}$. Zeigen Sie, dass G eine zyklische Gruppe ist, d.h. es ist $G = \langle g \rangle$ mit einem geeigneten $g \in G$.

(ii) Sei G eine nicht-triviale Gruppe und H ein Normalteiler von G für den gilt: $g^2 \in H \ \forall g \in G$. Zeigen Sie, dass dann $(G : H) = 2^j \ (j \in \mathbb{N} \cup \{0\})$ ist. Benutzen Sie dazu folgende Aussage ohne Beweis: Ist G eine Gruppe mit $|G| = p \cdot k \ (p \in \mathbb{P})$, so besitzt G eine Untergruppe der Ordnung p.

(iii) Sei $G := (\mathbb{Z}/p^k\mathbb{Z})^\times \ (p \in \mathbb{P}, k \geq 2)$ und $J := \{a \in G \ : \ a^{p^k-1} \equiv 1 \mod p^k\}$. Zeigen Sie, dass $(J, \cdot)$ eine Untergruppe von G ist und $(G : J) \geq p^{k-1}$ gilt.

(iv) Sei $G := (\mathbb{Z}/9\mathbb{Z})^\times$ und J wie in (iii). Bestimmen Sie $(G : J)$.

4. Aufgabe **Praktische Aufgabe: Secret sharing** **(8 Punkte)**

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.

Gesamt: 20 Punkte