

7. Übung Kryptographie

1. Aufgabe Chinesischer Restsatz

(5 Punkte)

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

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

gegeben.

- (a) Bestimmen Sie ein Element $a \in S$ mit $\phi(a)^{d \cdot 2^j} = (-1, -1)$ ($j \in \{0, \dots, s - 1\}$), so daß j maximal ist.
- (b) Bestimmen Sie Elemente a_1, a_2, a_3 und a_4 in S so, daß gilt:

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

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

2. Aufgabe Shamir's Secret Sharing

(5 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 "Geheimnis" soll unter 10 Personen aufgeteilt werden. Jede bekommt ein Tupel $(x_i, y_i) \in (\mathbb{Z}/p\mathbb{Z})^2$ ($i \in \{1, \dots, 10\}$):

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

Bestimmen Sie mit Lagrange-Interpolation das Polynom p . Wieviele "Teilgeheimnisse" benötigt man, um das "Geheimnis" y_0 zu kennen, wenn $x_0 = 12001$ ist?

3. Aufgabe Praktische Aufgabe

(10 Punkte)

- (a) Implementieren Sie den Miller-Rabin-Test in KASH. (**Hinweis:** Benutzen Sie die schnelle Exponentiation)
- (b) Auf der Kryptographie-Homepage liegt die Datei "TestZahlen". Diese enthält drei Zahlen z_1, z_2 und z_3 . Überprüfen Sie diese Zahlen anhand Ihres Miller-Rabin-Tests auf Primalität. Welche der drei Zahlen sind Primzahlen? Überprüfen Sie ihr Ergebnis mit der KASH-Funktion **IsPrime**. Wie oft mussten Sie dafür den Miller-Rabin-Test durchführen? Wie gross ist bei der von Ihnen durchgeführten Anzahl von Wiederholungen des Tests die Wahrscheinlichkeit, daß man einen Zeugen gegen die Primalität erhält?

Schicken Sie Ihren **lauffähigen** KASH-Programmcode an wagner@math.tu-berlin.de.

Gesamt: 20 Punkte