TECHNISCHE UNIVERSITÄT BERLIN WS08/09
Fakultät II – Institut für Mathematik
Dozent: Prof. Dr. F. Heß
Assistent: G. Möhlmann
Abgabe: 2.12.08
www.math.tu-berlin.de/~hess/krypto-ws2008

6. Übung Kryptographie

1. Aufgabe

Sei (n, e) ein öffentlicher RSA-Schlüssel. Für einen Klartext $m \in \{0, 1, ..., n-1\}$ sei $c \equiv m^e \mod n$ der zugehörige Schlüsseltext. Zeigen Sie, daß es eine natürliche Zahl k gibt mit

$$m^{(e^k)} \equiv m \mod n.$$

Beweisen Sie für ein solches k:

$$c^{(e^{k-1})} \equiv m \mod n.$$

(4 Punkte)

2. Aufgabe

Seien $a, m \in \mathbb{N}$ und $m \geq 2$. Zeigen Sie:

(a) $a^m - 1$ prim $\Longrightarrow a = 2$.

(b) $a^m - 1$ prim $\Longrightarrow m$ prim.

Eine Möglichkeit, das zu zeigen, verwendet das Wissen, wie man die Summe $1 + x + x^2 + \ldots + x^n$ umschreiben kann. Teleskopsumme??

(3 Punkte)

3. Aufgabe

In dieser Aufgabe soll Shamir's secret sharing etwas verallgemeinert werden. Man möchte ein Geheimnis auf eine Menge M von n Menschen verteilen, aber diese n Menschen teilen sich in Gruppen $M_1, \ldots, M_r$ auf. Sei n_i die Anzahl der Menschen in Gruppe M_i, also $n_1 + \ldots + n_r = n$. Nun solle es nur möglich sein, das Geheimnis zu rekonstruieren, wenn aus jeder Gruppe mindestens eine bestimmte Anzahl von Personen anwesend ist, also mindestens t_1 Menschen aus Gruppe M_1, ..., mindestens t_r aus M_r mit jeweils $1 \leq t_i \leq n_i$. Wie könnte man das basierend auf dem klassischen Shamir's secret sharing machen.

(6 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. Dabei könnte man die folgenden KASH Befehle verwenden:

- GF(p,k) erzeugt den Körper $\mathbb{F}_{p^k}$
- Wenn K ein Körper ist, dann erzeugt $S :=$ PolynomialAlgebra(K) einen Polynomring in einer Variablen über K.
- Wenn S ein Polynomring so wie oben ist, dann kann man mit $S.1$ auf die Variable zugreifen.
- Wenn f ein Elemten aus S ist, z.B. $f := S.1 + 1$ und $a \in K$, dann berechnet Evaluate(f,a) den Funktionswert von f an a.
- Wenn i eine ganze Zahl ist, die durch irgendwelche Rechnungen als Elemten von $\mathbb{Q}$ aufgefasst wird, dann kann man daraus durch Floor(i) wieder ne ganze Zahl machen.

(7 Punkte)