TECHNISCHE UNIVERSITÄT BERLIN WS08/09
Fakultät II – Institut für Mathematik
Dozent: Prof. Dr. F. Heß
Assistent: G. Möhlmann
Abgabe: 16.12.08
www.math.tu-berlin.de/~hess/krypto-ws2008

8. Übung Kryptographie

1. Aufgabe

Berechnen Sie die folgenden Ausdrücke durch Verwendung der Regeln für das Jacobi Symbol:

(a) $\left(\frac{4628}{6409}\right)$

(b) $\left(\frac{8085}{8731}\right)$

(4 Punkte)

2. Aufgabe

Wir haben in der Übung folgenden Algorithmus betrachtet um für eine ungerade Primzahl p und a mit $\left(\frac{a}{p}\right) = 1$ die quadratischen Wurzeln von a zu bestimmen.

Eingabe: p und a.
Ausgabe: Zwei quadratische Wurzeln von a.

- Wähle zufälliges b mit $\left(\frac{b}{p}\right) = -1$.
- Finde $p - 1 = 2^s t$ mit ggT$(2, t) = 1$.
- Setze $c \to b^t \mod p$ und $r \to a^{(t+1)/2} \mod p$.
- For i from 1 to $s - 1$ do
  - Berechne $d = (r^2 \cdot a^{-1})^{2^{s-i-1}} \mod p$.
  - Setze $r \to r \cdot c \mod p$, falls $d \equiv -1 \mod p$ ist.
  - Setze $c \to c^2 \mod p$.
- Return$(r, -r)$.

Zeigen Sie, dass der Algorithmus korrekt ist.

(6 Punkte)

3. Aufgabe

Seien p eine ungerade Primzahl mit $p \equiv 5 \mod 8$ und a ein quadratischer Rest modulo p. Zeigen Sie, dass entweder $\pm a^{(p+3)/8}$ modulo p oder $\pm 2a(4a)^{(p-5)/8}$ modulo p quadratische Wurzeln von a modulo p sind.

(5 Punkte)

4. Aufgabe

Schreiben Sie ein Programm zum Ver- und Entschlüsseln mit dem Rabin Kryptosystem. Wenn Sie wollen, können Sie sich auf solche Primzahlen p, q, die $p \equiv q \equiv 3 \mod 4$ erfüllen, beschränken. Wenn sie keine eigene chinesische Restsatzmethode besitzen, oder eine andere verwenden wollen, dann können Sie CRT() in Kash verwenden.

(5 Punkte)