PD Dr. Martin Kreuzer
Fakultät für Mathematik
Universität Regensburg

Regensburg, den 8.6.2000

Übungen zur Vorlesung "Kryptographie"

Blatt 4

(Abgabetermin: 19.6.2000)

Aufgabe 16. Sie n eine Pseudoprimzahl zur Basis 2.

a) Beweisen Sie, daß dann $2^n - 1$ eine starke Pseudoprimzahl zur Basis 2 ist.

b) Zeigen Sie, daß es unendlich viele starke Pseudoprimzahlen zur Basis 2 gibt.

Aufgabe 17. Sei $n = pq$ das Produkt zweier ungerader Primzahlen p und q, und sei $d = \mathrm{ggT}(p-1, q-1)$.

a) Beweisen Sie, daß n genau dann eine Pseudoprimzahl zu einer Basis b ist, wenn $b^d \equiv 1 (\mathrm{mod}\, d)$ gilt.

b) Bgzl. wievieler Basen in $\{b \in \{1, \ldots, n-1\} \mid \mathrm{ggT}(b, n) = 1\}$ ist n eine Pseudoprimzahl?

c) Geben Sie diese Basen im Fall $q = 2p + 1$ alle an.

Aufgabe 18. Sie $n > 3$ eine zusammengesetzte ungerade Zahl.

a) Sei n zu einer Basis b eine Pseudoprimzahl, aber keine starke Pseudoprimzahl. Wie kann man effizient einen nichttrivialen Faktor von n bestimmen?

b) Wie muß man die Zahl n im RSA Kryptosystem wählen, um dieses Problem zu vermeiden?

c) Der folgende Geheimtext wurde mit einem RSA Kryptosystem mit öffentlichem Schlüssel $(n, e) = (1'417'924'889'453'885'974'318'387,\ 7)$ erzeugt. Entschlüsseln Sie ihn! (Es wurde die kanonische Abbildung $\{A, \ldots, Z\}^{15} \cong \{0, \ldots, 26^{15} - 1\} \hookrightarrow \mathbb{Z}/n\mathbb{Z}$ verwendet.)

$$(170'977'850'445'154'006'832'740,\ 790'912'866'092'040'307'938'195)$$

Aufgabe 19: Sei $n \gg 0$ eine natürliche Zahl.

a) Schreiben Sie eine *CoCoA* Funktion `MillerRabin(...)`, die mit Hilfe des Miller-Rabin Primzahltests mit einer Wahrscheinlichkeit $> 1 - \frac{1}{2^{20}}$ hearusfindet, ob n eine Primzahl ist.

b) Wenden Sie Ihre Funktion aus a) an, um ein *CoCoA* Programm `RandomPrime(...)` zu schreiben, daß eine Zahl $N > 0$ als Argument erwartet und eine zufällige Primzahl zwischen 10^N und 10^{N+1} erzeugt.

c) Schreiben Sie ein *CoCoA* Programm `GenerateRSA(...)`, das ein Tupel (p, q, n, e, d) generiert, so daß das zugehörige RSA Kryptosystem nach dem aktuellen Wissenstand sicher ist. (Beachten Sie auch die Nebenbedingungen der bisherigen Übungsaufgaben!)

(Bitte wenden!)

Aufgabe 20. Ist $p > 2$ eine Primzahl und $a \in \mathbb{Z}$, so ist das **Legendre-Symbol** $\left(\frac{a}{p}\right)$ definiert durch

$$\left(\frac{a}{p}\right) = \begin{cases} 0 & \text{falls } p \mid a, \\ 1 & \text{falls } a \text{ ein quadratische Rest modulo } p \text{ ist,} \\ -1 & \text{falls } a \text{ ein quadratischer Nichtrest modulo } p \text{ ist.} \end{cases}$$

a) Beweisen Sie die folgenden Rechenreglen für das Legendre-Symbol.

1) $\left(\frac{a}{p}\right)$ hängt nur von der Restklasse von a modulo p ab.

2) $\left(\frac{ab}{p}\right) = \left(\frac{a}{p}\right) \cdot \left(\frac{b}{p}\right)$ für alle $a, b \in \mathbb{Z}$

3) $\left(\frac{ab^2}{p}\right) = \left(\frac{a}{p}\right)$ für $b \in \mathbb{Z}$ mit $p \nmid b$

4) $\left(\frac{a}{p}\right) \equiv a^{(p-1)/2} \bmod p$

Ist $n \in \mathbb{N}_+$ eine ungerade Zahl mit Primfaktorzerlegung $n = p_1^{\alpha_1} \cdots p_r^{\alpha_r}$, so definieren wir das **Jacobi-Symbol** $\left(\frac{a}{n}\right)$ durch

$$\left(\frac{a}{n}\right) = \left(\frac{a}{p_1}\right)^{\alpha_1} \cdots \left(\frac{a}{p_r}\right)^{\alpha_r}$$

b) Schreiben Sie eine *CoCoA* Funktion `Jacobi(...)`, die für zwei gegebene Zahlen $a \in \mathbb{Z}$, $n \in \mathbb{N}_+$ ungerade, das Jacobi-Symbol $\left(\frac{a}{n}\right)$ berechnet. Verwenden Sie dabei (ohne Beweis) die Formel $\left(\frac{2}{p}\right) = (-1)^{(p^2-1)/8}$ und das **quadratische Reziprozitätsgesetz** $\left(\frac{q}{p}\right) = (-1)^{(p-1)(q-1)/4} \cdot \left(\frac{p}{q}\right)$ für ungerade Primzahlen p, q. Vermeiden Sie es, die Zahlen a und n in ihre Primfaktoren zu zerlegen.

c) Sie nun $n = pq$ das Produkt zweier ungerader Primzahlen. Zeigen Sie, daß jeder quadratische Rest modulo n ein quadratischer Rest modulo p und modulo q ist. Folgern Sie ein Verfahren für die Erzeugung einer Zahl $y \in \{1, \ldots, n-1\}$ mit $\mathrm{ggT}(y, n) = 1$, die ein quadratischer Nichtrest modulo n ist und $\left(\frac{y}{n}\right) = 1$ erfüllt.

d) Implementieren Sie die Hashfunktion aus Beispiel 4.2 in einem *CoCoA* Programm `Muenzwurf(...)`, das als Eingabe ein Element von $\{0, 1\}$ und eine geeignete Zufallszahl erwartet und als Ausgabe eine große (ca. 20 stellige) Zahl liefert. Beschreiben Sie nochmals ausführlich, wie zwei *CoCoA* Anwender mit Hilfe dieses Programms den Münzwurf über das Internet bewerkstelligen können. (Die Kommunikation soll per E-Mail erfolgen.)