PD Dr. Martin Kreuzer
Fakultät für Mathematik
Universität Regensburg

Regensburg, den 24.5.2000

Übungen zur Vorlesung "Kryptographie"

Blatt 3

(Abgabetermin: 8.6.2000)

Aufgabe 12. (Babylonischer Algorithmus zur Wurzelberechnung)

a) Sei $r \in \mathbb{R}_+$ eine positive reelle Zahl. Wir definieren eine Folge $(x_i)_{i\geq 0}$ reeller Zahlen durch $x_0 = r$ und $x_{i+1} = \frac{1}{2}(x_i + \frac{r}{x_i})$ für $i \geq 0$. Beweisen Sie, daß diese Folge gegen $\sqrt{r}$ konvergiert.

b) Schreiben Sie eine *CoCoA* Funktion `Sqrt(...)`, die eine positive rationale Zahl $q \in \mathbb{Q}_+$ und eine positive ganze Zahl $n \in \mathbb{N}_+$ als Argumente hat und die $\sqrt{q}$ auf n Nachkommastellen genau berechnet.

Aufgabe 13. (Das RSA Kryptosystem)

Für das RSA Kryptosystem verwenden wir das übliche Alphabet mit 26 Buchstaben. Die Zahl $n = pq$ erfülle $26^9 < n < 26^{10}$.

a) Schreiben Sie *CoCoA* Funktionen `PreProcess(...)` und `PostProcess(...)`, die einen Klartext in eine Folge von Restklassen in $\mathbb{Z}/nZ$ umwandeln bzw. eine solche Folge in einen Geheimtext aus den 26 Buchstaben.

Hinweise: Ist die letzte Klartexteinheit zu kurz, so soll sie mit Zufallszeichen aufgefüllt werden. Finden Sie "gute" Injektionen $\mathbb{Z}/26^9\mathbb{Z} \hookrightarrow \mathbb{Z}/n\mathbb{Z} \hookrightarrow \mathbb{Z}/26^{10}\mathbb{Z}$.

b) Schreiben Sie zwei *CoCoA* Funktionen `RSAEncrypt(...)` und `RSADecrypt(...)`, die die Unterprogramme aus a) verwenden und die Verschlüsselungsfunktion $f : \mathbb{Z}/n\mathbb{Z} \longrightarrow \mathbb{Z}/n\mathbb{Z}$ $(x \mapsto x^e)$ bzw. $g : \mathbb{Z}/n\mathbb{Z} \longrightarrow \mathbb{Z}/n\mathbb{Z}$ $(x \mapsto x^d)$ implementieren.

Hinweis: Um große Potenzen x^e modulo n zu berechnen, stellt man e im Binärsystem dar und multipliziert die entsprechenden Potenzen x^{2^i}.

c) Verschlüsseln Sie die Nachricht "BITTE SOFORT DREI MILLIONEN EURO UEBERWEISEN" mit Hilfe des RSA Kryptosystems zum öffentlichen Schlüssel $(n, e) = (98\,022\,850\,618\,897, 31)$.

Aufgabe 14. (Attacken auf das RSA Kryptosystem)

a) In einer Firma wird stets das RSA Kryptosystem mit $e = 3$, aber verschiedenen $n = pq$ benutzt. Eines Tages versendet der Chef an drei Mitarbeiter die gleiche Nachricht. Erklären Sie, wie Sie die Nachricht entschlüsseln können. (Tip: Wenden Sie den Chinesischen Restsatz an.)

b) Durch einen Programmierfehler im Zufallsgenerator eines RSA Kryptosystems erhalten zwei Benutzer den gleichen RSA-Modul $n = pq$ zugeteilt. Zeigen Sie, daß jeder die Nachrichten des anderen wie folgt mitlesen kann.

1) Sei e_A der öffentliche Schlüssel des anderen, und seien e_B, d_B der öffentliche und der geheime Schlüssel des Benutzers. Er berechnet $h = (e_B d_B - 1)/\mathrm{ggT}(e_A, e_B d_B - 1)$.
2) Mit Hilfe des erweiterten Euklidischen Algorithmus findet er Zahlen $c, d \in \mathbb{Z}$ mit $c\,h + d\,e_A = 1$. (Warum geht dies?)
3) Er potenziert de Geheimtexte das anderen mit d.

c) Bei einem RSA Kryptosystem mit $n = pq$ wurden p und q sehr nahe beieinander gewählt. Zeigen Sie, daß man n wie folgt faktorisieren kann.
1) Prüfe für die ganzen Zahlen $t \geq \sqrt{n}$ der Reihe nach, ob $t^2 - n$ eine Quadratzahl ist.
2) Gilt $t^2 - n = s^2$, so setze $p = t + s$ und $q = t - s$.

d) Knacken Sie das Kryptosystem aus Aufgabe 13 c).

Aufgabe 15. (ElGamal Kryptographie mit Fermatschen Primzahlen)
Sei $p \geq 17$ eine Fermatsche Primzahl, d.h. eine Primzahl der Form $p = 2^{2^k} + 1$ mit $k \geq 2$.

a)* Beweisen Sie, daß die Restklasse von 5 die multiplikative Gruppe $(\mathbb{Z}/p\mathbb{Z})^\times$ erzeugt. (Hinweis: Verwenden Sie (ohne Beweis), daß es keine Zahl $a \in \mathbb{Z}$ gibt mit $a^2 \equiv 5 \pmod{p}$.)

b) Zeigen Sie, daß man das ElGamal Kryptosystem in $\mathbb{Z}/p\mathbb{Z}$ wie folgt knacken kann. Gegeben sei $a \in \mathbb{Z}$ und ein $g \in \mathbb{N}_+$, so daß die Restklasse von g ein Erzeuger von $(\mathbb{Z}/p\mathbb{Z})^\times$ ist. Gesucht sei ein $x \in \{0, \ldots, p-1\}$ mit $g^x \equiv a \pmod{p}$.
1) Sei $\ell = 2^k$ und sei a_0 die Restklasse von a in $\mathbb{Z}/p\mathbb{Z}$.
2) Für $j = 1, \ldots, \ell$ berechne $b_j = a_{j-1}^{2^{\ell-j}} \in \{1, -1\}$ und setze $x_{j-1} = 0$ falls $b_j = 1$ bzw. $x_{j-1} = 1$ falls $b_j = -1$. Ferner setze $g_j = g_{j-1}^2$ und $a_j = a_{j-1} \cdot g_{j-1}^{x_{j-1}}$.
3) Gib das Ergebnis $x = p - 1 - (x_0 + 2x_1 + \cdots + 2^{\ell-1}x_{\ell-1})$ aus.
Tip: Zeigen Sie $g_j = g^{2^j}$ und $a_j = g^{x_0 + 2x_1 + \cdots + 2^{j-1}x_{j-1}} \cdot a$ für $j = 0, \ldots, \ell$.

c) Bei einem ElGamal Kryptosystem mit $p = 65537$ und öffentlichem Schlüssel $5^a = 27849$ erreicht uns die Nachricht

$$(5660, 28471),\ (17747, 6537),\ (26694, 32563),\ (32609, 35447)$$

Ein Block von drei Buchstaben ABC wurde dabei in die Zahl $\alpha \cdot 26^2 + \beta \cdot 26 + \gamma$ umgewandelt, wobei α, β, γ die Nummern der entsprechenden Buchstaben sind. Entschlüsseln Sie die Nachricht!