Prof. Dr. M. Kreuzer
P. Ackermann

Abgabe: 02.05.2005, 10h

Kryptografie
Übungsblatt 3

Aufgabe 9:

a) Beweisen Sie die Endlichkeit und Korrektheit des erweiterten Euklidischen Algorithmus aus Satz 2.4.

b) Implementieren Sie diesen Algorithmus.

c) Bestimmen Sie experimentell einen Näherungswert für die Wahrscheinlichkeit, dass zwei Zufallszahlen teilerfremd sind. (Tipp für CoCoA: CoCoA-Funktion `Rand(...)` verwenden!)

Aufgabe 10:
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 Funktionen `PreProcess(...)` und `PostProcess(...)`, die einen Text in eine Folge von Restklassen in $\mathbb{Z}/n\mathbb{Z}$ umwandeln bzw. eine solche Folge in einen Text aus den 26 Buchstaben.
Hinweis: Ist die letzte Texteinheit 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 Funktionen `RSAEncrypt(...)` und `RSADecrypt(...)`, die die Unterprogramme aus a) verwenden, die Verschlüsselungsfunktion $f : \mathbb{Z}/n\mathbb{Z} \to \mathbb{Z}/n\mathbb{Z}, f(x) = x^e$ bzw. $g : \mathbb{Z}/n\mathbb{Z} \to \mathbb{Z}/n\mathbb{Z}, g(x) = x^d$ implementieren und einen Klartext (bestehend aus Buchstaben) in einen Geheimtext (bestehend aus Zahlen) verschlüsseln bzw. einen Geheimtext in einen Klartext entschlüsseln.
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 11:

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. Erlären Sie, wie Sie die Nachricht entschlüsseln können. (Tipp: 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 Nachricht 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 $ch + de_A = 1$. (Warum geht dies?)

3. Er potenziert die Geheimtexte des 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 $q = t - s$.

Aufgabe 12:
Knacken Sie das Kryptosystem und entschlüsseln Sie wieder den Geheimtext aus Aufgabe 10 c).