

9. Übungsblatt  
Kryptographie I (SS 2006)

Stefan Lucks, Emin Islam Tatli

**Besprechung:** Mittwoch, 27. Juni 2006

## Public Key Kryptographie

**Aufgabe 1** Sei  $n$  eine frei wählbare natürliche Zahl  $n$  mit  $1 < n < 2^{16}$ . Implementiere in Deiner bevorzugten Programmiersprache die folgenden Funktionen über natürlichen Zahlen  $x$  mit  $0 \leq x < n$ :

- a) Addition und Multiplikation zweier Zahlen modulo  $n$ .
- b) Berechnung des additiven und multiplikativen Inversen modulo  $n$  (also  $-x$  bzw.  $x^{-1}$ ). Zur Berechnung des multiplikativen Inversen kannst du den erweiterten Euklidischen Algorithmus verwenden.
- c) Ziehen einer zufälligen Primzahl, die höchstens so groß ist wie ein frei wählbares  $u$  ( $1 < u \leq 2^{16}$ ). Hierzu wird eine zufällige Zahl gezogen und dann geprüft, ob es sich um eine Primzahl handelt.
- d) Berechnen des größten gemeinsamen Teilers zweier Zahlen. Hierzu kann der Euklidische Algorithmus verwendet werden.

Im Folgenden sind der Euklidische und der erweiterte Euklidische Algorithmus im Pseudocode angegeben.

### Euklidischer Algorithmus

Seien  $p$  und  $q$  mit  $p \geq q$  zwei natürliche positive Zahlen. Der Euklidische Algorithmus berechnet den größten gemeinsamen Teiler (ggT) der beiden Zahlen.

1. Dividiere  $p$  ganzzahlig durch  $q$  mit Rest  $r$ .
2. Falls  $r = 0$ :  $q$  ist der gesuchte ggT. Stop.
3. Falls  $r > 0$ : Setze  $p := q$  und  $q := r$ .
4. Weiter bei 1.

### Erweiterter Euklidischer Algorithmus

Seien  $p$  und  $q$  mit  $p \geq q$  zwei natürliche positive Zahlen mit  $\text{ggT } g$ . Dann gibt es zwei ganze Zahlen  $\alpha$  und  $\beta$  mit

$$\alpha \cdot p + \beta \cdot q = g$$

Der erweiterte Euklidische Algorithmus berechnet  $\alpha$ ,  $\beta$  und  $g$ .

1. Setze  $\alpha' := 1$ ,  $\beta' := 0$ ,  $\alpha := 0$ ,  $\beta := 1$ .
2. Berechne ganzzahlige Division  $d := p/q$  mit Rest  $r$ .
3. Falls  $r = 0$ : Setze  $g := q$ . Ausgabe  $(g, \alpha, \beta)$ . Stop.
4. Falls  $r > 0$ : Setze  $(p, q, \alpha, \alpha', \beta, \beta') := (q, r, \alpha' - \alpha \cdot d, \alpha, \beta' - \beta \cdot d, \beta)$
5. Weiter bei 2.

**Aufgabe 2** Gegeben sei eine natürliche Zahl  $n \geq 2$  sowie zwei natürliche Zahlen  $a$  und  $b$ , wobei  $a < n$  ist.

- a) Entwirf einen möglichst effizienten Algorithmus, der die Funktion

$$f(a, b, n) = a^b \bmod n$$

berechnet. Diese Berechnung kann durch Ausführen von  $O(\log(b))$  Multiplikationen modulo  $n$  durchgeführt werden!

**Tipp:** überlege zunächst, wie sich beispielsweise  $7^{256} \bmod 10$  besonders clever berechnen lässt. Nutze dann die dabei gefunden Zwischenergebnisse aus, um  $7^{99} \bmod 10$  zu berechnen.

- b) Implementiere diese Potenzfunktion als Teil der obigen Programmbibliothek.

**Aufgabe 3** Führe einmal alle Rechenoperationen, die für das RSA-System erforderlich sind, von Hand durch (d.h. nur unter Verwendung eines Taschenrechners). Gegeben seien die Primzahlen  $p = 109$  und  $q = 149$ .

- a) **Schlüsselerzeugung I:** Berechne  $n$  und  $\phi(n)$ .
- b) **Schlüsselerzeugung II:** Häufig wird aus Effizienzgründen  $e = 3$  verwendet. Warum ist das hier nicht sinnvoll?
- c) **Schlüsselerzeugung III:** Wir wählen  $e = 115$ . Berechne das zugehörige  $d$ .
- d) **Ver-/Entschlüsselung:** Verschlüssele den Wert  $x = 517$ . Führe zur Probe auch die entsprechende Entschlüsselung durch.

**Bem.:** Zugegebenermaßen ist in Teil d) schon ziemlich viel Rechnerei erforderlich. So schlimm wird's in der Klausur wohl nicht werden, aber den Algorithmus aus Aufgabe 2 sollte man in jedem Fall draufhaben.

**Aufgabe 4** Der Sage nach erhielt der *Chinesische Restsatz* seinen Namen, weil ein chinesischer General ihn nutzte, um seine Armeen zu zählen. Dazu wählte er drei Primzahlen, z.B. 17, 23 und 29. Dann ließ er seine Soldaten in 17er-, 23er- und 29er-Reihen antreten und zählte jeweils nur die Soldaten, die übrig blieben. Nun konnte er den Chinesischen Restesatz benutzen, um die Größe seiner Armee zu bestimmen (solange sie weniger als  $17 \cdot 23 \cdot 29$  Soldaten umfasste).

- a) Angenommen, die Armee umfasst vor der Schlacht 8466 Mann. Wieviele Soldaten bleiben bei der ersten, zweiten bzw. dritten Zählung übrig?
- b) Als das gleiche Verfahren nach der Schlacht angewandt wird, bleiben bei den drei Zählungen 1, 20 und 8 Soldaten übrig. Benutze den Chinesischen Restesatz, um die verbleibende Größe der Armee zu bestimmen.