INSTITUT FÜR INFORMATIK
ALGORITHMEN UND KOMPLEXITÄT II
PROF. DR. JOHANNES KÖBLER

Sommersemester 2000
28. Juni 2000

Übungen zur Kryptologie

11. Übung

Abgabe am 19. Juli 2000

Aufgabe 40 (*schriftlich zu bearbeiten,* 9 Punkte)
Zeigen Sie: Folgende drei Aussagen sind für jede natürliche Zahl $m > 4$ äquivalent:

a) m ist prim,

b) $(m-1)! \equiv -1 \pmod{m}$,

c) $(m-1)! \not\equiv 0 \pmod{m}$.

Hinweis: Für primes m sind 1 und -1 die einzigen selbstinversen Elemente in $\mathbb{Z}_m^*$.

Aufgabe 41 (*schriftlich zu bearbeiten,* 3 Punkte)
Sei $n = p \cdot q$ (p, q prim). Berechnen Sie die Wahrscheinlichkeit, dass eine zufällig gewählte Zahl $\leq n-1$ einen Faktor mit n gemeinsam hat.

Aufgabe 42 (*schriftlich zu bearbeiten,* 16 Punkte)
Betrachten Sie folgendes Kryptosystem (nach Pohlig, Hellman): Sei p eine große Primzahl.

$$M := C := \{1, \ldots, p-1\};$$
$$K := K' := \{1 \leq k \leq p-2 : \mathrm{ggT}(k, p-1) = 1\};$$
$$E(m,k) := D(m,k) := m^k \text{ MOD } p.$$

Zeigen Sie:

a) Die Bedingung $D(E(m,k), k') = m$ ist genau dann für alle $m \in M$ erfüllt, wenn $k \cdot k' \equiv 1 \pmod{p-1}$ ist.

b) Es handelt sich um ein symmetrisches System, d.h. k' ist aus k und k ist aus k' leicht zu berechnen.

c) Bestimmen Sie m mit $E(m, 9) = 1669$, falls $p = 1823$ ist.

d) Überlegen Sie sich, wie das Verfahren so modifiziert werden könnte, dass ein Nachrichtenaustausch zwischen je zwei Teilnehmern möglich ist, ohne dass vorher ein geheimer Schlüssel vereinbart werden müsste. (No-Key-System von Shamir)
Hinweis: Jeder Teilnehmer besitzt ein geheimes Schlüsselpaar k, k'. Zum Senden einer Nachricht von Teilnehmer A zu Teilnehmer B müssen insgesamt drei Kryptotexte zwischen A und B verschickt werden: erst von A zu B, dann von B zurück zu A und zuletzt wieder von A zu B.

Aufgabe 43

Zeigen Sie:

a) Jede Carmichael-Zahl n ist quadratfrei, d. h. es gibt keine natürliche Zahl $m > 1$ so dass m^2 ein Teiler von n ist.

b) Eine Zahl n ist genau dann eine Carmichael-Zahl, wenn sie ungerade, zusammengesetzt und quadratfrei ist, und wenn für jeden Primteiler p von n die Zahl $p - 1$ ein Teiler von $n - 1$ ist.

c) Jede Carmichael-Zahl ist das Produkt von mindestens drei verschiedenen Primzahlen.

d) Ist $n = 561 = 3 \cdot 11 \cdot 17$ eine Carmichael-Zahl?

Aufgabe 44

a) Verschlüsseln Sie die Nachricht 444 nach dem RSA-Verfahren, falls $e = 613$ und $n = 989$ ist.

b) Entschlüsseln Sie die Nachricht 444, d. h. bestimmen Sie die Nachricht m für die gilt $E(m,\ (613, 989)) = 444$.

Aufgabe 45

Bestimmen Sie die Nachricht m, die unter dem RSA-Verfahren mit den beiden Schlüsseln $(e_1, n) = (1\,453, 450\,397)$ und $(e_2, n) = (2\,039, 450\,397)$ verschlüsselt wurde:

$$E(m,\ (1\,453, 450\,397)) = 257\,614 \quad \text{und} \quad E(m,\ (2\,039, 450\,397)) = 173\,394.$$

Aufgabe 46

Wir betrachten ein Public-Key-System mit bekanntem Schlüssel k und Verschlüsselungsfunktion E_k. Sei c ein abgefangener Kryptotext. Zeigen Sie, dass man mit folgendem Verfahren immer in endlicher Zeit den Klartext bestimmen kann.

a)
$x := c$
while $E_k(x) \neq c$ do $x := E_k(x)$ od
output x.

b) Wenden Sie das Verfahren beim RSA-Verfahren an, mit öffentlichem Schlüssel $(17,\ 2773)$ und $c = 1504$.