Institut für Informatik
Algorithmen und Komplexität II
Prof. Dr. Johannes Köbler

Sommersemester 2000
26. April 2000

Übungen zur Kryptologie

2. Übung

Abgabe am 3. Mai 2000

Aufgabe 5 (*schriftlich zu bearbeiten,* 4 Punkte)
Zeigen Sie, die Zahlen 0, …, $m-1$ bilden zusammen mit der Addition und Multiplikation modulo m

a) einen Ring,

b) einen Körper genau dann, wenn m eine Primzahl ist.

Aufgabe 6 (*schriftlich zu bearbeiten,* 4 Punkte)
Beweisen Sie den Satz aus der Vorlesung: Seien b, k und m ganze Zahlen mit $m \geq 1$, $b \neq 0$. Dann besitzt die lineare Kongruenzgleichung

$$bx \equiv_m k$$

genau dann eine eindeutige Lösung $x \in \{0, \ldots, m-1\}$, wenn $\text{ggT}(b, m) = 1$ ist.
Folgern Sie daraus, dass die Chiffrierfunktion $E_{b,c} : A \to A$ (A sei ein m-elementiges Alphabet) gegeben durch

$$E_{b,c}(x) = bx + c$$

genau dann injektiv ist, wenn $\text{ggT}(b, m) = 1$ ist.

Aufgabe 7 (*schriftlich zu bearbeiten,* 8 Punkte)
Betrachten Sie die folgenden Prozeduren

a) Euklid(a, b)
   /∗ Berechnet $\text{ggT}(a, b)$ ∗/
   if $b = 0$ then
      return a
   else
      return Euklid$(b, a \bmod b)$.

b) Extended-Euklid(a, b)
   /∗ Berechnet ein Tripel (w, x, y) mit $w = \text{ggT}(a, b) = ax + by$ ∗/
   if $b = 0$ then
      return $(a, 1, 0)$
   else
      (d, x', y'):= Extended-Euklid$(b, a \bmod b)$;
      $(d, x, y) := (d, y', x' - \lceil a/b \rceil \cdot y')$;
   return (d, x, y).

Zeigen Sie die Korrektheit der Algorithmen.

Aufgabe 8 (*schriftlich zu bearbeiten,* 4 Punkte)

Professor Oley schlägt eine Variante der affinen Chiffre vor. Als Schlüssel werden zwei Zahlen b, c verwendet. Verschlüsselt wird nach der Vorschrift $x \mapsto b(x+c)$ mod m. Begutachten Sie seinen Vorschlag.

Aufgabe 9 (*schriftlich zu bearbeiten,* 8 Punkte)

Dechiffrieren Sie folgende Kryptotexte:

a) 0413 2322 1334 0304 3230 2421 4301 1324 3302 1310 1032 0441 0432 3302 1221 4004 3333 0421 3404 3234 0443 34

b) ejft fwpo bvhv tuvt wfsx foef ufdb ftbs dijg gsfj tuxp imbv dimb vdim fjdi uavl obdl fo

c) azfx fscf wcrh saft zccf oxfz yfsl kkzy fyvu zkks fmfs xvuo hfxx focj dfyy fyxz fafy xvuo hfxx fofst zccf oy

d) 6011 6066 8200 8360 1808 4689 0160 2016 8200 0131 0506 6240 1040 4836 0182 8402 0506 6066 1893 4071 0124 8482 36011 0405 2480 8609 1052 0961 8101 6070 7601 2484 4010 7048 4014 16150 50201 1821 8318 4890 582 0705 61 066 83684 18784 020 503 601