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

Sommersemester 2000
19. April 2000

Übungen zur Kryptologie

1. Übung

Abgabe am 26. April 2000

Aufgabe 1 (*schriftlich zu bearbeiten,* 8 Punkte)
Verschlüsseln Sie den Klartext

„VERSCHLUESSELNSIEMICHGUT“

a) mittels einer Skytale mit Umfang 4 Buchstaben,

b) mittels einer Zick-Zack-Transposition der Höhe 3,

c) mittels einer Matrix-Transposition mit folgender Spaltenpermutation π

i	1	2	3	4	5	6
$\pi(i)$	4	6	1	3	2	5

,

d) mittels einer Block-Transposition gegeben durch die obige Permutation.

Aufgabe 2 (*schriftlich zu bearbeiten,* 6 Punkte)
Betrachten Sie die oben definierte Permutation π.

a) Geben Sie π in Zyklenschreibweise an.

b) Geben Sie einen Graphen an mit einer Hamiltonlinie, die π definiert.

c) Geben Sie ein Merkwort (Schlüsselwort) an, durch das π gemäß dem in der Vorlesung angegeben Verfahren bestimmt wird.

Aufgabe 3 (*schriftlich zu bearbeiten,* 8 Punkte)
Entschlüsseln Sie die folgenden Kryptotexte:

a) WLDI NLOT EFEE RERT RAAM BUSC UAEN KHFN SGYT SBCE TEOE HIAN LIRI

b) KNE CEL LOE SIS IKK NHU ENE NID EZZ CTC ESN ESA SS

c) PBR SRI EIO ENE SHC NIA HDC UAI EMT LSM TSE IEB LKT XOM RTC AIR API ONO TNS SIC HFE EIR RNF ITK RTE ZYO XXP TTY

d) NNNO UEIC NHIN EFEH EABC CKLT ONSR PAIT OISZ UOMN SCAH BSSL XU

Als *Hilfestellung*, die häufigsten Bigramme im Deutschen:

er en ch de ei nd te in ie ge es ne un st re he an be

Aufgabe 4 (*schriftlich zu bearbeiten,* 6 Punkte)
Zeigen Sie:

a) Eine Permutation π ist involutorisch genau dann, wenn alle Zyklen in der Zyklendarstellung von π maximal die Länge 2 besitzen.

   Eine Permutation ist echt involutorisch genau dann, wenn alle Zyklen die Länge 2 haben.

b) Für jede Permutation π gibt es eine Zahl $k > 0$ so, dass π^k (d. h. π k-mal hintereinander ausgeführt) die Identität liefert.

   (Hinweis: Betrachten Sie die Zyklendarstellung)

c) Die Ordnung einer Permutation π sei definiert durch

$$\mathrm{ord}(\pi) \; = \; \min\{k > 0 \mid \pi^k \text{ ist die Identität}\}\,.$$

   Besteht die Zyklendarstellung von π aus r Zyklen der Längen l_1, l_2, ..., l_r, so ist die Ordnung von π das kleinste gemeinsame Vielfache von l_1, l_2, ..., l_r:

$$\mathrm{ord}(\pi) \; = \; \mathrm{kgV}(l_1, \ldots, l_r)\,.$$

Literatur zur Vorlesung:

F.L. Bauer, Kryptologie, Springer 1993

A. Beutelspacher, Kryptologie, Vieweg 1993

A. Beutelspacher, J. Schwenk, K.-D. Wolfenstetter,
Moderne Verfahren der Kryptographie, Vieweg 1995

G. Brassard, Modern cryptology, Springer 1988

J. Buchmann, Einführung in die Kryptographie, Springer 1999

E. Kranakis, Primality and cryptography, Wiley 1986

A. J. Menezes and Oorschot, P. C. van and S. A. Vanstone,
Handbook of Applied Cryptography, CRC Press, 1997

A. Salomaa, Public-Key Cryptography, Springer 1990

B. Schneier, Applied Cryptography, Wiley 1994

D.R. Stinson, Cryptography: Theory and Practice, CRC Press, 1995

D. Welsh, Codes and cryptography, Oxford 1988