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

Sommersemester 2000
24. Mai 2000

Übungen zur Kryptologie

6. Übung

Abgabe am 7. Juni 2000

Aufgabe 24 (*schriftlich zu bearbeiten,* 16 Punkte)
Sei $L \subseteq \{\mathrm{A}, \ldots, \mathrm{Z}\}^*$ die deutsche Sprache (mit aufgelösten Umlauten und Scharf-s und ohne Zwischenräume und Sonderzeichen).

a) Bestimmen Sie $H(L_1)$ und $R_{\mathrm{abs}}(L_1)$.

b) Ein Schätzwert für die Redundanz der deutschen Sprache ist $3,5$. Wir nehmen im folgenden an, dass die Schlüssel jeweils unter Gleichverteilung gezogen werden. Geben Sie die untere Schranke

$$\frac{H(K)}{R_{\mathrm{abs}}(L)}$$

für die Eindeutigkeitsdistanzen der folgenden Kryptosysteme an:

(i) additive Chiffre.
(ii) multiplikative Chiffre.
(iii) affine Chiffre.
(iv) Vigenère Chiffre der Länge $d \geq 2$.
(v) einfache Substitution.
(vi) Blocksubstitution auf Blöcken der Länge $d \geq 2$.
(vii) Blocktransposition der Länge $d \geq 2$.

Verwenden Sie ggf. die Stirling'sche Formel: $n! \sim \sqrt{2\pi n}\left(\frac{n}{e}\right)^n$.

c) Geben Sie für jeden der obigen Punkte einen möglichst langen Kryptotext an, der mittels zwei verschiedenen Schlüsseln aus zwei Klartexten der deutschen Sprache hervorgeht (wählen Sie ggf. jeweils ein $d \leq 5$).

d) Begründen Sie: Gibt es für zwei mögliche Schlüssel k_1 und k_2 ($k_1 \neq k_2$) mögliche Klartexte $x_1, x_2 \in \{\mathrm{A}, \ldots, \mathrm{Z}\}^n$ mit

$$E(k_1, x_1) = E(k_2, x_2)\,,$$

dann ist die Eindeutigkeitsdistanz größer n.

Aufgabe 25 (*schriftlich zu bearbeiten,* 12 Punkte)

a) Definieren Sie formal, wann zwei Kryptosysteme als gleich (besser: isomorph) anzusehen sind. Betrachten Sie zunächst den Fall ohne Wahrscheinlichkeitsverteilungen.

b) Nun sei zusätzlich pro Kryptosystem eine Wahrscheinlichkeitsverteilung über die Schlüssel gegeben. Modifizieren Sie Ihre Definition geeignet.

c) Sei nun S_1 eine additive Chiffre und S_2 eine multiplikative Chiffre über dem üblichen Alphabet. Wir nehmen an, die Schlüssel werden jeweils unter Gleichverteilung gewählt. Zeigen Sie mittels Ihrer Definition

   (i) $S_1 \times S_2 = S_2 \times S_1$,

   (ii) $S_1 \times S_1 = S_1$.

   Gilt dies bei beliebigen Verteilungen auf den Schlüsseln?