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

Sommersemester 2000
17. Mai 2000

Übungen zur Kryptologie

5. Übung

Abgabe am 31. Mai 2000

Aufgabe 19 (*schriftlich zu bearbeiten,* 4 Punkte)
Entschlüsseln Sie die folgenden Kryptotexte (mit englischen Klartexten).

a) (Hinweis: Lauftext-Verschlüsselung mittels englischem Text)

`MOIKIRGTEZUSSYKRCSKCZXHPVGKKFXDPXJEFTFZELL`

b) (Hinweis: Beide Kryptotexte wurden durch das gleiche *one-time tape* aus Klartexten erzeugt, die beide mit TH beginnen.)

`LKLBYQGDVVSMBVLNMOHRYHPROWMEINCBQALO`

`LKLANKHAEXSFEFEKOFWWSITPGKFTUFACFUWU`

Aufgabe 20 (*schriftlich zu bearbeiten,* 6 Punkte)
Gegeben sei folgendes Kryptosystem: $M = \{a, b, c\}$ mit $p(a) = 1/2$, $p(b) = 1/3$ und $p(c) = 1/6$. $K = \{k_1, k_2, k_3\}$ mit $p(k_1) = 1/2$, $p(k_2) = 1/4$, $p(k_3) = 1/4$ und $C = \{1, 2, 3, 4\}$. Die Verschlüsselungsfunktion ist definiert durch

E	a	b	c
k_1	1	2	3
k_2	2	3	4
k_3	3	4	1

a) Berechnen Sie die (bedingten) Wahrscheinlichkeiten $p(x)$ und $p(x|y)$ für alle Klartextnachrichten $x \in M$ und Kryptotextnachrichten $y \in C$.

b) Berechnen Sie die Entropie $H(X)$ der Klartexte, sowie die Entropie $H(K)$ des Schlüsselraumes und die Entropie $H(Y)$ der Kryptotexte.

c) Berechnen Sie die bedingten Entropien $H(X|Y)$ und $H(K|Y)$.

Aufgabe 21 (*schriftlich zu bearbeiten,* 6 Punkte)
Zeigen Sie das Lemma aus der Vorlesung

a) $H(X, Y) = H(Y, X)$,

b) $H(X, Y) = H(X|Y) + H(Y) = H(Y|X) + H(X)$,

c) $H(X, Y) = H(X) + H(Y)$, falls X und Y unabhängig sind.

Zusatz: Es gilt sogar $H(X,Y) < H(X) + H(Y)$, falls X und Y nicht unabhängig sind. D. h. auch die Umkehrung von c) gilt. Zeigen Sie diese Behauptung!

Sie können dazu die Jensen'sche Ungleichung verwenden: Ist f eine stetige, streng konkave Funktion (d.h. $f(\frac{x+y}{2}) > \frac{f(x)+f(y)}{2}$) und sei $g_i \in [0,1]$ für $1 \leq i \leq n$ und $g_1 + \cdots + g_n = 1$, dann gilt für alle $x_1, \ldots, x_n$ aus dem Definitionsbereich von f,

$$g_1 f(x_1) + \cdots + g_n f(x_n) \leq f(g_1 x_1 + \cdots + g_n x_n) .$$

Dabei ergibt sich Gleichheit genau dann, wenn $x_1 = \ldots = x_n$

Aufgabe 22 (*schriftlich zu bearbeiten,* 7 Punkte)

Im folgenden betrachten wir ausschließlich Kryptosysteme, bei denen der Schlüssel unabhängig vom Klartext gewählt wird. Wir nehmen auch an, dass alle Werte in K, M, C möglich sind (d.h. eine Wahrscheinlichkeit > 0 besitzen).

Beweisen Sie folgende Aussagen.

a) In jedem Kryptosystem ist $\|M\| \leq \|C\|$.

b) Ein Kryptosystem ist absolut sicher, wenn für alle Klartexte x und alle Kryptotexte y gilt: $\sum_{E(k,x)=y} p(k) = 1/\|M\|$.

c) Ein Kryptosystem mit $\|C\| = \|M\|$ ist genau dann absolut sicher, wenn für alle Klartexte x und alle Kryptotexte y gilt: $\sum_{E(k,x)=y} p(k) = 1/\|M\|$.

d) Ein Kryptosystem mit $\|K\| < \|M\|$ kann nicht absolut sicher sein.

e) Ein Kryptosystem mit $\|K\| < \|C\|$ kann nicht absolut sicher sein.

f) Ein Kryptosystem ist genau dann absolut sicher, wenn $H(X|Y) = H(X)$ ist.

g) Ist ein Kryptosystem sicher, dann ist es für alle Apriori-Wahrscheinlichkeitsverteilungen sicher (d.h., auch wenn die Klartexte unter anderer Wahrscheinlichkeitsverteilung auftreten. Ein sicheres Kryptosystem für deutsche Klartexte, ist also auch für englische Klartexte sicher).

Aufgabe 23 (*schriftlich zu bearbeiten,* 6 Punkte)

Zeigen Sie oder widerlegen Sie folgende Aussagen (es gelte die Vorbemerkung von Aufgabe 22):

a) Ist ein Kryptosystem absolut sicher, so gilt $p(y_1) = p(y_2)$ für alle $y_1, y_2 \in C$.

b) In einem absolut sicheren Kryptosystem gilt $H(X) \leq H(K)$.

c) In jedem Kryptosystem gilt $H(K|Y) \geq H(X|Y)$.