Übungen zur Kryptologie 1 Sommersemester 2002

Johannes Köbler/Olaf Beyersdorff

Übungsblatt 7

Aufgabe 25

Zeigen Sie:

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

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

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

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

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

f) Ist ein Kryptosystem absolut sicher, dann ist es für alle Apriori-Wahrscheinlichkeitsverteilungen absolut sicher (also unabhängig davon, mit welchen Wahrscheinlichkeiten die Klartexte auftreten). Ein sicheres Kryptosystem für deutsche Klartexte, ist somit auch für englische Klartexte sicher.

Aufgabe 26 (schriftlich, 10 Punkte)

Zeigen oder widerlegen Sie folgende Aussagen:

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 $H(K|Y) \geq H(X|Y)$.

Aufgabe 27

Seien S_1 und S_2 Vigenère-Chiffren mit Schlüsselwortlänge d_1 bzw. d_2.

a) Zeigen Sie: Ist d_1 ein Teiler von d_2, so gilt $S_1 \times S_2 = S_2$.

b) Lässt sich Teilaufgabe a) verallgemeinern zu $S_1 \times S_2 = S_3$, wobei S_3 die Vigenère-Chiffre mit Schlüsselwortlänge $d = \mathrm{kgV}(d_1, d_2)$ ist?