Wolfgang K. Seiler
Tel. 2515

B6, B4.08

21. September 2022

3. Übungsblatt Kryptologie

Aufgabe 1:
Das Mannheimer Institut für Deutsche Sprache hat auf der Grundlage einer Textsammlung aus 147 148 193 692 Buchstaben folgende Buchstabenhäufigkeiten berechnet:

A	B	C	D	E
0,060067477706	0,021480751076	0,026900980520	0,047182137047	0,160061266048
F	G	H	I	J
0,018323709896	0,030642574549	0,042497859499	0,077526004178	0,002978121104
K	L	M	N	O
0,015368289907	0,037871919697	0,027983071757	0,096608077356	0,026841202334
P	Q	R	S	T
0,010497044240	0,000282903133	0,077377610953	0,063439603408	0,063693071514
U	V	W	X	Y
0,038209944546	0,009188013866	0,014275418694	0,000517091308	0,001079873609
Z	ß	Ä	Ö	Ü
0,012376156182	0,001706185925	0,005489485951	0,002698198599	0,006835955398

a) Berechnen Sie daraus die Tabelle der Häufigkeiten die entsteht, wenn man ß durch SS, Ä durch AE, Ö durch OE und Ü durch UE ersetzt!

b) Berechnen Sie sodann für $n = 0, \ldots, 25$ die Summen $\sum_{i=1}^{26} p_i p_{i \oplus n}$, wobei p_i die Häufigkeit des i-ten Buchstaben bezeichnet und $i \oplus n = i + n$ ist für $i + n \leq 26$ und $i + n - 26$ sonst!

c) Berechnen Sie auch für jedes n die Korrelation zwischen den Häufigkeiten der Buchstaben des Alphabets und des zyklisch um n verschobenen Alphabets!

Aufgabe 2:
Welche Elemente von Konfusion und Diffusion haben die in der Vorlesung betrachteten klassischen Kryptoverfahren von Caesar, Vigenère, die allgemeine monoalphabetische Substitution sowie die Transpositionschiffre?

Aufgabe 3:
Entschlüsseln Sie das erste Kryptogramm von Aufgabe 3 des zweiten Übungsblatts!

Aufgabe 4:
In einem Feistel-Netzwerk wird ein Nachrichtenblock $(L_0, R_0) \in \mathbb{F}_2^N \times \mathbb{F}_2^N$ in r Schritten transformiert zu einem Block (R_r, L_r), wobei gilt $L_i = R_{i-1}$ und $R_i = f(s_i, R_{i-1}) \oplus L_{i-1}$ für $i \geq 1$ mit der Feistel-Funktion $f\colon \mathbb{F}_2^k \times \mathbb{F}_2^N \to \mathbb{F}_2^N$ und dem i-ten Rundenschlüssel s_i.

a) Wie kann man aus (R_r, L_r) und den s_i die Nachricht (L_0, R_0) rekonstruieren?

b) Angenommen, $k = N$, alle Rundenschlüssel s_i sind gleich einem festen Schlüssel $s \in \mathbb{F}_2^N$ und $f(s, R_{i-1}) = s \oplus R_{i-1}$, wobei $\oplus$ die Addition im Vektorraum $\mathbb{F}_2^n$ bezeichnet. Ist das (für hinreichend große N) ein sicheres Kryptoverfahren?

c) Welcher Bedingung muß f mindestens genügen, damit Shannons Forderungen nach Konfusion und Diffusion erfüllt sind?

Besprechung am Mittwoch, dem 28. September 2022, um 15.30 Uhr