Geheime Botschaften

Sommersemester 2017

Dr. T. Moede
t.moede@tu-bs.de
Universitätsplatz 2, Raum 426
0531 391-7527

Technische Universität Braunschweig

Übungsblatt 2

Aufgabe 1. (Minimaler Koinzidenzindex)
Seien $p_0, \ldots, p_{25}$ die Häufigkeiten der Buchstaben $a, \ldots, z$ in einem Text.

- Zeigen Sie, dass gilt:
$$\sum_{i=0}^{25} p_i^2 = \frac{1}{26} + \sum_{i=0}^{25} \left(p_i - \frac{1}{26}\right)^2.$$
- Benutzen Sie dies, um zu folgern, dass immer gilt:
$$\sum_{i=0}^{25} p_i^2 \geq \frac{1}{26}.$$
In welchem Fall gilt hier Gleichheit?

Aufgabe 2. (Vigenère-Chiffren und Autokorrelation)
Jemand schlägt Ihnen folgendes Verfahren zur Bestimmung der Schlüssellänge einer Vigenère-Chiffre vor:

- Betrachte für hinreichend viele Zahlen i den Geheimtext und darunter einen um i Stellen verschobenen Geheimtext.
- Zähle die Anzahl der Übereinstimmungen von direkt übereinanderstehenden Buchstaben.
- Bestimme die Zahlen i, für welche die Anzahl an Übereinstimmungen möglichst groß ist, und lese die Schlüssellänge aus den Abständen dieser Zahlen i ab.

Funktioniert dieses Verfahren?

Aufgabe 3. (ADFGX)

„Die manuelle Verschluesselung von Texten ist wirklich anstrengend.“

Sie verspüren den Drang den obigen Text durch das **ADFGX**-Verfahren mit den Schlüsselwörtern **SCHLUESSEL** und **LANGSCHNABELIGEL** zu verschlüsseln. Dazu gehen sie wie folgt vor:

Schritt 1 (Substitution):
Sie schreiben zeilenweise das erste Schlüsselwort in das folgende Schema (ohne Wiederholung von doppelten Buchstaben). Danach füllen Sie den Rest mit den verbliebenen Buchstaben des Alphabets in umgekehrter Reihenfolge und ohne den Buchstaben **j**.

	A	D	F	G	X
A					
D					
F					
G					
X					

Sie ersetzen nun den Buchstaben durch das Paar, welches Sie am Rand des ADFGX-Schemas ablesen können (erst Zeile, dann Spalte).

D	i	e	m	a	n	u	e	l	l	e	V	e	r	s	c	h	l	u	e	s	s	e	l	u	n	g
v	o	n	T	e	x	t	e	n	i	s	t	w	i	r	k	l	i	c	h	a	n	s	t	r	e	n
g	e	n	d																							

Schritt 2 (Transposition):
Sie erstellen nun ein weiteres Schema mit Spaltenanzahl entsprechend der Länge des zweiten Schlüsselworts. Die Buchstaben dieses Schlüsselwortes nummerieren Sie in alphabetischer Reihenfolge (bei mehrfach vorkommenden Buchstaben von links nach rechts).

L	A	N	G	S	C	H	N	A	B	E	L	I	G	E	L
11	1	14	7	S	4	9	15	2	3	5	12	10	8	6	13

Sie tragen nun den in Schritt 1 substituierten Text zeilenweise in das Schema ein und erhalten den Geheimtext durch spaltenweises Ablesen (in der Reihenfolge der Nummerierung).