Mathematische Methoden in der Kommunikationstheorie

(Sommersemester 2018)

Dr. Tobias Moede
t.moede@tu-bs.de
Universitätsplatz 2, Raum 515
0531 391-7516

Alexander Cant, M.Sc.
a.cant@tu-bs.de
Universitätsplatz 2, Raum 515
0531 391-7516

Technische Universität Braunschweig

Übungsblatt 1

(Präsenzübung am 13.04.2018)

Aufgabe 1. (Vigenère-Chiffre – Verschlüsselung & Entschlüsselung)

Ver- und Entschlüsselung werden beim Vigenère-Verfahren mit Hilfe des sogenannten **Vigenère-Quadrates** durchgeführt (siehe Seite 3). Es handelt sich um eine Menge periodisch verwendeter Verschiebechiffren. Wir schreiben zur Unterscheidung Klartexte klein, Geheimtexte & Schlüssel groß.

- Verschlüsseln sie den Text **supergeheim** mit dem Schlüssel **KEKS**.
- Entschlüsseln sie den Text **WEOVDOEPKNMO** mit dem Schlüssel **ECHIDNA**.

Aufgabe 2. (Vigenère-Chiffre – Kryptoanalyse)

- Überlegen Sie sich, warum es zum Brechen der Vigenère-Chiffre ausreicht die Schlüssellänge zu bestimmen.
- Betrachten Sie zwei identische Klartextfolgen. Machen Sie sich klar: Wenn die jeweiligen Anfangsbuchstaben unter dem gleichen Schlüsselbuchstaben stehen, dann wird die komplette Folge identisch verschlüsselt. Dies tritt genau dann auf, wenn der Abstand der Anfangsbuchstaben ein Vielfaches der Schlüssellänge ist!
- **(Kasiski-Test)**: Suchen Sie nun umgekehrt möglichst lange gleiche Buchstabenfolgen im verschlüsselten Text. Sie können nun vermuten, dass Ihr Abstand ein Vielfaches der Schlüssellänge ist.
- **(Friedman-Test)**: Berechnen Sie eine Abschätzung für die Schlüssellänge h mit Hilfe der Formel

$$h \approx \frac{(\kappa_{deu} - \frac{1}{26})n}{\kappa(n-1) - \frac{1}{26}n + \kappa_{deu}}$$

  wobei $\kappa_{deu} \approx 0.0762$ der **Koinzidenzindex** der deutschen Sprache, n die Länge des Textes, n_i die Anzahl des Auftretens des i-ten Buchstaben ($n_0 \mathrel{\hat{=}}$ Anzahl der a's, ...) und

$$\kappa = \frac{\sum_{i=0}^{25} n_i(n_i - 1)}{n(n-1)}$$

  der **Koinzidenzindex** des Textes sind.
- Entschlüsseln Sie den Vigenère-verschlüsselten Text auf Seite 2. Nutzen Sie dabei die aus Kasiski- & Friedman-Test bestimmbare Schlüssellänge und Häufigkeitsanalyse für die auftretenden Verschiebechiffren.

```
EYRYC  FWLJH  FHSIU  BHMJO  UCSEG  TNEER  FLJLV  SXMVY
SSTKC  MIKZS  JHZVB  FXMXK  PMMVW  OZSIA  FCRVF  TNERH
MCGYS  OVYVF  PNEVH  JAOVW  UUYJU  FOISH  XOVUS  FMKRP
TWLCI  FMWVZ  TYOIS  UUIIS  ECIZV  SVYVF  PCQUC  HYRGO
MUWKV  BNXVB  VHHWI  FLMYF  FNEVH  JAOVW  ULYER  AYLER
VEEKS  OCQDC  OUXSS  LUQVB  FMALF  EYHRT  VYVXS  TIVXH
EUWJG  JYARS  ILIER  JBVVF  BLFVW  UHMTV  UAIJH  PYVKK
VLHVB  TCIUI  SZXVB  JBVVP  VYVFG  BVIIO  VWLEW  DBXMS
SFEJG  FHFVJ  PLWZS  FCRVU  FMXVZ  MNIRI  GAESS  HYPFS
TNLRH  UYR
```

Vigenère-verschlüsselter Text zu Aufgabe 2

Blaise de Vigenère (5. April 1523 – 19. Februar 1596)

a	b	c	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z
A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A
C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B
D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C
E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D
F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E
G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F
H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G
I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H
J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I
K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J
L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K
M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L
N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M
O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N
P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O
Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P
R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q
S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R
T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S
U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T
V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U
W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V
X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W
Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X
Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y

Hilfsmittel: Das Vigenère-Quadrat

$\mathbf{E_K(m)}$: Wir schreiben wiederholt das Schlüsselwort K über den zu verschlüsselnden Text m. Der jeweilige Geheimtextbuchstabe ist dann der Schnittpunkt der Zeile, die mit dem Schlüsselwortbuchstaben beginnt, mit der Spalte, die mit dem jeweiligen Klartextbuchstaben beginnt.

$\mathbf{D_K(c)}$: Wir schreiben wiederholt das Schlüsselwort K über den zu entschlüsselnden Text c. Dann suchen wir in der Zeile, die mit dem jeweiligen Schlüsselwortbuchstaben beginnt, den Geheimtextbuchstaben und entschlüsseln ihn zu dem in dieser Spalte stehenden Klartextbuchstaben.