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

Sommersemester 2000
10. Mai 2000

Übungen zur Kryptologie

4. Übung

Abgabe am 24. Mai 2000

Aufgabe 15 (*schriftlich zu bearbeiten,* 9 Punkte)

a) Beschreiben Sie einen *Angriff bei bekanntem Klartext* auf eine Hill-Chiffre (der Schlüssel soll ermittelt werden).

b) Bestimmen Sie die Schlüsselmatrix einer Hill-Chiffre, die die Klartextsequenz „`KLARTEXTZEICHEN`“ auf die Kryptotextsequenz „`ufakmrnuvwcsbfd`“ abbildet.

c) Betrachten Sie folgenden Angriff auf eine Hill-Chiffre mit kleiner Blocklänge l (und bekanntem Kryptotext).

Der Kryptotext wird in Blöcke von jeweils l Buchstaben (l-Gramme) unterteilt. Auf diesen l-Grammen wird eine Häufigkeitsanalyse durchgeführt. Häufige l-Gramme im Kryptotext gehen vermutlich auf l-Gramme zurück, die in der Klartextsprache häufig vorkommen. Mit den vermuteten Klartext/Kryptotext-Paaren wird wie im Aufgabenteil a) versucht, die Schlüsselmatrix zu bestimmen.

Verwenden Sie diesen Ansatz, um für $l = 2$ den folgenden Kryptotext, der aus einem englischen Klartext entstanden ist, zu entschlüsseln.

```
FC QG EB AU UG EB FC KM WQ LC EB SP WQ MW SG KJ JL LP
WQ FC YU KE DX KF NT KA SE XD UG EB FC KZ QX DZ AT
```

Hinweis: `TH` und `IN` sind im Englischen häufig.

Aufgabe 16 (*schriftlich zu bearbeiten,* 3 Punkte)

Führen Sie die Entschlüsselung einer Autokey-Chiffre mit Klartext-Schlüsselstrom und einem Schlüsselwort der Länge d auf die Entschlüsselung einer Vigenére-Chiffre mit einem Schlüsselwort der Länge $2d$ zurück.

Aufgabe 17 (*schriftlich zu bearbeiten,* 4 Punkte)

Folgender Kryptotext wurde durch ein Vigenère-System aus einem englischen Klartext erzeugt.

```
LBRKN HVYAL MUGOY VUPIO VJYNK GHUBR PJRJC RFWRG ZVFXR HYAVY
ALQBJ ENKJB KMVTF RTOGA ZUWCF DYSLU YGHRO CGZBV KJEGF REQVL
BBMNN FSUWF CGLJA NUAHF MZSAW VWHGZ YYHBR EULEU XWHBH LBYLR
KMNLU YD
```

Bestimmen Sie die verwendete Periode nach den Methoden von Kasiski und Friedman (Koinzidenzindex) und führen Sie eine statistische Analyse durch, um den Schlüssel zu ermitteln.

Aufgabe 18 (*schriftlich zu bearbeiten,* 12 Punkte)

a) Sei $A = \{\mathtt{A}, \ldots, \mathtt{Z}\}$. Seien $p_{\mathtt{A}}, \ldots, p_{\mathtt{Z}}$ beliebige reele Zahlen. Sei d ein Buchstabe. Zeigen Sie, dass die Funktion $K : A \to \mathbb{R}$ mit

$$K(d) \;=\; \sum_{a \in A} p_a p_{a+d}$$

für $d = \mathtt{A}$ maximal wird.

Hinweis: Benützen Sie die Ungleichung

$$x_1^2 + x_2^2 + \cdots + x_n^2 \geq x_1 x_2 + x_2 x_3 + \cdots + x_{n-1} x_n + x_n x_1 \,.$$

(wobei Gleichheit genau dann gilt, wenn alle x_i identisch sind).

Zusatz: Zeigen Sie, dass diese Ungleichung gilt.

b) Seien nun c_1 und c_2 Kryptotexte, die mittels einer additiven Chiffre und den Schlüssel k_1 bzw. k_2 aus zwei Klartexten derselben (unbekannten) Sprache entstanden sind. Wie kann man die Erkenntnis aus Teil a) benützen, um ein d mit $k_1 + d = k_2$ zu erhalten?

c) Ein genügend großer Klartext aus einer unbekannten Sprache sei mittels Vigenère-Chiffre verschlüsselt worden. Erklären Sie, wie die Entschlüsselung des Kryptotext auf die Entschlüsselung einer additiven Chiffre auf einem Krytpotext derselben Länge zurückgeführt werden kann.

d) Verwenden Sie die Methode an folgendem Kryptotext (Schlüssellänge 4)

```
HUDS KUAE ZGXR AVTF PGWS WGWS ZHTP PBIL LRTZ PZHW LOIJ
VFIC VBTH LUGI LGPR KHWM YHTI UAXR BHTW UCGX OSPW AOCH
IMCS YHWQ HWCF YOCG OGTZ LBIL SWBF LOHX ZWSI ZVDS ATGS
THWI SSUX LMTS MHWI KSPX OGWI HRPF LSAM USUV VAIL LHGI
LHWV VIVL AVTW OCIJ PTIC MSTX VII
```

Der häufigste Klartextbuchstabe ist `E`.

Vigenère-Tableau:

	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25
0	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
1	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
2	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
3	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
4	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
5	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
6	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
7	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
8	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
9	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
10	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
11	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
12	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
13	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
14	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
15	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
16	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
17	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
18	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
19	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
20	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
21	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
22	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
23	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
24	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
25	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

Buchstaben- und Bigramm-Häufigkeiten in einem deutschen Klartext (Quelle: Winnetou 1, K.May, http://karlmay.uni-bielefeld.de/kmg/primlit/reise/winn_1/win1.zip). Angaben in Promille bzw. 1000tel Prozent.

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
60	19	37	47	176	15	27	59	79	2	11	32	26	104	25	5	0	68	68	56	43	6	24	0	0	10

	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	23	450	324	71	493	67	261	155	27	2	14	472	218	970	2	53		464	751	326	704	23	65	0	1	24
B	92	1	0	15	1131	1	22	6	119	1	3	112	6	7	30	0		127	54	96	57	1	13		0	7
C	4		0		1			3451	1		213	0			6			5				0			0	
D	864	37	5	153	1880	27	45	40	779	10	20	42	45	42	105	7	1	88	161	18	207	28	95		5	31
E	220	443	246	497	272	275	450	705	2179	23	163	664	521	4173	26	44	3	3499	1567	595	470	85	326	3	4	116
F	199	10	0	72	337	87	21	6	60	3	6	60	22	13	102	2		125	27	90	188	4	17			12
G	188	14		54	1571	11	29	20	77	4	17	103	18	32	17	1	0	139	95	193	104	12	30		0	17
H	821	65	1	233	1096	40	89	92	387	18	43	198	260	384	216	12	1	556	182	784	167	55	177			55
I	37	43	1728	122	1491	43	328	471	17	2	11	180	138	1754	52	7		519	465	483	18	6	10	0	0	18
J	94				90				0						1						16					
K	128	5	1	9	345	2	7	4	60		6	93	2	15	222	1		51	23	89	66	3	10		0	8
L	315	86	150	126	647	19	55	19	486	2	15	460	22	41	76	7		3	245	274	118	13	28		5	21
M	305	34	0	68	587	23	48	57	546	8	23	43	242	29	79	40	1	27	96	65	153	19	56		1	25
N	585	214	11	1928	1291	133	696	252	800	53	274	112	250	726	174	39	1	77	885	450	495	104	586		1	221
O	14	82	208	99	299	46	49	117	16	2	11	285	134	340	6	33		400	124	91	65	14	90	0	1	6
P	99		0	1	47	110	0	2	22		0	20	0	0	12	17		76	4	46	27	0	0		1	0
Q																					13					
R	587	192	60	675	961	178	230	238	428	30	192	170	212	383	178	29	1	122	540	420	410	89	276		7	154
S	390	68	654	191	1200	55	155	104	774	15	48	47	101	75	460	135	5	26	891	980	113	60	214		1	70
T	339	58	1	326	2023	54	115	118	387	25	36	110	125	95	168	6	0	178	336	321	238	61	264		1	213
U	34	90	289	80	688	290	130	66	18	3	23	48	254	1278	3	51	0	277	377	191	24	23	42	0		13
V	18			0	217		0		70			0			302						0					
W	572	1		1	737	0	5	4	638		30		1	1	272			0	2		112		1		1	0
X	1				1				1							0				1			0			0
Y	2	2	0	1	2	1	1	1	1	0	0	1	1	1	5	0		1	2	1	1	0	2		0	1
Z	33	6	1	12	163	2	11	2	51	0	1	12	2	2	19	1		2	5	85	524	5	75		0	8