Die Ressourcenuniversität. Seit 1765.

Melanie Nentwich

Polygraphische Systeme

Digraphische Hill-Systeme

15. April 2011

Seminarvortrag zur mathematischen Vertiefungsrichtung
Mathematische Methoden der Informatik

Teil I.

Einführung

Definitionen

Chiffrierung: Verschlüsselung eines Textes (encryption)

Dechiffrierung: Entschlüsselung eines Textes (decryption)

Kryptanalyse: Analyse von Chiffrierverfahren, um diese zu brechen [2]

Digraphen: Buchstabenpaare

Trigraphen: Buchstabentripel

Historie der Verschlüsselung 1 [3]

Altertum:	■ Skytale ■ Caesar-Chiffre
Mittelalter:	■ sieben Verschlüsselungsmethoden des Roger Bacon
Neuzeit:	■ Chiffrierscheibe ■ Vignère-Chiffre ■ Voynich-Manuskript (ungelöst)
19. Jhd.:	■ Beale-Chiffre (ungelöst) ■ Dorabella Chiffre (ungelöst)
1. Weltkrieg:	■ ADFGX-Verfahren der Deutschen

Historie der Verschlüsselung 2 [3]

Verschlüsselung mit Maschine:

- One-Time-Pad
- Kryha-Maschine
- Hagelin-Maschinen
- Enigma

Verschlüsselung mit Computer:

- Data Encryption Standard (DES)
- publik-key Kryptographie (z. B. RSA)
- Pretty Good Privacy (PGP)

Allgemeine Hilfsmittel

- Häufigkeitstafel der Buchstaben des Geheimtextes
- Trigraphentafel zur Bestimmung von Wiederholungen
- Häufigkeiten von Buchstaben, Digraphen und Trigraphen einer Sprache bekannt
- measure of roughness M. R. (ca. 0,028 in englischen Texten [1])

$$\text{M. R.} = \sum_{i=A}^{i=Z} \left(\frac{f_i}{N} - \frac{1}{26} \right)^2 = \sum_{i=A}^{i=Z} \left(\frac{f_i}{N} \right)^2 - \frac{1}{26}$$

- index of coincidence I. C. (ca. 0,066 in englischen Texten [1])

$$\text{I. C.} = \frac{1}{N(N-1)} \sum_{i=A}^{i=Z} f_i \left(f_i - 1 \right)$$

- Länge des Textes N, absolute Häufigkeit f_i des Buchstabens i

Teil II.

Digraphische Hill-Systeme

Chiffrierung

Grundlagen

- Klartextalphabet: $\mathtt{A}$ bis $\mathtt{Z}$, Geheimtextalphabet: $\mathtt{a}$ bis $\mathtt{z}$
- Ersetzen der Buchstaben $\mathtt{A}$ bis $\mathtt{Z}$ durch Zahlen 1 bis 26
  $\rightarrow$ „Rechnen“ mit Text modulo 26
- Ersetzen von Klartextdigraphen K_1K_2 durch Geheimtextdigraphen G_1G_2 mittels Matrix A

$$\begin{pmatrix} G_1 \\ G_2 \end{pmatrix} \equiv A \begin{pmatrix} K_1 \\ K_2 \end{pmatrix} \equiv \begin{pmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \end{pmatrix} \begin{pmatrix} K_1 \\ K_2 \end{pmatrix} \mod 26$$

$$G_1 \equiv a_{11}K_1 + a_{12}K_2 \mod 26$$

$$G_2 \equiv a_{21}K_1 + a_{22}K_2 \mod 26$$

- Auslöschung der monoalphabetischen Häufigkeiten

Beispiel

- Klartext: `PREPARE TO EVACUATE AT ONCE`
  Länge: 23 (ungerade), daher Auffüllen nötig, z. B. mit `X`
- Matrix $A = \begin{pmatrix} 7 & 9 \\ 3 & 12 \end{pmatrix}$
- `PR` $\rightarrow$ 16 18:

$$\begin{pmatrix} 7 & 9 \\ 3 & 12 \end{pmatrix} \begin{pmatrix} 16 \\ 18 \end{pmatrix} \equiv \begin{pmatrix} 274 \\ 264 \end{pmatrix} \equiv \begin{pmatrix} 14 \\ 04 \end{pmatrix}$$

  14 04 $\rightarrow$ `nd`
- `PR EP AR ET OE VA CU AT EA TO NC EX`
  `nd wy mk gu ta gz ba ei ra of uz qq`

Probleme und Behebung

Probleme: hoher Rechenaufwand, hohe Fehlerwahrscheinlichkeit

Behebung:

- Skalierung von K_1 bzgl. G_1: $a_{11}K_1$ als 7er-Reihe mod 26
- analog: Skalierung von K_1, K_2 bzgl. G_1, G_2
- für PR:

$$G_1 \equiv a_{11}K_1 + a_{12}K_2 \equiv 8 + 6 \equiv 14$$
$$G_2 \equiv a_{21}K_1 + a_{22}K_2 \equiv 22 + 8 \equiv 30 \equiv 4$$

K_1, K_2	A	B	C	D	E	F	G	H	I	J	K	L	M
$a_{11}K_1$	7	14	21	2	9	16	23	4	11	18	25	6	13
$a_{21}K_1$	3	6	9	12	15	18	21	24	1	4	7	10	13
$a_{12}K_2$	9	18	1	10	19	2	11	20	3	12	21	4	13
$a_{22}K_2$	12	24	10	22	8	20	6	18	4	16	2	14	26

K_1, K_2	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
$a_{11}K_1$	20	1	**8**	15	22	3	10	17	24	5	12	19	26
$a_{21}K_1$	16	19	**22**	25	2	5	8	11	14	17	20	23	26
$a_{12}K_2$	22	5	14	23	**6**	15	24	7	16	25	8	17	26
$a_{22}K_2$	12	24	10	22	**8**	20	6	18	4	16	2	14	26

Dechiffrierung

Vorgehen

- Umwandlung der Geheimtextdigraphen G_1G_2 in Klartextdiagraphen K_1K_2 mit Hilfe der Inversen A^{-1} zu $A \mod 26$

$$\begin{pmatrix} K_1 \\ K_2 \end{pmatrix} \equiv A^{-1} \begin{pmatrix} G_1 \\ G_2 \end{pmatrix} \mod 26$$

- Bestimmung von A^{-1} mit $d = |A| = a_{11}a_{22} - a_{12}a_{21}$ [1]:

$$A^{-1} = \frac{1}{d} \begin{pmatrix} a_{22} & -a_{12} \\ -a_{21} & a_{11} \end{pmatrix}$$

- Existenz von $\frac{a_{ij}}{d}$, falls d nicht teilbar durch 2 und 13 (hinreichend und notwendig) [1]

Beispiel, Fortsetzung

- $A = \begin{pmatrix} 7 & 9 \\ 3 & 12 \end{pmatrix}$, damit $\det A = 7 \cdot 12 - 3 \cdot 9 = 57 \equiv 5$ und

$$A^{-1} = \frac{1}{5}\begin{pmatrix} 12 & -9 \\ -3 & 7 \end{pmatrix} \equiv 21 \begin{pmatrix} 12 & 17 \\ 23 & 7 \end{pmatrix} \equiv \begin{pmatrix} 252 & 357 \\ 483 & 147 \end{pmatrix}$$
$$\equiv \begin{pmatrix} 18 & 19 \\ 15 & 17 \end{pmatrix}$$

- Geheimtext: `ndwym kguta gzbae iraof uzqq`
- `nd` $\rightarrow$ 14 04:

$$\begin{pmatrix} 18 & 19 \\ 15 & 17 \end{pmatrix} \begin{pmatrix} 14 \\ 04 \end{pmatrix} \equiv \begin{pmatrix} 328 \\ 278 \end{pmatrix} \equiv \begin{pmatrix} 16 \\ 18 \end{pmatrix}$$

16 18 $\rightarrow$ `PR`

Kryptanalyse

Beispieltext

```
BPCNT QZVNS CWVWZ GBPRI IBYLA CULBP DEZSB PECLE UKGXQ
AGPCW FKIZX GOZCZ KWUUN TRWBP MBGHD IKGPH BEPDQ AGPPM
SUZPX WDSIU GQYTG MKJDS JOKOG MKGGX UHPMK MXAPH LSBIG
RQFOQ IZYLB QSUAG TMNYT GTUJO YSLSA YBUYL VVUUT GBPAT
IZYXC ZKWUU NTXJF QBPHY TQNVR IOPKK EIAGP MSUZP ALZSK
APIQK NNULB PBWGM GCONM BAOAG WBNMZ MONBP DEXGB PNSWB
ACYLJ ZQAKM ESNIZ PBPXG MSZPY LBQUL BPTQB QYLGM RVDEK
MRJQM KTBQB PRIAS TEULM WKWRG CDPMS UZPUH IBQDX GYQOQ
ULNMZ MGZGR MWKWW BBPAT CHYXQ QNNNG DEYLF JSNXG LBBAN
PPOEH XOONB QTXKV BIIUL OWFFM ONDBO ECRUU SUKMO NYNOV
```

450 Zeichen
ursprüngliche Sprache: Englisch
aus [1], Übung 73

Häufigkeitsverteilung

Buchstabe	A	B	C	D	E	F	G	H	I	J	K	L	M
f_i	17	34	12	11	12	6	30	8	15	7	20	18	24
f_i/N in %	3,8	7,6	2,7	2,4	2,7	1,3	6,7	1,8	3,3	1,6	4,4	4,0	5,3

Buchstabe	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
f_i	23	18	32	22	10	18	15	25	8	16	14	16	19
f_i/N in %	5,1	4,0	7,1	4,9	2,2	4,0	3,3	5,6	1,8	3,6	3,1	3,6	4,2

- M. R. $= 0,0073 \ll 0,028$
- häufigster englischer Buchstabe: E, mit Wahrscheinlichkeit 13%
- häufigster Buchstabe des Textes: B, mit Wahrscheinlichkeit $7,6\%$
- Ausschluss einer monoalphabetischen Verschlüsselung

$\rightarrow$ polyalphabetische Verschlüsselung? Analyse der Wiederholungen mit Hilfe einer Trigraphentabelle

Trigraphentabelle, A – M

A	B	C	D	E	F	G	H	I	J	K	L	M
LC	·P	PN	PE	DZ	WK	ZB	GD	RI	KD	UG	YA	PB
QG	GP	SW	HI	PC	QO	KX	PB	IB	SO	FI	UB	PS
QG	IY	AU	PQ	LU	JQ	AP	UP	KZ	UO	ZW	CE	GK
XP	LP	EL	WS	BP	LJ	XO	PL	DK	XF	IG	HS	GK
UG	SP	PW	JS	KI	WF	BH	PY	SU	LZ	MJ	YB	PK
SY	WP	ZZ	PE	DX	FM	KP	UI	BG	RQ	OO	SS	KX
PT	MG	XZ	VE	MS		AP	CY	QZ	FS	MG	YV	TN
IG	HE	GO	CP	DK		UQ	EX	TZ		MM	AZ	PS
PL	SI	AY	QX	TU		TM		RO		ZW	UB	GG
KP	LQ	GD	GE	DY		OM		EA		PK	YJ	NB
BO	YU	TH	NB	OH		KG		PQ		KE	YB	NZ
OG	GP	ER		OC		GX		NZ		SA	UB	ZO
BC	QP					IR		RA		QN	YG	KE
QK	LP					AT		HB		AM	UM	GS
IS	PW					TT		BI		EM	UN	GR
PT	MA					TB		IU		MT	YF	KR
BN	WN					AP				WW	GB	QK
	NP					WM				WW	UO	LW
	GP					MC				XV		PS
	WA					AW				UM		NZ
	PP					XB						ZG
	...					...						...

Trigraphentabelle, N – Z

N	O	P	Q	R	S	T	U	V	W	X	Y	Z
CT	GZ	BC	TZ	PI	NC	NQ	CL	ZN	CV	GQ	BL	QV
VS	JK	BR	XA	TW	ZB	NR	EK	WW	VZ	ZG	QT	WG
UT	KG	BD	DA	GQ	MU	YG	WU	LV	CF	PW	ZL	ES
MY	FQ	BE	GY	VI	DI	GM	UN	VU	KU	GU	NT	IX
UT	JY	GC	RF	MV	DJ	YG	SZ	NR	RB	MA	OS	OC
QV	IP	BM	OI	MJ	LB	GU	IG	RD	XD	YC	AB	CK
KN	CN	GH	BS	PI	QU	UG	XH	KB	KU	TJ	UL	UP
NU	AA	ED	FB	WG	YL	AI	SA	O·	BG	EG	ZX	IY
OM	MN	GP	TN	GM	LA	NX	TJ		GB	PG	HT	IY
BM	QQ	PM	IK	CU	MU	YQ	BY		SB	PL	CL	CK
OB	PE	ZX	ZA		ZK	PQ	VU		MK	DG	QL	UP
PS	XO	HM	BU		NW	KB	UT		KR	YQ	GQ	LS
SI	ON	AH	TB		EN	SE	WU		MK	NG	HX	MM
LM	LW	BA	BY		MZ	AC	UN		KW	HO	EL	JQ
QN	MN	BH	JM		AT	QX	SZ		WB	TK	NN	IP
NN	BE	OK	BB		MU		NL		OF			SP
NG	MN	GM	BD		JN		QL					UP
SX	NV	ZA	YO		UU		EL					MM
AP		AI	OU				SZ					GG
OB		BB	XQ				PH					
OD		BD	QN				QL					
...		...	...				...					

Analyse der Wiederholungen

Wiederholungen	Position erster Buchstabe		Intervall	Faktoren
CZKWUUNT	59	185	126	2, 3, 3, 7
PMSUZP	89	215	126	2, 3, 3, 7
MWKW	335	371	36	2, 2, 3, 3
QAGP	45	85	40	2, 2, 2, 5
ULBP	27	233	206	2, 103
YLBQ	143	295	152	2, 2, 2, 19
BPDE	29	259	230	2, 5, 23
BPRI	17	325	308	2, 2, 7, 11
BPAT	177	377	200	2, 2, 2, 5, 5
NMZM	254	363	110	2, 5, 11

- einziger gemeinsamer Teiler: 2
  $\rightarrow$ dialphabetische Verschlüsselung möglich
- I. C. $= 0,0431$, Hinweis auf etwa 5 Alphabete

$\rightarrow$ digraphische Verschlüsselung? Analyse der Digraphentafel

Digraphentabelle, A – M

	A	B	C	D	E	F	G	H	I	J	K	L	M
A	0	0	2	0	0	0	3	0	0	0	0	1	0
B	1	0	0	0	1	0	0	0	2	0	0	0	0
C	0	0	0	1	0	0	0	1	0	0	0	0	0
D	0	1	0	0	4	0	0	0	1	0	0	0	0
E	0	0	1	0	0	0	0	1	1	0	0	0	0
F	0	0	0	0	0	0	0	0	0	1	1	0	1
G	0	0	1	0	0	0	0	1	0	0	0	0	4
H	0	0	0	0	0	0	0	0	0	0	0	0	0
I	0	2	0	0	0	0	0	0	0	0	0	0	0
J	0	0	0	0	0	0	0	0	0	0	0	0	0
K	1	0	0	0	0	0	2	0	0	1	1	0	4
L	0	1	0	0	1	0	0	0	0	0	0	0	0
M	0	2	0	0	0	0	0	0	0	0	0	0	0
N	0	0	0	0	0	0	1	0	1	0	0	0	2
O	0	0	0	0	1	0	0	0	0	0	0	0	0
P	0	0	0	1	0	0	0	2	1	0	0	0	4
Q	3	0	0	1	0	1	0	0	0	0	1	0	1
R	0	0	0	0	0	0	1	0	3	1	0	0	0
S	0	0	0	0	0	0	0	0	0	0	0	0	0
T	0	0	0	0	1	0	2	0	0	0	0	0	1
U	0	0	0	0	0	0	0	2	0	0	1	5	0
V	0	0	0	0	0	0	0	0	0	0	0	0	0
W	0	3	0	0	0	1	0	0	0	0	0	0	0
X	1	0	0	0	0	0	5	0	0	1	0	0	0
Y	0	0	0	0	0	0	0	0	0	0	0	7	0
Z	0	0	0	0	0	0	1	0	0	0	0	0	2

Digraphentabelle, N – Z

	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
A	0	1	0	0	0	1	2	0	0	0	0	1	0
B	0	0	14	5	0	0	0	1	0	1	0	0	0
C	1	0	0	0	1	0	0	0	0	2	0	0	2
D	0	0	0	0	0	2	0	0	0	0	0	0	0
E	0	0	0	0	0	1	0	0	0	0	0	0	0
F	0	0	0	1	0	0	0	0	0	0	0	0	0
G	0	0	2	1	2	0	0	0	0	0	2	0	1
H	0	0	0	0	0	0	0	0	0	0	0	1	0
I	0	0	0	0	0	0	0	2	0	0	0	0	3
J	0	2	0	0	0	0	0	0	0	0	0	0	1
K	0	1	0	0	0	0	1	0	1	4	0	0	0
L	0	1	0	0	0	2	0	0	0	0	0	0	0
M	0	0	0	0	0	1	0	0	0	2	0	0	0
N	2	0	1	0	0	2	2	0	1	0	0	1	0
O	5	0	1	2	0	0	0	0	1	0	0	0	1
P	0	1	0	0	0	0	0	0	0	0	0	0	0
Q	0	0	0	1	0	0	0	0	0	0	0	0	0
R	0	0	0	0	0	0	0	0	1	1	0	0	0
S	1	0	0	0	0	0	0	5	0	0	0	0	0
T	0	0	0	3	0	0	0	1	0	0	1	0	0
U	0	0	0	0	0	0	0	4	0	0	0	0	0
V	0	0	0	0	0	0	0	0	1	1	0	0	0
W	0	0	0	0	0	0	0	0	0	0	0	0	0
X	0	1	0	0	0	0	0	0	0	1	0	0	0
Y	1	0	0	1	0	1	1	0	0	0	2	0	0
Z	0	0	5	0	0	2	0	0	1	0	0	0	0

I. C. und M. R. der Digraphen

$$\text{M. R.} = \sum_{i=AA}^{i=ZZ} \left(\frac{f_i}{N}\right)^2 - \frac{1}{26^2}, \qquad \text{I. C.} = \frac{1}{N(N-1)} \sum_{i=AA}^{i=ZZ} f_i(f_i - 1)$$

- Anzahl der Digraphen N, absolute Häufigkeit f_i des Digraphen i
- vorgelegter Text:
  - M. R. $= 0,012960$
  - I. C. $= 0,010040$
- durchschnittlicher, englischer Text (berechnet nach [1], Appendix A):
  - M. R. $= 0,009152$
  - I. C. $= 0,009137$
- gute Übereinstimmung der I. C.-Werte, hohe Wahrscheinlichkeit einer digraphischen Verschlüsselung

Analyse der Digraphen

- häufigster englischer Digraph: `th`
- häufigster Geheimtextdigraph: `BP`
- Annahme 1: `BP` entspricht `th`
- Annahme 2: `th` stets gefolgt von `e`
- Folgedigraphen von `BP` mit Positionen im Alphabet:
  - `AT` $\rightarrow$ 01 20
  - `BW` $\rightarrow$ 02 23
  - `CN` $\rightarrow$ 03 14
  - `DE` $\rightarrow$ 04 05
  - `EC` $\rightarrow$ 05 03
  - `HY` $\rightarrow$ 08 25
  - `MB` $\rightarrow$ 13 02
  - `NS` $\rightarrow$ 14 19
  - `RI` $\rightarrow$ 18 09
  - `TQ` $\rightarrow$ 20 17
  - `XG` $\rightarrow$ 24 07

Analyse der Digraphen

- Kongruenz einiger Digraphen ($K_1 = b_{11}G_1 + b_{12}G_2$):

$$02b_{11} + 23b_{12} \equiv 5 \qquad 18b_{11} + 09b_{12} \equiv 5$$
$$04b_{11} + 05b_{12} \equiv 5 \qquad 20b_{11} + 17b_{12} \equiv 5$$
$$14b_{11} + 19b_{12} \equiv 5 \qquad 24b_{11} + 07b_{12} \equiv 5$$

- Subtraktion einer Äquivalenz von der vorherigen: $2b_{11} + 8b_{12} \equiv 0$
- zwei Lösungen:

$$\left(\begin{array}{cc|c} 4 & 5 & 5 \\ 2 & 8 & 0 \end{array}\right) \rightsquigarrow \left(\begin{array}{cc|c} 0 & -11 & 5 \\ 2 & 8 & 0 \end{array}\right)$$
$$\left(\begin{array}{cc|c} 0 & 3 & 1 \\ 2 & 8 & 0 \end{array}\right) \rightsquigarrow \left(\begin{array}{cc|c} 0 & 1 & 9 \\ 2 & 0 & 0 \end{array}\right)$$
$$\left(\begin{array}{cc|c} 0 & 1 & 9 \\ 2 & 0 & 6 \end{array}\right) \Rightarrow b_{12} \equiv 9, b_{11} \equiv 3 \text{ oder } b_{11} \equiv 16$$

1. Fall: $b_{12} \equiv 9, b_{11} \equiv 16$

- Test: $G_1 b_{11} + G_2 b_{12} \equiv K_1$ mit $G_1 G_2 \equiv \texttt{BP}$, $K_1 \equiv \texttt{t}$:
  $16 \cdot 2 + 9 \cdot 16 \equiv 176 \equiv 20 \rightarrow \texttt{t}$
- weitere Folgebuchstaben von `th`:
  - `CN`: $3 \cdot 16 + 14 \cdot 9 \equiv 174 \equiv 18 \rightarrow \texttt{r}$
  - `EC`: $5 \cdot 16 + 3 \cdot 9 \equiv 107 \equiv 3 \rightarrow \texttt{c}$
  - `MB`: $13 \cdot 16 + 2 \cdot 9 \equiv 226 \equiv 18 \rightarrow \texttt{r}$
  - `AT`: $1 \cdot 16 + 20 \cdot 9 \equiv 196 \equiv 14 \rightarrow \texttt{n}$
  - `HY`: $8 \cdot 16 + 25 \cdot 9 \equiv 353 \equiv 15 \rightarrow \texttt{o}$
- Informationen über b_{21}, b_{22} durch $\texttt{BP} \rightarrow \texttt{th}$:
  $2 \cdot b_{21} + 16 \cdot b_{22} \equiv 8$
  zwei Lösungen

1. Fall: $b_{12} \equiv 9, b_{11} \equiv 16$

```
BP CN TQ ZV NS CW VW ZG BP RI IB YL AC UL BP DE ZS BP
th r_ e_ p_ e_ u_ m_ k_ th e_ f_ n_ q_ b_ th e_ o_ th

EC LE UK GX QA GP CW FK IZ XG OZ CZ KW UU NT RW BP MB
c_ c_ s_ p_ u_ v_ u_ m_ n_ e_ f_ v_ s_ e_ b_ a_ th r_
```

- AC UL $\rightarrow$ q_ b_
- q häufig gefolgt von u im Englischen
- qu stets gefolgt von einem Vokal; hier aber b
- auch sonst keine sinnvollen Kombinationen

$\rightarrow$ Verwerfen

2. Fall: $b_{12} \equiv 9, b_{11} \equiv 3$

- Test: $G_1 b_{11} + G_2 b_{12} \equiv K_1$ mit $G_1 G_2 \equiv \texttt{BP}$, $K_1 \equiv \texttt{t}$:
  $3 \cdot 2 + 9 \cdot 16 \equiv 150 \equiv 20 \rightarrow \texttt{t}$
- weitere Folgebuchstaben von `th`:
  - `CN`: $3 \cdot 3 + 14 \cdot 9 \equiv 135 \equiv 5 \rightarrow \texttt{e}$
  - `EC`: $5 \cdot 3 + 3 \cdot 9 \equiv 42 \equiv 16 \rightarrow \texttt{p}$
  - `MB`: $13 \cdot 3 + 2 \cdot 9 \equiv 57 \equiv 5 \rightarrow \texttt{e}$
  - `AT`: $1 \cdot 3 + 20 \cdot 9 \equiv 183 \equiv 1 \rightarrow \texttt{a}$
  - `HY`: $8 \cdot 3 + 25 \cdot 9 \equiv 249 \equiv 15 \rightarrow \texttt{o}$
- Informationen über b_{21}, b_{22} durch $\texttt{BP} \rightarrow \texttt{th}$:

$$2 \cdot b_{21} + 16 \cdot b_{22} \equiv 8 \tag{1}$$

zwei Lösungen

2. Fall: $b_{12} \equiv 9, b_{11} \equiv 3$

```
BP CN TQ ZV NS CW VW ZG BP RI IB YL AC UL BP DE ZS BP
th e_ e_ p_ e_ h_ m_ k_ th e_ s_ a_ d_ o_ th e_ o_ th

EC LE UK GX QA GP CW FK IZ XG OZ CZ KW UU NT RW BP MB
p_ c_ f_ c_ h_ i_ h_ m_ a_ e_ s_ i_ f_ r_ n_ a_ th e_
```

- `BP EC` $\rightarrow$ `th p_`, unwahrscheinliche Kombination, daher Wortende zwischen Digraphen
- `EC LE UK GX` $\rightarrow$ `p_ c_ f_ c_`; Annahme: `pacific_`:

$$\texttt{EC}: 05b_{21} + 03b_{22} \equiv 1 \quad (2)$$

$$\texttt{LE}: 12b_{21} + 05b_{22} \equiv 9 \quad (3)$$

$$\texttt{UK}: 21b_{21} + 11b_{22} \equiv 9 \quad (4)$$

2. Fall: $b_{12} \equiv 9, b_{11} \equiv 3$

- Lösen des LGS, impliziert von (2), (3)

$$\left(\begin{array}{cc|c} 5 & 3 & 1 \\ 12 & 5 & 9 \end{array}\right) \quad \rightsquigarrow \quad \left(\begin{array}{cc|c} -1 & 15 & 5 \\ 12 & 5 & 9 \end{array}\right)$$

$$\left(\begin{array}{cc|c} 1 & 11 & 21 \\ 12 & 5 & 9 \end{array}\right) \quad \rightsquigarrow \quad \left(\begin{array}{cc|c} 1 & 11 & 21 \\ 0 & 3 & 17 \end{array}\right)$$

$$\left(\begin{array}{cc|c} 1 & 11 & 21 \\ 0 & 1 & 23 \end{array}\right) \quad \rightsquigarrow \quad \left(\begin{array}{cc|c} 1 & 0 & 2 \\ 0 & 1 & 23 \end{array}\right)$$

$$\Rightarrow \quad b_{21} \equiv 2, b_{22} \equiv 23$$

- Test mit (4): $21 \cdot 2 + 11 \cdot 23 \equiv 295 \equiv 9$
- Test mit (1): $2 \cdot 2 + 16 \cdot 23 \equiv 372 \equiv 8$
- Lösungsmatrix: $\begin{pmatrix} 3 & 9 \\ 2 & 23 \end{pmatrix}$

kompletter Klartext

```
BP CN TQ ZV NS CW VW ZG BP RI IB YL AC UL BP DE ZS BP EC LE UK GX QA GP CW FK
th ep eo pl ew ho ma ke th ei sl an ds of th es ou th pa ci fi ct he ir ho me

IZ XG OZ CZ KW UU NT RW BP MB GH DI KG PH BE PD QA GP PM SU ZP XW DS IU GQ YT
ar ea sd if fe re nt as th et op og ra ph yo ft he ir is la nd se ac hg ro up

GM KJ DS JO KO GM KG GX UH PM KM XA PH LS BI GR QF OQ IZ YL BQ SU AG TM NY TG
ha sr ac ia lc ha ra ct er is ti cs ph ys ic al ap pe ar an ce la ng ua ge ss

TU JO YS LS AY BU YL VV UU TG BP AT IZ YX CZ KW UU NT XJ FQ BP HY TQ NV RI OP
oc ia ls ys te ms an dd re ss th at ar ed if fe re nt fr om th os eo fn ei gh

KK EI AG PM SU ZP AL ZS KA PI QK NN UL BP BW GM GC ON MB AO AG WB NM ZM ON BP
bo ri ng is la nd gr ou ps ye ta ll of th em ha ve on et hi ng in co mm on th

DE XG BP NS WB AC YL JZ QA KM ES NI ZP BP XG MS ZP YL BQ UL BP TQ BQ YL GM RV
es ea th ew in ds an dt he ti de sa nd th ea bu nd an ce of th eo ce an ha rv

DE KM RJ QM KT BQ BP RI AS TE UL MW KW RG CD PM SU ZP UH IB QD XG YQ OQ UL NM
es ti nf lu en ce th ei rw ay of li fe mo st is la nd er sl iv ea ty pe of co

ZM GZ GR MW KW WB BP AT CH YX QQ NN NG DE YL FJ SN XG LB BA NP PO EH XO ON BQ
mm un al li fe in th at ch ed vi ll ag es an dh av ea br oa df am il yc on ce

TX KV BI IU LO WF FM ON DB OE CR UU SU KM ON YN OV
pt wh ic hg oe sb ey on db lo od re la ti on sh ip
```

The people who make the islands of the south pacific their home are as different as the topography of their islands. Each group has racial characteristics. Physical appearance, languages, social systems and dress that are different from those of neighboring islandgroups, yet all of them have one thing in common: the sea, the winds and the tides and the abundance of the ocean harvest influence their way of life. Most islanders live a type of communal life in that ch ed villages and have a broad family concept which goes beyond blood relationship.

Teil III.

Ausblick

Ausblick

- Hill-Systeme mit $n \geqslant 3$ [1]
- Permutation der Alphabete (A $\equiv$ 5, B $\equiv$ 18, C $\equiv$ 2, . . .), Anzahl der Unbekannten steigt von 4 auf 30 [1]
- Playfair-Verschlüsselung, [1] [4]

Teil IV.

Quellen

Quellen

[1] Abraham Sinkov, Elementary Cryptanalysis – A Mathematical Approach, The Mathematical Association of America, 1966

[2] http://de.wikipedia.org/wiki/Kryptanalyse,
letzte Änderung: 17. Januar 2011 um 23:15 Uhr

[3] http://de.wikipedia.org/wiki/Geschichte_der_Kryptographie,
letzte Änderung: 25. Januar 2011 um 21:05 Uhr

[4] http://de.wikipedia.org/wiki/Playfair,
letzte Änderung: 3. Januar 2011 um 16:59 Uhr