College Cryptografie

Cursusjaar 2003

Analyse van Polyalfabetische Substitutie

7 februari 2003

Alfabet matching

Kasiski analyse

Kulp-letter

Crib dragging

Generatrix methode

Nihilist substitutie

Gemengd pt-alfabet

Symmetrie in positie

Isomorfie

ONDERWERPEN

Periodieke polyalfabetische substitutie met normaal alfabet
o.a. Vigenère, Beaufort, Porta.

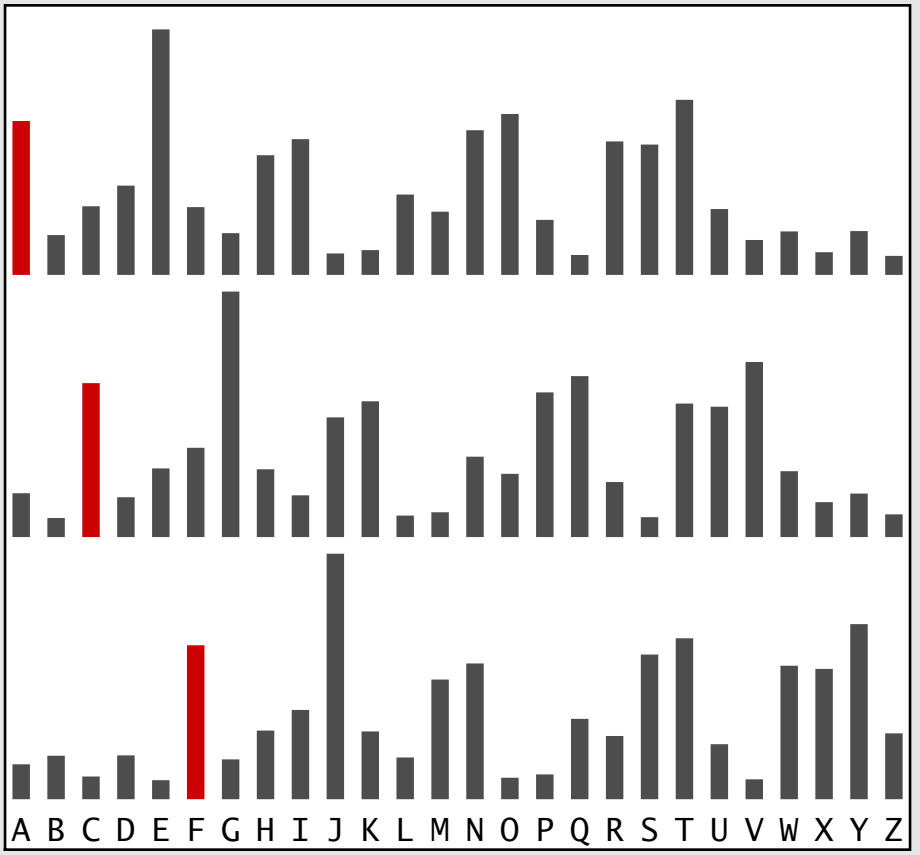
startpunt: bepaal de periode

- alfabet matching
- Kasiski analyse
- waarschijnlijk woord
- speciaal geval: Porta
- selecteren generatrix
- speciaal geval: Nihilist

Vigenère
sleutel ACF

Engelse standaard
frequenties

klaartekst A
A–Z = cijfertekst

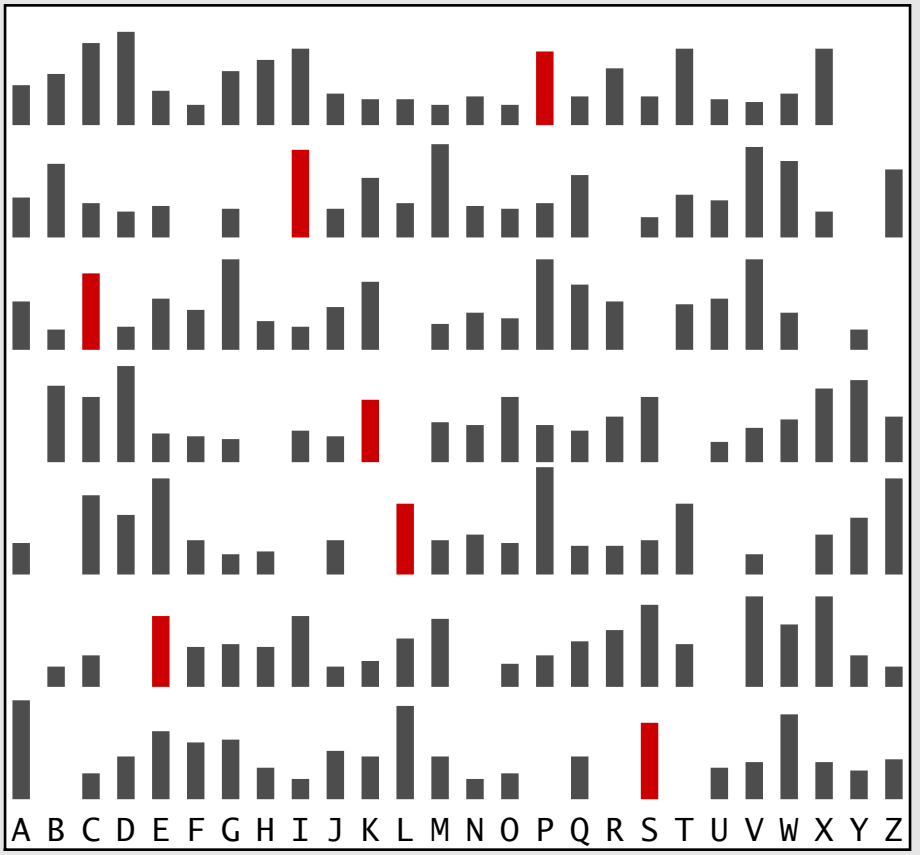


Alfabet matching

Vigenère
sleutel PICKLES

1673 letters
239 per sleutelletter

klaartekst A
A–Z = cijfertekst



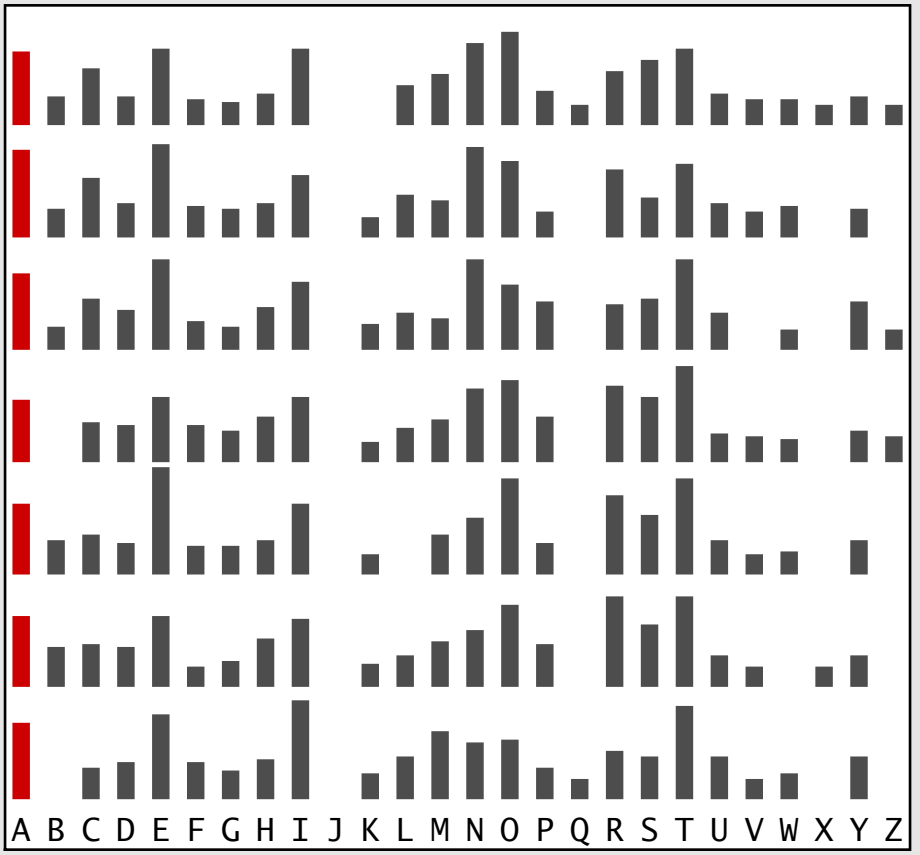
Alfabet matching

Vigenère
sleutel PICKLES

1673 letters
239 per sleutelletter

klaartekst A
A–Z = cijfertekst

Frequenties gematched



Alfabet matching

Tot 1863 is Vigenère ‘le chiffre indéchiffrable’

Majoor F.W. Kasiski publiceert:

Die Geheimschriften und die Dechiffrir-kunst

Dit boek bevat methode voor bepaling sleutellengte in periodieke polyalfabetische substitutie:

benut herhalingen in klaartekst in fase met periode

Andere methode:

William F. Friedman, Riverbank Publication no. 22, 1920

The Index of Coincidence and Its Applications in Cryptography

pt	EENCURSUSVANHETMATHEMATISCHCENTRUM	echt
k	STOEIPOESSTOEIPOESSTOEIPOESSTOEIPO	
ct	WXBGCGGYKNTBLMIAELZXAEBXGGZUXBXZJA	

Herhalingen

pt	EENCURSUSVANHETMATHEMATISCHCENTRUM	echt
k	STOEIPOESSTOEIPOESSTOEIPOESSTOEIPO	
ct	WXBGCGGYKNTBLMIAELZXAEBXGGZUXBXZJA	
pt	EENCURSUSVANHETMATHEMATISCHCENTRUM	vals
k	STOEIPOESSTOEIPOESSTOEIPOESSTOEIPO	
ct	WXBGCGGYKNTBLMIAELZXAEBXGGZUXBXZJA	

Herhalingen

pt	EENCURSUSVANHETMATHEMATISCHCENTRUM	echt
k	STOEIPOESSTOEIPOESSTOEIPOESSTOEIPO	
ct	WXBGCGGYKNTBLMIAELZXAEBXGGZUXBXZJA	
pt	EENCURSUSVANHETMATHEMATISCHCENTRUM	vals
k	STOEIPOESSTOEIPOESSTOEIPOESSTOEIPO	
ct	WXBGCGGYKNTBLMIAELZXAEBXGGZUXBXZJA	
pt	EENCURSUSVANHETMATHEMATISCHCENTRUM	toeval
k	STOEIPOESSTOEIPOESSTOEIPOESSTOEIPO	
ct	WXBGCGGYKNTBLMIAELZXAEBXGGZUXBXZJA	

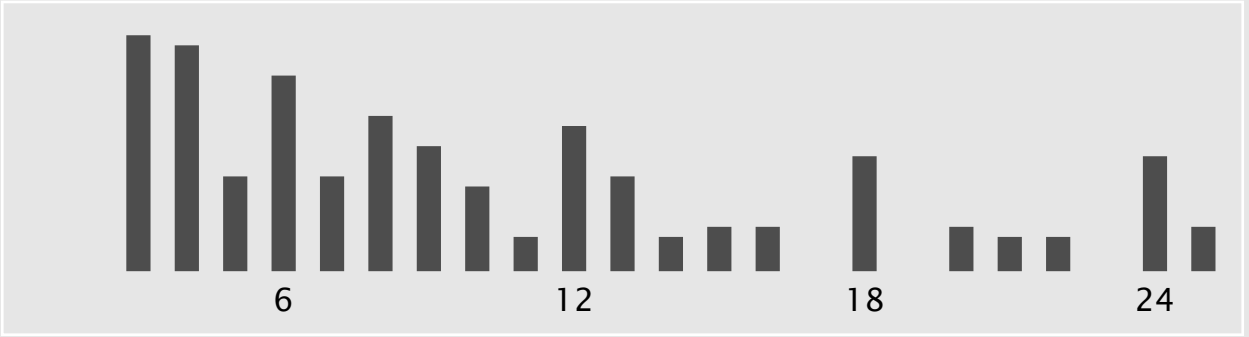
Herhalingen

Brief in 1839 van mr. Kulp. Lewiston, Pennsylvania, USA,
aan
Edgar Allen Poe, redacteur Alexander's Weekly Messenger

Ge Jeasgdxv,
Zij gl mw, laam, xzy zmlwhfzek ejlvdxw kwkw tx lbr atgh lbmx aanu bai Vsmukks pwn vlwk agh gnumk wdlnzweg jnbxvv oaeg enwb zwmgy mo mlw wnbx mw al pnfdcfpkh wzkex hssf xkiyahul. Mk num yexdm wbxy sbc hv wzx Phwkgnamcuk?

Ge Jeasgdxv,
Zij gl mw, laam, xzy zmlwhfzek ejlvdxw kwkw tx lbr atgh lbmx aanu bai Vsmukks pwn vlwk agh gnumk wdlnzweg jnbxvv oaeg enwb zwmgy mo mlw wnbx mw al pnfdcfpkh wzkex hssf xkiyahul. Mk num yexdm wbxy sbc hv wzx Phwkgnamcuk?

histogram factoren herhalingsafstanden



Ge Jeasgdxv,
Zij gl mw, laam, xzy zmlwhfzek ejlvdxw kwkw tx
lbr atgh lbmx aanu bai Vsmukks pwn vlwk agh gnumk
wdlnzweg jnbxvv oaeg enwb zwmgy mo mlw wnbx mw al
pnfdcfpkh wzkex hssf xkiyahul. Mk num yexdm wbxy
sbc hv wzx Phwkgnamcuk?

Veronderstelling (te optimistisch):

alle woorden van 3 letters = the

In de hoop dat een sleutelwoord is gebruikt:

vinden sleutelwoord

Kulp analyse

positities woorden 3 letters op periode 12

I	J										Z	ZIJ
Y										X	Z	XZY
B	R										L	LBR
		B	A	I								BAI
	P	W	N									PWN
								A	G	H		AGH
									M	L	W	MLW
N	U	M										NUM
S	B	C										SBC
					W	Z	X					WZX

sleutelletters als woorden 3 letters = the

B	F										G	ZIJ
U										E	S	XZY
U	N										S	LBR
		I	T	E								BAI
	W	P	J									PWN
								H	Z	D		AGH
									T	E	S	MLW
U	N	I										NUM
Z	U	Y										SBC
					D	S	T					WZX

dezelfde letter meer dan eens in kolom

B	F										G	ZIJ
U										E	S	XZY
U	N										S	LBR
		I	T	E								BAI
	W	P	J									PWN
								H	Z	D		AGH
									T	E	S	MLW
U	N	I										NUM
Z	U	Y										SBC
					D	S	T					WZX

alle drie sleutelletters ok

B	F										G	ZIJ
U										E	S	XZY
U	N										S	LBR
		I	T	E								BAI
	W	P	J									PWN
								H	Z	D		AGH
									T	E	S	MLW
U	N	I										NUM
Z	U	Y										SBC
					D	S	T					WZX
U	N	I	T	E					T	E	S	

oplossing nu evident

B	F										G	ZIJ
U										E	S	XZY
U	N										S	LBR
		I	T	E								BAI
	W	P	J									PWN
								H	Z	D		AGH
									T	E	S	MLW
U	N	I										NUM
Z	U	Y										SBC
					D	S	T					WZX
U	N	I	T	E	D	S	T	A	T	E	S	

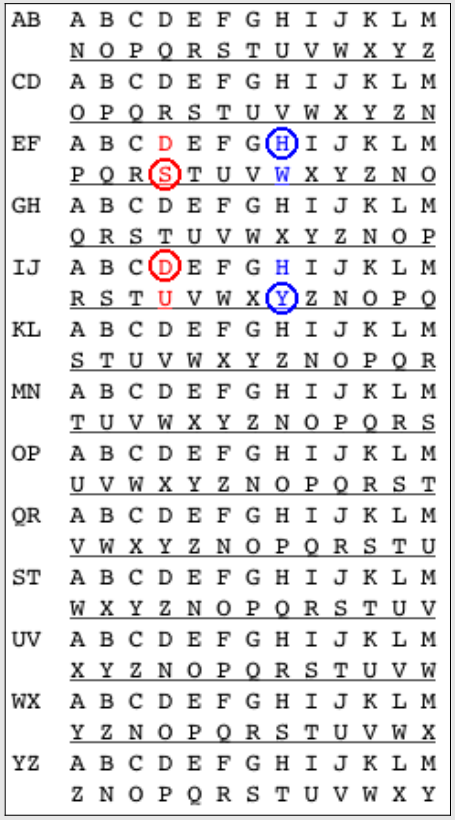
waarschijnlijk woord SUPPLIES op alle posities

	U	S	Z	H	L	W	D	B	P	B	G	G	F	S
S:	C	A	H	P	T	E	L	J	X	J	O	O	N	A
U:		Y	F	N	R	C	J	H	V	H	M	M	L	Y
P:			K	S	W	H	O	M	A	M	R	R	Q	D
P:				S	W	H	O	M	A	M	R	R	Q	D
L:					A	L	S	Q	E	Q	V	V	U	H
I:						O	V	T	H	T	Y	Y	X	K
E:							Z	X	L	X	C	C	B	O
S:								J	X	J	O	O	N	A

sleutel blijkt COMET

	U	S	Z	H	L	W	D	B	P	B	G	G	F	S
S:	C	A	H	P	T	E	L	J	X	J	O	O	N	A
U:		Y	F	N	R	C	J	H	V	H	M	M	L	Y
P:			K	S	W	H	O	M	A	M	R	R	Q	D
P:				S	W	H	O	M	A	M	R	R	Q	D
L:					A	L	S	Q	E	Q	V	V	U	H
I:						O	V	T	H	T	Y	Y	X	K
E:							Z	X	L	X	C	C	B	O
S:								J	X	J	O	O	N	A

Crib dragging



Substitutiepatroon in Porta systeem

```
klaartekst: S U P P L I E S
   patroon: 2 2 2 2 1 1 1 2
substituut: 1 1 1 1 2 2 2 1
```

Lokaliseer patroon en bepaal sleutel:

```
.. G A J J X N Q M ..
.. 1 1 1 1 2 2 2 1 ..
```

Analoog bij *Gronsfeld* = Vigenère
met sleutel beperkt tot 0–9 = A–J

Crib dragging

AJZJNEZAIJ	UAYMFTHYLK	KMMIMIBMVU	HKWGLMHZMT	YIMXXIRMEG
BKAKOFABJK	VBZNGUIZML	LNNJNJCNWV	ILXHMNIANU	ZJNYYJSNFH
CLBLPGBCKL	WCAOHVJANM	MOOKOKDOXW	JMYINOJBOV	AKOZZKTOGI
DMCMQHCDLM	XDBPIWKBON	NPPLPLEPYX	KNZJOPKCPW	BLPAALUPHJ
ENDNRIDEMN	YECQJXLCPO	OQQMQMFQZY	LOAKPQLDQX	CMQBBMVQIK
FOEOSJEFNO	ZFDRKYMDQP	PRRNRNGRAZ	MPBLQRMERY	DNRCCNWRJL
GPFPTKFGOP	AGESLZNERQ	QSSOSOHSBA	NQCMRSNFSZ	EOSDDOXSKM
HQGQULGHPQ	BHFTMAOFSR	RTTPTPITCB	ORDNSTOGTA	FPTEEPYTLN
...	...	...	...	...
SBRBFWRSAB	MSQEXLZQDC	CEEAEATENM	ZCOYDEZREL	QAEPPAJEWY
TCSCGXSTBC	NTRFYMARED	DFFBFBUFON	ADPZEFASFM	RBFQQBKFXZ
UDTDHYTUCD	OUSGZNBSFE	EGGCGCVGPO	BEQAFGBTGN	SCGRRCLGYA
VEUEIZUVDE	PVTHAOCTGF	FHHDHDWHQP	CFRBGHCUHO	TDHSSDMHZB
WFVFJAVWEF	QWUIBPDUHG	GIIEIEXIRQ	DGSCHIDVIP	UEITTENIAC
XGWGKBWXFG	RXVJCQEVIH	HJJFJFYJSR	EHTDIJEWJQ	VFJUUFOJBD
...	...	...	...	...

Generatrix methode

AJZJNEZAIJ	UAYMFTHYLK	KMMIMIBMVU	HKWGLMHZMT	YIMXXIRMEG
BKAKOFABJK	VBZNGUIZML	LNNJNJCNWV	ILXHMNIANU	ZJNYYJSNFH
CLBLPGBCKL	WCAOHVJANM	MOOKOKDOXW	JMYINOJBOV	AKOZZKTOGI
DMCMQHCDLM	XDBPIWKBON	NPPLPLEPYX	KNZJOPKCPW	BLPAALUPHJ
ENDNRIDEMN	YECQJXLCPO	OQQMQMFQZY	LOAKPQLDQX	CMQBBMVQIK
FOEOSJEFNO	ZFDRKYMDQP	PRRNRNGRAZ	MPBLQRMERY	DNRCCNWRJL
GPFPTKFGOP	AGESLZNERQ	QSSOSOHSBA	NQCMRSNFSZ	EOSDDOXSKM
HQGQULGHPQ	BHFTMAOFSR	RTTPTPITCB	ORDNSTOGTA	FPTEEPYTLN
...	...	...	...	...
SBRBFWRSAB	MSQEXLZQDC	CEEAEATENM	ZCOYDEZREL	QAEPPAJEWY
TCSCGXSTBC	NTRFYMARED	DFFBFBUFON	ADPZEFASFM	RBFQQBKFXZ
UDTDHYTUCD	OUSGZNBSFE	EGGCGCVGPO	BEQAFGBTGN	SCGRRCLGYA
VEUEIZUVDE	PVTHAOCTGF	FHHDHDWHQP	CFRBGHCUHO	TDHSSDMHZB
WFVFJAVWEF	QWUIBPDUHG	GIIEIEXIRQ	DGSCHIDVIP	UEITTENIAC
XGWGKBWXFG	RXVJCQEVIH	HJJFJFYJSR	EHTDIJEWJQ	VFJUUFOJBD
...	...	...	...	...

Generatrix methode

Generatrix methode

gekozen generatrices naast elkaar plaatsen:

E N C O U
N T E R E
D R E D I
N F A N T
R Y E S T
I M A T E
D A T O N
E R E G I
M E N T A
N D M A C

ENCOUNTERED RED INFANTRY
ESTIMATED AT ONE REGIMENT
AND MAC...

John Holt Schooling 1896

Pall Mall Magazine, artikel *Secrets in Cipher*

„...the meaning of the cipher which now follows will never be solved by any one”

36 49 97 65 45 43 30 24 76 88 66
54 45 26 44 55 59 57 22 36 ?? ??

Nihilist substitutie = een periodiek polyalfabetisch systeem

Nihilist substitutie

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

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

M	e	e	t	M	e	I	n	P	a	r	i	s	M	o	n	d	a	y
32	15	15	44	32	15	24	33	35	11	42	24	43	32	34	33	14	11	54
T	y	r	a	n	t	T	y	r	a	n	t	T	y	r	a	n	t	T
44	54	42	11	33	44	44	54	42	11	33	44	44	54	42	11	33	44	44
76	69	57	55	65	59	68	87	77	22	75	68	87	86	76	44	47	55	98

Nihilist substitutie

Meet me in Paris Monday

sleutel:	T	y	r	a	n	t
	44	54	42	11	33	44
cryptogram:	76 68 87 98	69 87 86	57 77 76	55 22 44	65 75 47	59 68 55

tientallen: 4 + [1,2,3,4,5] → [5,6,7,8,9]

eenheden: 2 + [1,2,3,4,5] → [3,4,5,6,7]

Nihilist substitutie

In $x + y$ zijn x en y beperkt tot:

- 11–15
- 21–25
- 31–35
- 41–45
- 51–55

Zodat elk cijfer van $x + y$ in:

- sleutel = 1 → [2–6]
- sleutel = 2 → [3–7]
- sleutel = 3 → [4–8]
- sleutel = 4 → [5–9]
- sleutel = 5 → [6–0]

Check of veronderstelde periode hiermee consistent

p = 2	p = 3	p = 4	p = 5	p = 6
36 49	36 49 97	36 49 97 65	36 49 97 65 45	36 49 97 65 45 43
97 ..	65 45 43	45 43 ..	43 30 24 ..	30 24 ..
	30 ..			

p = 7	p = 8	p = 9
36 49 97 65 45 43 30	36 49 97 65 45 43 30 24	36 49 97 65 45 43 30 24 76
24 76 88 66 54 45 26	76 88 66 54 45 26 44 ..	88 ..
44 55 59 57 22 36		

p = 10	p = 11
36 49 97 65 45 43 30 24 76 88	36 49 97 65 45 43 30 24 76 88 66
66 54 ..	54 45 26 ..

Bepaal periode

Som tientallen/eenheden beperkt de mogelijkheden

- unieke combinaties
  - 0 = 5 + 5
  - 22 = 11 + 11
  - 30 = 15 + 15
- effect op waardenrange
  - 23 = 11 + 12 of 12 + 11
  - 32 = 11 + 21 of 21 + 11, etc.
  - voorbeeld

23	tientallen 2 en 6: tiental = 1
64	eenheden 3 en 4: eenheid = 1, 2 of 3

Bepaal sleutel

1	2	3	4	5	6	7
36	49	97	65	45	43	30
24	76	88	66	54	45	26
44	55	59	57	22	36	

kolom	mogelijkheden	sleutel	klaartekst
1	24 = 11 + 13	A	KCN
	12 + 12	B	IBM
	13 + 11	C	HAL
2	range → 24/34	I/O	KWL/ERF
3	range → 44/45	T/U	XTE/WSD
5	22 = 11 + 11	A	OSA
6	11/12/21/22	A/B/F/G	MOK/LNI/GIE/FHD
7	30 = 15 + 15	E	EA

Oplossing

Voorkeursletters ingevuld

1	2	3	4	5	6	7
H	E	W	65	O	43	E
A	R	S	66	S	45	A
L	F	D	57	A	36	

sleutel						
A	I	T		A	A	E
B	O	U			B	
C					F	
					G	

Oplossing

Sleutelwoord geraden

1	2	3	4	5	6	7
H	E	W	65	O	43	E
A	R	S	66	S	45	A
L	F	D	57	A	36	

sleutel						
C	O	U	R	A	G	E
A	I	T			A	
B					B	
					F	

Oplossing

Sleutelwoord COURAGE ingevuld

1	2	3	4	5	6	7
H	E	W	H	O	F	E
A	R	S	I	S	H	A
L	F	D	E	A	D	

Oplossing

pt LEAVNWORTHBCDFGIJKMPQSUXYZ
ct ABCDEFGHIJKLMNOPQRSTUVWXYZ

k=A AV....T
ct CD....I: $C \xrightarrow{1} D \xrightarrow{5} I$

k=C AV....T
ct EF....K: $E \xrightarrow{1} F \xrightarrow{5} K$

Conclusies

- voor elke sleutelletter dezelfde volgorde in frequentietelling
- distributie cryptogram-letters is permutatie van [A-Z]

Oplossen

- match alfabet als bij normale Vigenère, etc.
- los de resulterende monoalfabetische substitutie op

Gemengd pt-alfabet

pt ABCDEFGHIJKLMNOPQRSTUVWXYZ
ct LEAVNWORTHBCDFGIJKMPQSUXYZ

k=A AB....G
ct LE....O: $L \overset{1}{\rightarrow} E \overset{5}{\rightarrow} O$
A–Z LE....O: $L \overset{19}{\rightarrow} E \overset{10}{\rightarrow} O$

k=C AB....G
ct AV....T: $A \overset{1}{\rightarrow} V \overset{5}{\rightarrow} T$
A–Z AV....T: $A \overset{21}{\rightarrow} V \overset{24}{\rightarrow} T$

Conclusies

- voor elke sleutelletter andere volgorde in frequentietelling
- matchen van distributies niet mogelijk

Oplossen vergt vinden van het ct-alfabet

Gemengd ct-alfabet

Bepaling van het ct-alfabet

- symmetrie in positie
- isomorfie

Vervolgstap

- pt-alfabet normaal: klaar
- pt-alfabet ook gemengd: monoalfabetische substitutie

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

Symmetrie in positie

Conclusies uit frequentie-, digram- en trigramanalyse

waarden tussen () onzeker

alfabet	klinkers	medeklinkers	toekenning
1	IMC	QVBLR(G)	I=e M=o Q=r V=t C=a/i
2	WPI	BCDT	W=e
3	GZ	JNDYF	(G=e)
4	C(ERB)	YZJQ	C=e
5	QLU	GNAIW	Q=e

pt	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	C				I				C						M			Q		V						
2					W																					
3					G																					
4					C																					
5					Q																					

p	klinkers	medeklinkers	toekenning
1	IMC	QVBLR(G)	I=e M=o Q=r V=t C=a/i
2	WPI	BCDT	W=e
3	GZ	JNDYF	(G=e)
4	C(ERB)	YZJQ	C=e
5	QLU	GNAIW	Q=e

Symmetrie in positie

pt	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	C				I				C						M			Q		V						
2					W																					
3					G																					
4					C																					
5					Q																					

symmetrie in positie

als in 1 Q→V = 2 dan ook in 5 Q→V = 2, etc.

Symmetrie in positie

pt	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	C				I				C						M			Q		V						
2					W																					
3					G																					
4					C																					
5		M			Q		V							C				I				C				

kan C worden opgelost?

vergelijk frequentie C in 5 met n/v

pt	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					I				C						M			Q		V						
2					W																					
3					G																					
4					C																					
5		M			Q		V											I				C				

C komt niet voor in 5 daarom C=v

pt	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					I				C						M			Q		V						
2					W																					
3					G																					
4	I				C						M			Q		V										
5		M			Q		V											I				C				

symmetrie toegepast op 4

pt	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					I				C						M			Q		V						
2					W																					
3					G																					
4	I				C						M			Q		V										
5		M			Q		V											I				C				

invullen in cryptogram

1	2	3	4	5	1		5	1	2	3	4	5	1
Q	W	B	R	I	V		S	Q	W	B	I	I	J
r	e	?	?	r	t		?	r	e	?	a	r	e

pt	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					I				C						M			Q		V						
2					W																					
3					G																					
4	I				C						M			Q		V										
5		M			Q		V											I				C				

report/prepare geeft 3B=p, 4R=o, 5S=p

1	2	3	4	5	1		5	1	2	3	4	5	1
Q	W	B	R	I	V		S	Q	W	B	I	I	J
r	e	p	o	r	t		p	r	e	p	a	r	e

Symmetrie in positie

pt	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					I				C						M			Q		V						
2					W																					
3					G											B										
4	I				C						M			Q	R	V										
5		M			Q		V									S		I				C				

nieuwe waarden invullen en symmetrie laten werken

1	2	3	4	5	1
Q	W	B	R	I	V
r	e	p	o	r	t

5	1	2	3	4	5	1
S	Q	W	B	I	I	J
p	r	e	p	a	r	e

Symmetrie in positie

pt	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			S		I				C						M			Q	R	V						
2					W																					
3					G											B										
4	I				C						M			Q	R	V									S	
5		M			Q	R	V									S		I				C				

p	klinkers	medeklinkers	toekenning
1	IMC	QVBLR(G)	I=e M=o Q=r V=t C=a/i
2	WPI	BCDT	1W=u? waar dan C,I?
3	GZ	JNDYF	(G=e)
4	C(ERB)	YZJQ	C=e
5	QLU	GNAIW	Q=e

Symmetrie in positie

pt	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			S		I				C						M			Q	R	V	W					
2	P	Q	R	V	W								S		I				C						M	
3					G											B										
4	I				C						M			Q	R	V									S	
5		M			Q	R	V									S		I				C				

p	klinkers	medeklinkers	toekenning
1	IMC	QVBLR(G)	I=e M=o Q=r V=t C=a/i
2	WPI	BCDT	P=a?
3	GZ	JNDYF	(G=e)
4	C(ERB)	YZJQ	C=e
5	QLU	GNAIW	Q=e

Symmetrie in positie

- ...ABABCD.....ABABCD *herhaling*
  ontstaat als positie-$\Delta = k.p$
- ...ABABCD.....KQKQAZ *isomorf*
  ontstaat als positie-$\Delta = \delta + k.p, \delta \neq 0$
- ontstaat uit klaartekstherhaling als $f' = f_{monoalfabetisch}(f)$
- zoeken van isomorfen
  - begin en eind herhaling onzeker met kans $\pm 1/26$
  - begin en eind isomorf onzeker met kans $\pm 25/26$
  - gebruik herhaalde letters als gidsletters

Isomorfie

- polyalfabetische substitutie
  pt-alfabet normaal, ct-alfabet gemengd
  isolog-1: p = 3 isolog-2: p = 4

- Opgave: reconstrueer ct-alfabet

- k1: 123123123123123123123123123123123...
  c1: QWYXTEXBUPRNTRKDJZVLFILUELRXTEXBUPRN...
  k2: 123412341234123412341234123412341234...
  c2: BQTRZDWSGIPACVGPPSIRZDWSPSIRZDWSGIPA...

- (1,1): $C^{-k_1(1)}(\mathrm{Q}) = C^{-k_2(1)}(\mathrm{B}), C^{-k_1(1)}(\mathrm{T}) = C^{-k_2(1)}(\mathrm{C}), \ldots$
  (2,2): $C^{-k_1(2)}(\mathrm{W}) = C^{-k_2(2)}(\mathrm{Q}), C^{-k_1(2)}(\mathrm{R}) = C^{-k_2(2)}(\mathrm{V}), \ldots\ldots$

Voorbeeld isomorfie

A1-B1:	QB	TC	EP	TC	ZH	QB
A2-B2:	WQ	RV	LS	RV	HF	CL
A3-B3:	YT	KG	RI	KG	BS	XQ
A1-B4:	XR	DP	XR	DP	YS	QI
A2-B1:	TZ	JP	TZ	HO	SC	ZV
A3-B2:	ED	ZS	ED	BK	NL	GQ
A1-B3:	XW	VI	XW	YX	HG	CB
A2-B4:	BS	LR	BS	SV	TO	WP
A3-B1:	UG	FZ	UG	NH	IJ	WB
A1-B2:	PI	ID	PI	HX	ZL	XS
A2-B3:	RP	LW	RP	TB	BX	IK
A3-B4:	NA	US	NA	IL	TN	

12 groepen isomorfe relaties

Voorbeeld isomorfie

A1-B1:	QB	TC	EP	TC	ZH	QB
A2-B2:	WQ	RV	LS	RV	HF	CL
A3-B3:	YT	KG	RI	KG	BS	XQ
A1-B4:	XR	DP	XR	DP	YS	QI
A2-B1:	TZ	JP	TZ	HO	SC	ZV
A3-B2:	ED	ZS	ED	BK	NL	GQ
A1-B3:	XW	VI	XW	YX	HG	CB
A2-B4:	BS	LR	BS	SV	TO	WP
A3-B1:	UG	FZ	UG	NH	IJ	WB
A1-B2:	PI	ID	PI	HX	ZL	XS
A2-B3:	RP	LW	RP	TB	BX	IK
A3-B4:	NA	US	NA	IL	TN	

A3-B3 = A2-B4 kunnen gecombineerd

Voorbeeld isomorfie

A1-B1:	QB	TC	EP	TC	ZH	QB
A2-B2:	WQ	RV	LS	RV	HF	CL
A3-B3:	YT	KG	RI	KG	BS	XQ
A1-B4:	XR	DP	XR	DP	YS	QI
A2-B1:	TZ	JP	TZ	HO	SC	ZV
A3-B2:	ED	ZS	ED	BK	NL	GQ
A1-B3:	XW	VI	XW	YX	HG	CB
A2-B4:	BS	LR	BS	SV	TO	WP
A3-B1:	UG	FZ	UG	NH	IJ	WB
A1-B2:	PI	ID	PI	HX	ZL	XS
A2-B3:	RP	LW	RP	TB	BX	IK
A3-B4:	NA	US	NA	IL	TN	

Y(?)T/K(?)G/... kies YT/KG/RI/...

Reconstructie CT-alfabet

A1-B1:	QB	TC	EP	TC	ZH	QB
A2-B2:	WQ	RV	LS	RV	HF	CL
A3-B3:	YT	KG	RI	KG	BS	XQ
A1-B4:	XR	DP	XR	DP	YS	QI
A2-B1:	TZ	JP	TZ	HO	SC	ZV
A3-B2:	ED	ZS	ED	BK	NL	GQ
A1-B3:	XW	VI	XW	YX	HG	CB
A2-B4:	BS	LR	BS	SV	TO	WP
A3-B1:	UG	FZ	UG	NH	IJ	WB
A1-B2:	PI	ID	PI	HX	ZL	XS
A2-B3:	RP	LW	RP	TB	BX	IK
A3-B4:	NA	US	NA	IL	TN	

rijg kettingen: BS+SV=BSV, LR+RI=LRI, YT+TO=YTO, KG, WP, XQ

Reconstructie CT-alfabet

A1-B1:	QB	TC	EP	TC	ZH	QB	A2-B2:	WQ	RV	LS	RV	HF	CL
A3-B3:	YT	KG	RI	KG	BS	XQ	A1-B4:	XR	DP	XR	DP	YS	QI
A2-B1:	TZ	JP	TZ	HO	SC	ZV	A3-B2:	ED	ZS	ED	BK	NL	GQ
A1-B3:	XW	VI	XW	YX	HG	CB	A2-B4:	BS	LR	BS	SV	TO	WP
A3-B1:	UG	FZ	UG	NH	IJ	WB	A1-B2:	PI	ID	PI	HX	ZL	XS
A2-B3:	RP	LW	RP	TB	BX	IK	A3-B4:	NA	US	NA	IL	TN	

opstellen relaties

. B S V . . L R I . . Y T O . . K G . . W P . . X Q

Reconstructie CT-alfabet

A1-B1:	QB	TC	EP	TC	ZH	QB	A2-B2:	WQ	RV	LS	RV	HF	CL
A3-B3:	YT	KG	RI	KG	BS	XQ	A1-B4:	XR	DP	XR	DP	YS	QI
A2-B1:	TZ	JP	TZ	HO	SC	ZV	A3-B2:	ED	ZS	ED	BK	NL	GQ
A1-B3:	XW	VI	XW	YX	HG	CB	A2-B4:	BS	LR	BS	SV	TO	WP
A3-B1:	UG	FZ	UG	NH	IJ	WB	A1-B2:	PI	ID	PI	HX	ZL	XS
A2-B3:	RP	LW	RP	TB	BX	IK	A3-B4:	NA	US	NA	IL	TN	

kies een tweede — onafhankelijke — relatie

```
  T                                I       L R     B
. B S V . . L R I . . Y T O . . K G . . W P . . X Q
```

Reconstructie CT-alfabet

A1-B1:	QB	TC	EP	TC	ZH	QB	A2-B2:	WQ	RV	LS	RV	HF	CL
A3-B3:	YT	KG	RI	KG	BS	XQ	A1-B4:	XR	DP	XR	DP	YS	QI
A2-B1:	TZ	JP	TZ	HO	SC	ZV	A3-B2:	ED	ZS	ED	BK	NL	GQ
A1-B3:	XW	VI	XW	YX	HG	CB	A2-B4:	BS	LR	BS	SV	TO	WP
A3-B1:	UG	FZ	UG	NH	IJ	WB	A1-B2:	PI	ID	PI	HX	ZL	XS
A2-B3:	RP	LW	RP	TB	BX	IK	A3-B4:	NA	US	NA	IL	TN	

expandeer de toegevoegde relatie en combineer

```
Y T O                           I       L R     B
. B S V . . L R I . . Y T O . . K G . . W P . . X Q
  X Q       W P K G
```

Reconstructie CT-alfabet

A1-B1:	QB	TC	EP	TC	ZH	QB	A2-B2:	WQ	RV	LS	RV	HF	CL
A3-B3:	YT	KG	RI	KG	BS	XQ	A1-B4:	XR	DP	XR	DP	YS	QI
A2-B1:	TZ	JP	TZ	HO	SC	ZV	A3-B2:	ED	ZS	ED	BK	NL	GQ
A1-B3:	XW	VI	XW	YX	HG	CB	A2-B4:	BS	LR	BS	SV	TO	WP
A3-B1:	UG	FZ	UG	NH	IJ	WB	A1-B2:	PI	ID	PI	HX	ZL	XS
A2-B3:	RP	LW	RP	TB	BX	IK	A3-B4:	NA	US	NA	IL	TN	

zoek een derde — afhankelijke — relatie erbij

Reconstructie CT-alfabet

A1-B1:	QB	TC	EP	TC	ZH	QB	A2-B2:	WQ	RV	LS	RV	HF	CL
A3-B3:	YT	KG	RI	KG	BS	XQ	A1-B4:	XR	DP	XR	DP	YS	QI
A2-B1:	TZ	JP	TZ	HO	SC	ZV	A3-B2:	ED	ZS	ED	BK	NL	GQ
A1-B3:	XW	VI	XW	YX	HG	CB	A2-B4:	BS	LR	BS	SV	TO	WP
A3-B1:	UG	FZ	UG	NH	IJ	WB	A1-B2:	PI	ID	PI	HX	ZL	XS
A2-B3:	RP	LW	RP	TB	BX	IK	A3-B4:	NA	US	NA	IL	TN	

combineer fragmenten en completeer relatie

```
          Y T O
            B S V
            X Q
. . . . . D L R I . . . . . .
              W P K G
```

Reconstructie CT-alfabet

A1-B1:	QB	TC	EP	TC	ZH	QB	A2-B2:	WQ	RV	LS	RV	HF	CL
A3-B3:	YT	KG	RI	KG	BS	XQ	A1-B4:	XR	DP	XR	DP	YS	QI
A2-B1:	TZ	JP	TZ	HO	SC	ZV	A3-B2:	ED	ZS	ED	BK	NL	GQ
A1-B3:	XW	VI	XW	YX	HG	CB	A2-B4:	BS	LR	BS	SV	TO	WP
A3-B1:	UG	FZ	UG	NH	IJ	WB	A1-B2:	PI	ID	PI	HX	ZL	XS
A2-B3:	RP	LW	RP	TB	BX	IK	A3-B4:	NA	US	NA	IL	TN	

zoek een volgende relatie erbij

```
        Y T O
          B S V
          X Q
. . . . . . . . . D L R I . . . . . . . . . . . . . . .
            W P K G
```

Reconstructie CT-alfabet

A1-B1:	QB	TC	EP	TC	ZH	QB	A2-B2:	WQ	RV	LS	RV	HF	CL
A3-B3:	YT	KG	RI	KG	BS	XQ	A1-B4:	XR	DP	XR	DP	YS	QI
A2-B1:	TZ	JP	TZ	HO	SC	ZV	A3-B2:	ED	ZS	ED	BK	NL	GQ
A1-B3:	XW	VI	XW	YX	HG	CB	A2-B4:	BS	LR	BS	SV	TO	WP
A3-B1:	UG	FZ	UG	NH	IJ	WB	A1-B2:	PI	ID	PI	HX	ZL	XS
A2-B3:	RP	LW	RP	TB	BX	IK	A3-B4:	NA	US	NA	IL	TN	

expandeer de relatie

```
          Y T O
            B S V
            X Q     D
. . . . . H D L R I . . . . . . . . . . . . . .
          I Z W P K G
```

Reconstructie CT-alfabet

A1-B1:	QB	TC	EP	TC	ZH	QB	A2-B2:	WQ	RV	LS	RV	HF	CL
A3-B3:	YT	KG	RI	KG	BS	XQ	A1-B4:	XR	DP	XR	DP	YS	QI
A2-B1:	TZ	JP	TZ	HO	SC	ZV	A3-B2:	ED	ZS	ED	BK	NL	GQ
A1-B3:	XW	VI	XW	YX	HG	CB	A2-B4:	BS	LR	BS	SV	TO	WP
A3-B1:	UG	FZ	UG	NH	IJ	WB	A1-B2:	PI	ID	PI	HX	ZL	XS
A2-B3:	RP	LW	RP	TB	BX	IK	A3-B4:	NA	US	NA	IL	TN	

concentreer op een lijn

```
          Y T O
      Y T O   B S V
        B S V   X Q   D
. . . . . X Q . H D L R I Z W P K G . . . . . . . .
          I Z W P K G
```

Reconstructie CT-alfabet

A1-B1:	QB	TC	EP	TC	ZH	QB	A2-B2:	WQ	RV	LS	RV	HF	CL
A3-B3:	YT	KG	RI	KG	BS	XQ	A1-B4:	XR	DP	XR	DP	YS	QI
A2-B1:	TZ	JP	TZ	HO	SC	ZV	A3-B2:	ED	ZS	ED	BK	NL	GQ
A1-B3:	XW	VI	XW	YX	HG	CB	A2-B4:	BS	LR	BS	SV	TO	WP
A3-B1:	UG	FZ	UG	NH	IJ	WB	A1-B2:	PI	ID	PI	HX	ZL	XS
A2-B3:	RP	LW	RP	TB	BX	IK	A3-B4:	NA	US	NA	IL	TN	

concentreer nog verder op een lijn

```
          Y T O
      Y T O   B S V
        B S V   X Q     D
. B S V . X Q . H D L R I Z W P K G . . . Y T O .
          I Z W P K G
```

Reconstructie CT-alfabet

A1-B1:	QB	TC	EP	TC	ZH	QB	A2-B2:	WQ	RV	LS	RV	HF	CL
A3-B3:	YT	KG	RI	KG	BS	XQ	A1-B4:	XR	DP	XR	DP	YS	QI
A2-B1:	TZ	JP	TZ	HO	SC	ZV	A3-B2:	ED	ZS	ED	BK	NL	GQ
A1-B3:	XW	VI	XW	YX	HG	CB	A2-B4:	BS	LR	BS	SV	TO	WP
A3-B1:	UG	FZ	UG	NH	IJ	WB	A1-B2:	PI	ID	PI	HX	ZL	XS
A2-B3:	RP	LW	RP	TB	BX	IK	A3-B4:	NA	US	NA	IL	TN	

alle relaties gebruikt — maar wat is “B ? S” nu echt?

```
          Y T O
    Y T O     B S V
      B S V   X Q     D
F B S V U X Q M H D L R I Z W P K G C A E N Y T O J
          I Z W P K G
```

Reconstructie CT-alfabet

```
 1: F B S V U X Q M H D L R I Z W P K G C A E N Y T O J
 3: F V Q D I P C N O B U M L Z K A Y J S X H R W G E T
 5: F X L P E J U D W A O V H Z C T S M I G Y B Q R K N
 7: F M W N S D K T U R C J Q Z E B H P Y V L G O X I A
 9: F D C B L A S R E V I N U Z Y X W T Q P O M K J H G
11: F R Y M C V W J L N Q G S Z O D E X K B I T H A U P
15: F P U A H T I B K X E D O Z S G Q N L J W V C M Y R
17: F G H J K M O P Q T W X Y Z U N I V E R S A L B C D
19: F A I X O G L V Y P H B E Z Q J C R U T K D S N W M
21: F N K R Q B Y G I M S T C Z H V O A W D U J E P L X
23: F T E G W R H X S J Y A K Z L M U B O N C P I D Q V
25: F J O T Y N E A C G K P W Z I R L D H M Q X U V S B
```

alle *decimaties:* $x, x+d, x+2d, x+3d, \ldots \; ggd(d,26)=1$

Reconstructie CT-alfabet

```
 1: F B S V U X Q M H D L R I Z W P K G C A E N Y T O J
 3: F V Q D I P C N O B U M L Z K A Y J S X H R W G E T
 5: F X L P E J U D W A O V H Z C T S M I G Y B Q R K N
 7: F M W N S D K T U R C J Q Z E B H P Y V L G O X I A
 9: F D C B L A S R E V I N U Z Y X W T Q P O M K J H G
11: F R Y M C V W J L N Q G S Z O D E X K B I T H A U P
15: F P U A H T I B K X E D O Z S G Q N L J W V C M Y R
17: F G H J K M O P Q T W X Y Z U N I V E R S A L B C D
19: F A I X O G L V Y P H B E Z Q J C R U T K D S N W M
21: F N K R Q B Y G I M S T C Z H V O A W D U J E P L X
23: F T E G W R H X S J Y A K Z L M U B O N C P I D Q V
25: F J O T Y N E A C G K P W Z I R L D H M Q X U V S B
```

alfabet blijkt sleutelwoord te hebben

Reconstructie CT-alfabet