

# Universiteit van Stellenbosch

## Toegepaste Wiskunde 314

### Tutoriaal 3: Donderdag 4 Maart 2004

#### MEMORANDUM

- (1) Die kriptoteks is: XLDMPFPBPWDBTQDMPMPZWD.
- (2) Die skoonteks is: letthehealingfountainstart, oftewel “let the healing fountain start.”
- (3) (a) Die volgende letterfrekwensies word verkry:

A:	35	J:	44	S:	18
B:	20	K:	0	T:	3
C:	37	L:	2	U:	17
D:	8	M:	9	V:	60
E:	3	N:	14	W:	65
F:	1	O:	70	X:	49
G:	34	P:	107	Y:	59
H:	27	Q:	74	Z:	15
I:	5	R:	3		

Die indeks van ooreenstemming, gebaseer op enkel letterfrekwensies alleenlik, is  $I_o = 0.0720$ . Die natuurlike taal van die onderliggende skoonteks kan moontlik Spaans wees.

- (b) Die sleutel is

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

Die skoonteks

“Auden first gained attention in nineteen thirty, when his short verse play called ‘Paid on Both Sides’ was published in TS Eliot’s periodical ‘The Criterion.’ In the same year appeared Auden’s ‘POEMS,’ his first commercially published book in which he carefully avoided Yeatsian romantic self expression. The poems were short, untitled and slightly cryptic. Auden soon gained fame as a leftist intellectual. He showed interest in Marx and Freud, and he wrote passionately on social problems among others in ‘LOOK STRANGER!’ in nineteen thirty six. Compressed figures of speech, direct statement and musical effect characterized ‘ON THIS ISLAND’ in nineteen thirty seven and ‘ANOTHER TIME’ in nineteen forty. In the late nineteen thirties Auden’s poems were perhaps less radical politically; suffering and injustice are not rejected as a part of ordinary life. The last works from this decade astonished readers with their light comic tone and domesticity.”

word ná invoeging van spasies en leestekens verkry.

- (4) Die indekse van ooreenstemming vir die spesifieke teks is  $I_o = 0.0650$ . Die teks is dus na alle waarskynlikheid in Engels.
- (5) Die kriptoteks is: **SPLFVAV**.
- (6) Die skoonteks is: **intheprisonofhisdaysteachthefreemanhowtopraise**, oftewel “in the prison of his days teach the free man how to praise.”
- (7) Die volgende herhalings (van lengte 5 of langer) word waargeneem:

$i$	String	Posisies	Afstand, $d_i$
1	WGFMROWFIEM	80, 355	275
2	UUNAJMKNWWK	47, 227	180
3	KMULAIA	308, 338	30
4	LNEWGF	77, 397	320
5	GTCGF	278, 413	135

Die sleutellengte is dus na alle waarskynlikheid

$$\text{ggd}(275, 180, 30, 320, 135) = \text{ggd}(5^2 \times 11, 2^2 \times 3^2 \times 5, 2 \times 3 \times 5, 2^6 \times 5, 3^3 \times 5) = 5.$$

Letterfrekwensie tellings vir die 5 subtekste:

	1	2	3	4	5		1	2	3	4	5		1	2	3	4	5
A:	6	4	8	8	5	J:	4	0	2	4	5	S:	4	3	3	4	5
B:	1	4	2	0	1	K:	6	0	3	5	8	T:	12	4	0	0	2
C:	3	8	4	0	1	L:	1	4	9	7	7	U:	6	4	3	3	6
D:	1	3	2	3	1	M:	6	3	5	3	4	V:	0	0	5	5	2
E:	3	16	0	3	0	N:	7	8	4	0	3	W:	1	2	9	22	8
F:	2	2	4	11	12	O:	6	6	4	1	3	X:	6	1	3	1	7
G:	8	1	8	5	6	P:	0	1	1	1	0	Y:	2	5	12	3	5
H:	0	6	5	2	0	Q:	0	2	0	3	0	Z:	8	0	0	5	4
I:	4	5	3	0	3	R:	2	8	0	0	0						

Die 5 letters van die kodewoord is dus waarskynlik P/D/V, A, U, S en B/G/S onderskeidelik. As die laaste letter as **S** gekies word, m.a.w. vir 'n kodewoord van die vorm **\*AUSS**, word die volgende dekripsie verkry:

KheesJentiRlideRbehiEdconXruenTeswaJalreRdyusVdintYesevVnteeEthanUei  
ghKeentYcentLriesRndmaEyspeTialfRctscFncerEingcFngruVncesNerenFtedfF  
rexaDpletYeconXruenTesofWermaKeuleIandwZlsonUatefIomthZsperZodduIing  
tYeeigYteenKhcenKuryfLrtheIcontIibutZonswVremaUebylRgranXeandCeganUr  
ehoNeverKhereRlbirKhofcFngruVncesRsacoYerenKtheoIyoccLrredZn1799witY  
thepLblicRtionFfgauJsdisHuisiKioneJmathVmatiTaietNasgaLsswhFfirsKsys  
tVmatiTallyJtudiVdconXruenTesfoItheiIownsRkeanUwhoiEtrodLcedtYeconMe  
nieEtnotRtionJtillZnuse

Teks in kleinletters blyk korrek te wees, terwyl hoofletters foutief gedekripteerde teks voorstel. Die onderstreepte segmente blyk herhalings van die woord “**congruences**” te wees. Indien hierdie vermoede korrek is, behoort die (eerste) letter **t** na **Z** te

enkripteer, wat bewerkstellig kan word, indien die eerste kodeletter G is. Met die  
kodewoord GAUSS dekripteer die kriptoteks dan na

the essential idea behind congruences was already used in the seventeenth and ei  
gteenth centuries and many special facts concerning congruences were noted fo  
r example the congruences of fermat euler and wilson date from this period during  
the eighteenth century further contributions were made by lagrange and legandr  
e however the real birth of congruences as a coherent theory occurred in 1799 with  
the publication of gauss disquisitiones mathematicae it was gauss who first sys  
tematically studied congruences for their own sake and who introduced the conve  
nient notation still in use

oftewel na

“the essential idea behind congruences was already used in the seventeenth and  
eighteenth centuries and many special facts concerning congruences were noted for  
example the congruences of fermat euler and wilson date from this period during  
the eighteenth century further contributions were made by lagrange and legandre  
however the real birth of congruences as a coherent theory occurred in 1799 with  
the publication of gauss disquisitiones mathematicae it was gauss who first system  
atically studied congruences for their own sake and who introduced the convenient  
notation still in use”

ná invoeging van spasies.