College Cryptografie

Cursusjaar 2003

Analyse van Monoalfabetische Substitutie

28 januari 2003

Caesar oplossen door
afdraaien van het alfabet
25 mogelijkheden
de goede opsporen

voorbeeld: UJLQNKNTSN

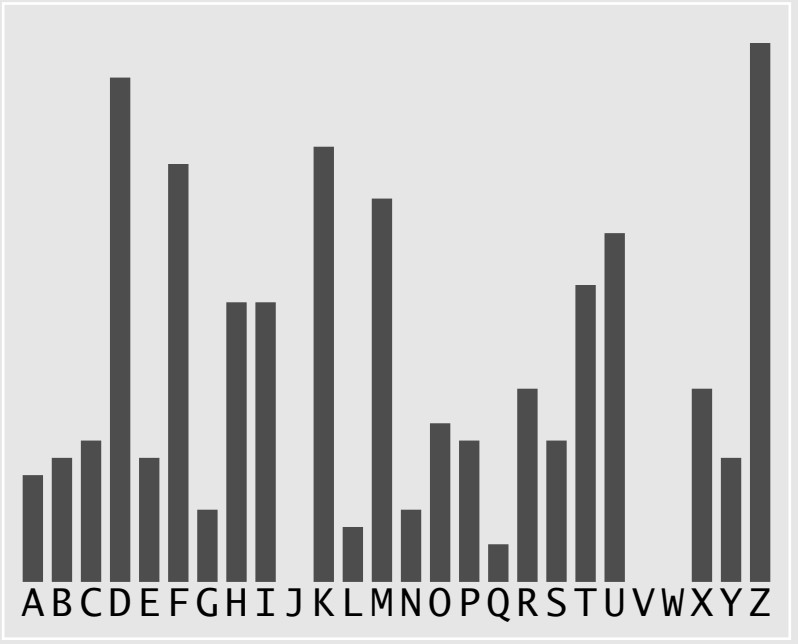
A	UJLQNKNTSN	N	HWYDAXAGFA
Z	VKMROLOUTO	M	IXZEBYBHGB
Y	WLNSPMPVUP	L	JYAFCZCIHC
X	XMOTQNQWVQ	K	KZBGDADJID
W	YNPURORXWR	J	LACHEBEKJE
V	ZOQVSPSYXS	I	MBDIFCFLKF
U	APRWTQTZYT	H	NCEJGDGMLG
T	BQSXURUAZU	G	ODFKHEHNMH
S	CRTYVSVBAV	F	PEGLIFIONI
R	DSUZWTWCBW	E	QFHMJGJPOJ
Q	ETVAXUXDCX	D	RGINKHKQPK
P	FUWBYVYEDY	C	SHJOLILRQL
O	GVXCZWZFEZ	B	TIKPMJMSRM

Caesar substitutie

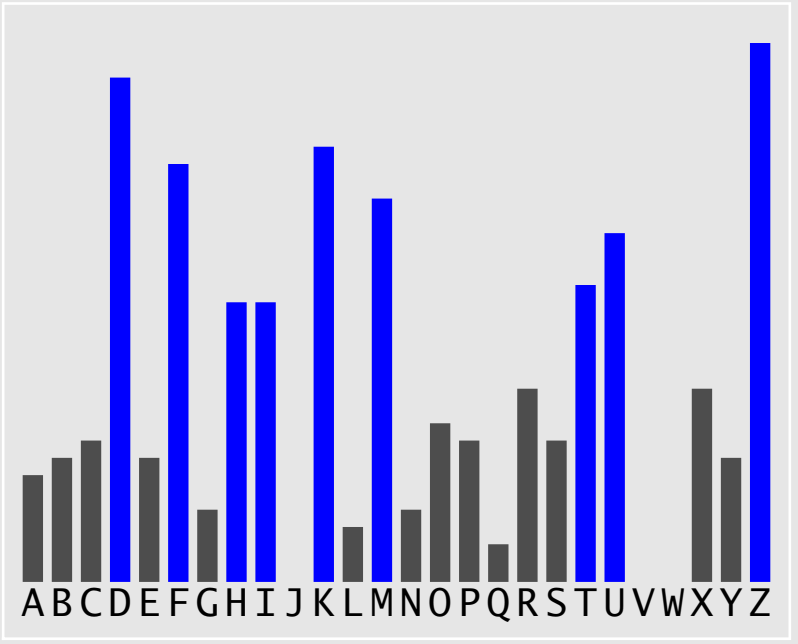
KFDKT BDFZM EUBDK FDPZY IOMMZ TXKUK ZYGUR BZHAK FTHCM
URMFU DMZHX MFTNM ZHXMD ZYTHC PZQUR EZSSZ CDMZH XGTHC
MZHXP FAKFD MDZTM SUTYT HCFUK ZHXPF DKFDI NTCMF ZLDPT
HCMSO KPZTK ZSTKK FDUAM KDIME ITDXS DRUID PDFZL DUOIE
FZKRU IMUBD UROMZ IDUOK URSID ZKFZH XZYYU ROMZI DRZKH
UFOII AMZTX KFDEZ INDHK DIKFD AKFZH GDXFT BBOEF RUIKF
ZK

A.S. Tanenbaum
opgave in *Computer Networks*
in groepen van 5 gezet

Monoalfabetische substitutie

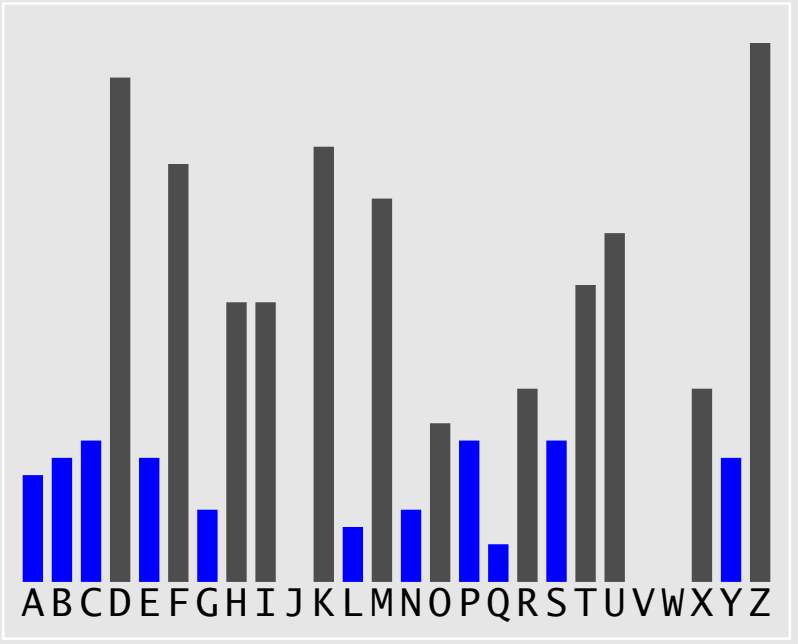


Lettertelling



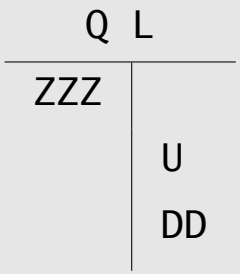
meest voorkomend ETAONISRH

Hoge frequentie



minst voorkomend BCFGJKMPQUVWXYZ

Lage frequentie



doorgaan tot gevoel zegt “stop”

beter als woordverdeling bekend

Q L G N A B Y C P S	
ZZZZZZZZZZ	ZZZZZ
UUU	UUUU
RR	
DDDD	DDDDDDDDD
XXXX	X
TTTTT	TTTTTT
MM	MMMMMMM
III	II
HHHHHH	
K	KKK
F	FFF
	OO

trends in contactgedrag

klinkers links *en* rechts

medeklinkers links *of* rechts

A, E, I, O meest *ook* hoge frequentie

Contacten

Q L G N A B Y C P S	
ZZZZZZZZZZ	ZZZZZ
UUU	UUUU
RR	
DDDD	DDDDDDDDD
XXXX	X
TTTTT	TTTTTT
MM	MMMMMMM
III	II
HHHHHH	
K	KKK
F	FFF
	OO

trends in contactgedrag

klinkers links *en* rechts

Z (30) U (19) D (28)

T (16)

medeklinkers links *of* rechts

X (10) H (15) K (24)

F (23)

Voorschrift:

1. tel de contacten als $< i \mid j >$ en $< j \mid i >$ maar niet $< i \mid i >$
2. sommeer de contacten per letter
3. hoogste positieve som waarschijnlijk een klinker
4. verwijder contacten met laatst gekozen klinker
5. herhaal vorige twee stappen zolang een som > 0

Sukhotin algoritme

Voorbeeld met tekst “SAGITTAS”

	A	G	I	S	T	Σ	Δ	Σ	Δ	Σ
A	-	1	0	2	1	4	klinker			
G	1	-	1	0	0	2	-2	0	-2	-2
I	0	1	-	0	1	2	0	2	klinker	
S	2	0	0	-	0	2	-4	-2	0	-2
T	1	0	1	0	-	2	-2	0	-2	-2

KFDKT BDFZM EUBDK FDPZY IOMMZ TXKUK ZYGUR BZHAK FTHCM
URMFU DMZHX MFTNM ZHXMD ZYTHC PZQUR EZSSZ CDMZH XGTHC
MZHXP FAKFD MDZTM SUTYT HCFUK ZHXPF DKFDI NTCMF ZLDPT
HCMSO KPZTK ZSTKK FDUAM KDIME ITDXS DRUID PDFZL DUOIE
FZKRU IMUBD UROMZ IDUOK URSID ZKFZH XZYYU ROMZI DRZKH
UFOII AMZTX KFDEZ INDHK DIKFD AKFZH GDXFT BBOEF RUIKF ZK

- contacten: klinkers D T U Z medeklinkers F H K M X
- Sukhotin vindt achtereenvolgens: Z D U T 0 klinkers
- KF 11× en FK 0× steeds gevolgd door D, T of Z: KF $\stackrel{?}{=}$ th
  KFD 7× KFT 1× KFZ 3×: D $\stackrel{?}{=}$ e, Z $\stackrel{?}{=}$ a en T,U $\stackrel{?}{=}$ i,o

Waarnemingen

KFDKT BDFZM EUBDK FDPZY IOMMZ TXKUK ZYGUR BZHAK FTHCM
URMFU DMZHX MFTNM ZHXMD ZYTHC PZQUR EZSSZ CDMZH XGTHC
MZHXP FAKFD MDZTM SUTYT HCFUK ZHXPF DKFDI NTCMF ZLDPT
HCMSO KPZTK ZSTKK FDUAM KDIME ITDXS DRUID PDFZL DUOIE
FZKRU IMUBD UROMZ IDUOK URSID ZKFZH XZYYU ROMZI DRZKH
UFOII AMZTX KFDEZ INDHK DIKFD AKFZH GDXFT BBOEF RUIKF ZK

- voornamelijk klinkers D T U Z voorafgaand aan H
- typerend voor $\mathtt{H} \stackrel{?}{=} \mathtt{n}$
- probeer nu:
  K=t F=h D=e Z=a TU=io IM=rs H=n

Waarnemingen

KFDKT BDFZM EUBDK FDPZY IOMMZ TXKUK ZYGUR BZHAK FTHCM
theti .ehas .o.et he.a. r.ssa i.tot a..o. .an.t hin.s
theto .ehar .i.et he.a. s.rra o.tit a..i. .an.t hon.r

URMFU DMZHX MFTNM ZHXMD ZYTHC PZQUR EZSSZ CDMZH XGTHC
o.sho esan. shi.s an.se a.in. .a.o. .a..a .esan ..in.
i.rhi eran. rho.r an.re a.on. .a.i. .a..a .eran ..on.

MZHXP FAKFD MDZTM SUTYT HCFUK ZHXPF DKFDI NTCMF ZLDPT
san.. h.the seais .oi.i n.hot an..h ether .i.sh a.e.i
ran.. h.the reaor .io.o n.hit an..h ethes .o.rh a.e.o

HCMSO KPZTK ZSTKK FDUAM KDIME ITDXS DRUID PDFZL DUOIE

Proberen

KFDKT BDFZM EUBDK FDPZY IOMMZ TXKUK ZYGUR BZHAK FTHCM
theti .ehas .o.et he.a. r.ssa i.tot a..o. .an.t hin.s
theto .ehar .i.et he.a. s.rra o.tit a..i. .an.t hon.r

URMFU DMZHX MFTNM ZHXMD ZYTHC PZQUR EZSSZ CDMZH XGTHC
o.sho esan. shi.s an.se a.in. .a.o. .a..a .esan ..in.
i.rhi eran. rho.r an.re a.on. .a.i. .a..a .eran ..on.

MZHXP FAKFD MDZTM SUTYT HCFUK ZHXPF DKFDI NTCMF ZLDPT
san.. h.the seais .oi.i n.hot an..h ether .i.sh a.e.i
ran.. h.the reaor .io.o n.hit an..h ethes .o.rh a.e.o

HCMSO KPZTK ZSTKK FDUAM KDIME ITDXS DRUID PDFZL DUOIE

Oplossen io/rs

KFDKT BDFZM EUBDK FDPZY IOMMZ TXKUK ZYGUR BZHAK FTHCM
theti .ehas .o.et he.a. r.ssa i.tot a..o. .an.t hings

URMFU DMZHX MFTNM ZHXMD ZYTHC PZQUR EZSSZ CDMZH XGTHC
o.sho esand shi.s andse a.in. .a.o. .a..a .esan ..in.

MZHXP FAKFD MDZTM SUTYT HCFUK ZHXPF DKFDI NTCMF ZLDPT
san.. h.the seais .oi.i n.hot an..h ether .i.sh a.e.i

HCMSO KPZTK ZSTKK FDUAM KDIME ITDXS DRUID PDFZL DUOIE
n.s.. t.ait a.itt heo.s ters. rie.. e.ore .eha. eo.r.

FZKRU IMUBD UROMZ IDUOK URSID ZKFZH XZYYU ROMZI DRZKH
hat.o rso.e o..sa reo.t o..re athan .a..o ..sar e.atn

Oplossen bijzoeken

KFDKT BDFZM EUBDK FDPZY IOMMZ TXKUK ZYGUR BZHAK FTHCM
theti mehas .o.et he.a. r.ssa idtot a..o. manyt hings

URMFU DMZHX MFTNM ZHXMD ZYTHC PZQUR EZSSZ CDMZH XGTHC
o.sho esand shi.s andse a.ing .a.o. .a..a gesan d.ing

MZHXP FAKFD MDZTM SUTYT HCFUK ZHXPF DKFDI NTCMF ZLDPT
sand. h.the seais boili nghot and.h ether .igsh a.e.i

HCMSO KPZTK ZSTKK FDUAM KDIME ITDXS DRUID PDFZL DUOIE
ngs.. t.ait a.itt heoys ters. ried. e.ore .eha. eo.r.

FZKRU IMUBD UROMZ IDUOK URSID ZKFZH XZYYU ROMZI DRZKH
hat.o rso.e o..sa reo.t o..re athan da..o ..sar e.atn

Oplossen bijzoeken

KFDKT BDFZM EUBDK FDPZY IOMMZ TXKUK ZYGUR BZHAK FTHCM
theti mehas comet hewal russa idtot alkof manyt hings

URMFU DMZHX MFTNM ZHXMD ZYTHC PZQUR EZSSZ CDMZH XGTHC
ofsho esand ships andse aling waxof cabba gesan dking

MZHXP FAKFD MDZTM SUTYT HCFUK ZHXPF DKFDI NTCMF ZLDPT
sandw hythe seais boili nghot andwh ether pigsh avewi

HCMSO KPZTK ZSTKK FDUAM KDIME ITDXS DRUID PDFZL DUOIE
ngsbu twait abitt heoys tersc riedb efore wehav eourc

FZKRU IMUBD UROMZ IDUOK URSID ZKFZH XZYYU ROMZI DRZKH
hatfo rsome ofusa reout ofbre athan dallo fusar efatn

Oplossen afmaken

- gebruik letterfrequenties etaonirsh
- contactgedrag van letters
  klinkers veel variatie e het meest
  omkeringen th-ht, es-se, verdubbeling ll
- begin- en eindletters woorden
- classificatie klinker-medeklinker
  contactgedrag, Sukhotin
  afwisseling +++-+--+ niet ------- of +++++++
- patroonherkenning XYZZYXPPQABCYYQ = massamoordenaar
- sleutelwoord in klaar- of cijferalfabet
- waarschijnlijke woorden

Samenvatting