Cursus Cryptografie

Breken monoalfabeet

16-02–2016

Technieken

- Caesar oplossen
- Monoalfabeet met frequenties
- Klinkers en medeklinkers
  - Consonantlijn
  - Sukhotin - zie syllabus hoofdstuk 6.5

Caesar

26 sleutels - uitputtend zoeken

“afdraaien van het alfabet”

Voorbeeld

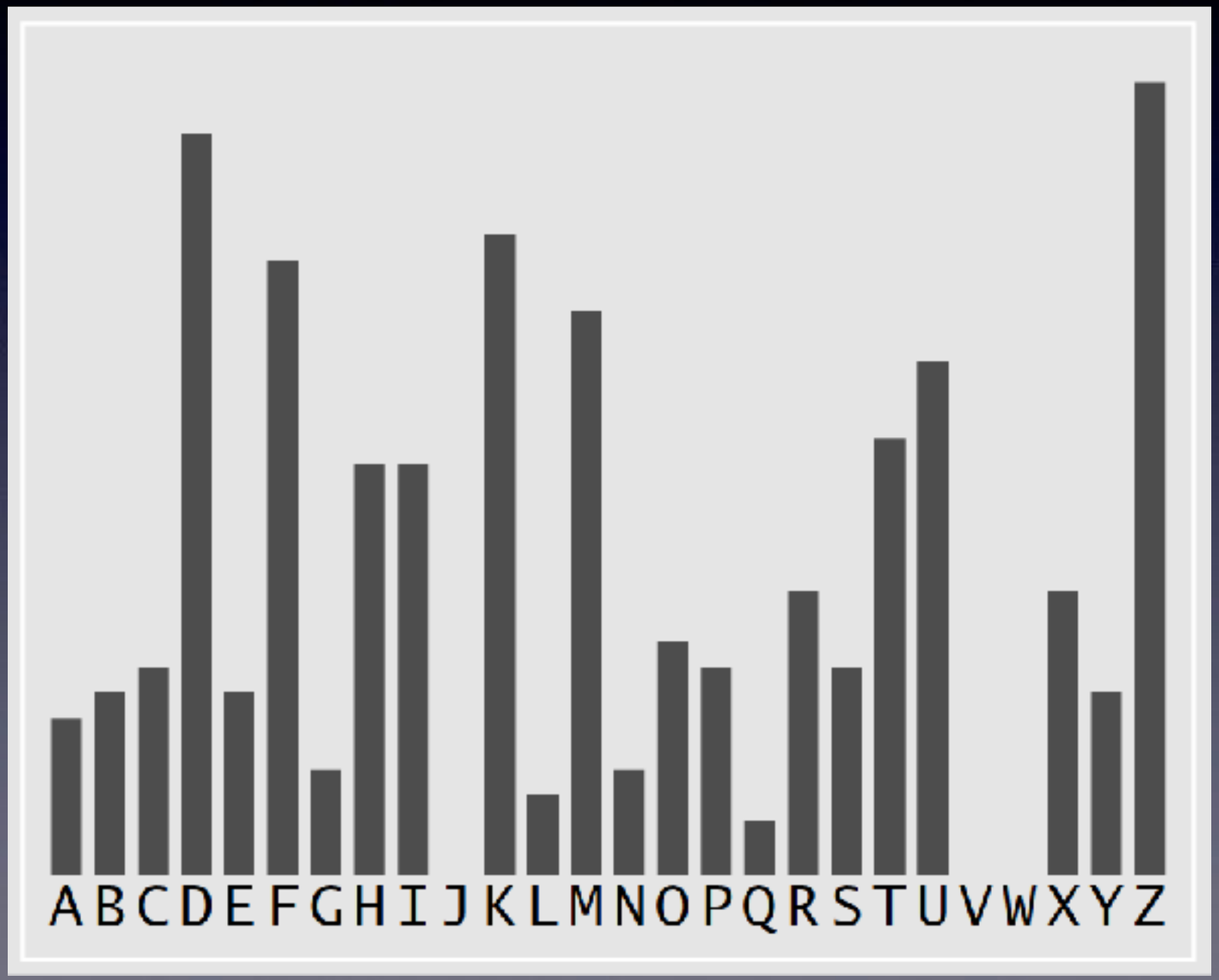
UJLQNKNTSN	HWYDAXAGFA	HWYDAXAGFA
VKMROLOUTO	IXZEBYBHGB	IXZEBYBHGB
WLNSPMPVUP	JYAFCZCIHC	JYAFCZCIHC
XMOTQNQWVQ	KZBGDADJID	KZBGDADJID
YNPURORXWR	LACHEBEKJE	LACHEBEKJE
ZOQVSPSYXS	MBDIFCFLKF	MBDIFCFLKF
APRWTQTZYT	NCEJGDGMLG	NCEJGDGMLG
BQSXURUAZU	ODFKHEHNMH	ODFKHEHNMH
CRTYVSVBAV	PEGLIFIONI	PEGLIFIONI
DSUZWTWCBW	QFHMJGJPOJ	QFHMJGJPOJ
ETVAXUXDCX	RGINKHKQPK	RGINKHKQPK
FUWBYVYEDY	SHJOLILRQL	SHJOLILRQL
GVXCZWZFEZ	TIKPMJMSRM	TIKPMJMSRM

Monoalfabeet

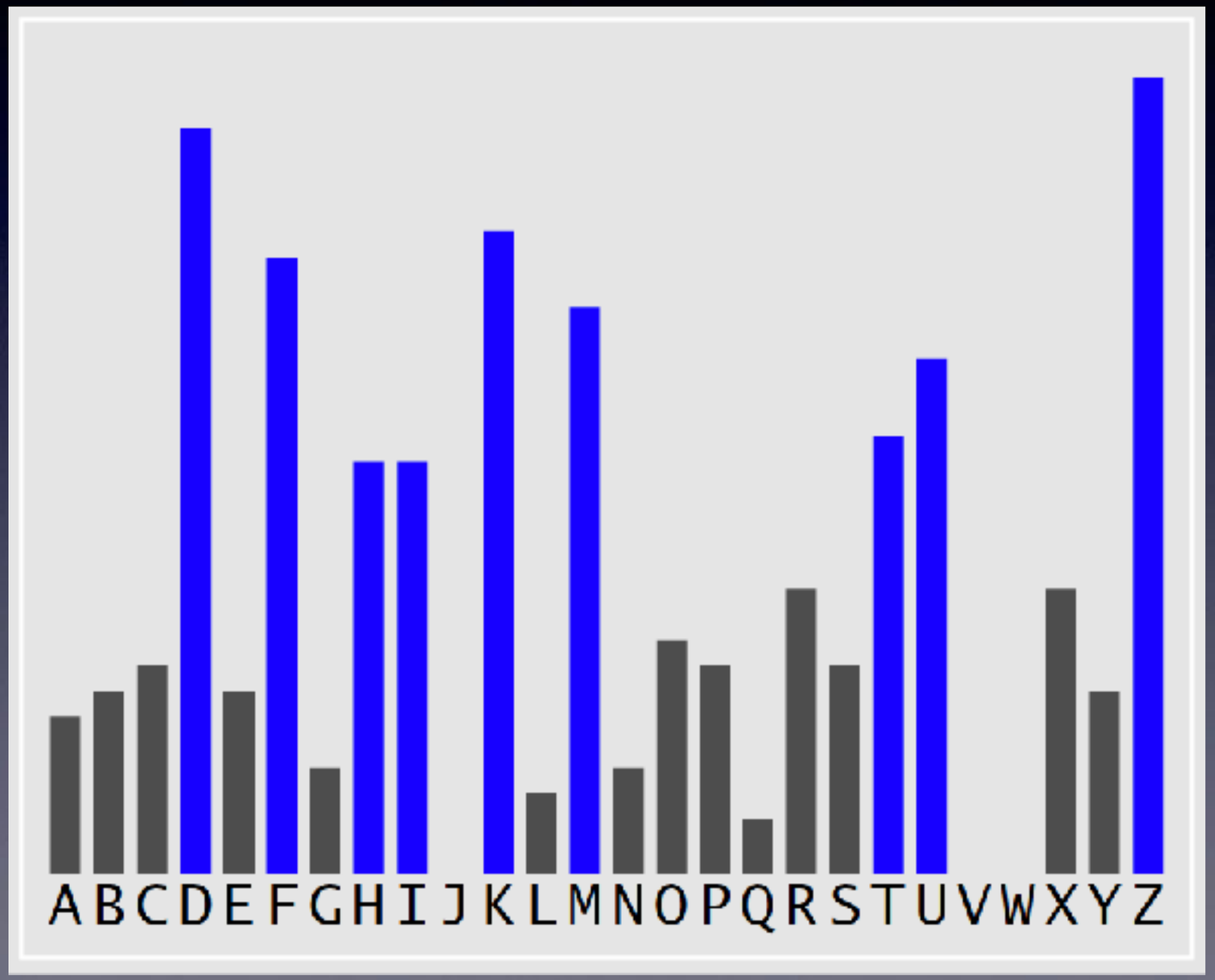
KFDKT BDFZM EUBDK FDPZY IOMMZ TXKUK ZYGUR
BZHAK FTHCM URMFU DMZHX MFTNM ZHXMD ZYTHC
PZQUR EZSSZ CDMZH XGTHC MZHXP FAKFD MDZTM
SUTYT HCFUK ZHXPF DKFDI NTCMF ZLDPT HCMSO
KPZTK ZSTKK FDUAM KDIME ITDXS DRUID PDFZL
DUOIE FZKRU IMUBD UROMZ IDUOK URSID ZKFZH
XZYYU ROMZI DRZKH UFOII AMZTX KFDEZ INDHK
DIKFD AKFZH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

A.S. Tanenbaum *Computer Networks*
maar hier in 5-letter groepen i.p.v. woordverdeling

Lettertelling

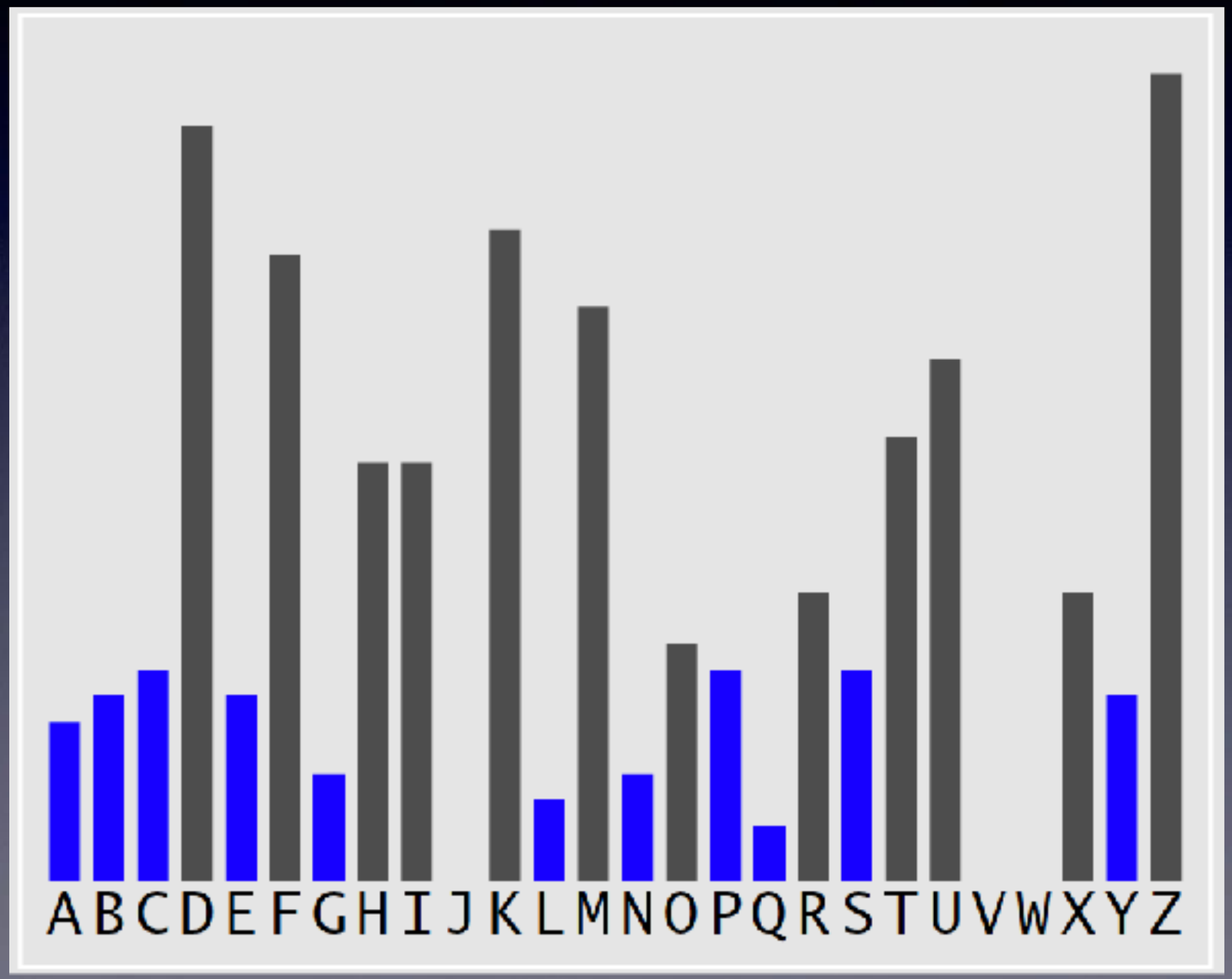


Hoge frequentie



E T A O N I R S H

Lage frequentie



B
C
F
G
J
K
M
P
Q
U
V
W
X
Y
Z

Contacten in kaart brengen
Consonantlijn

			Q	L
Z	Z	Z		
			U	
			D	D

Consonantlijn compleet

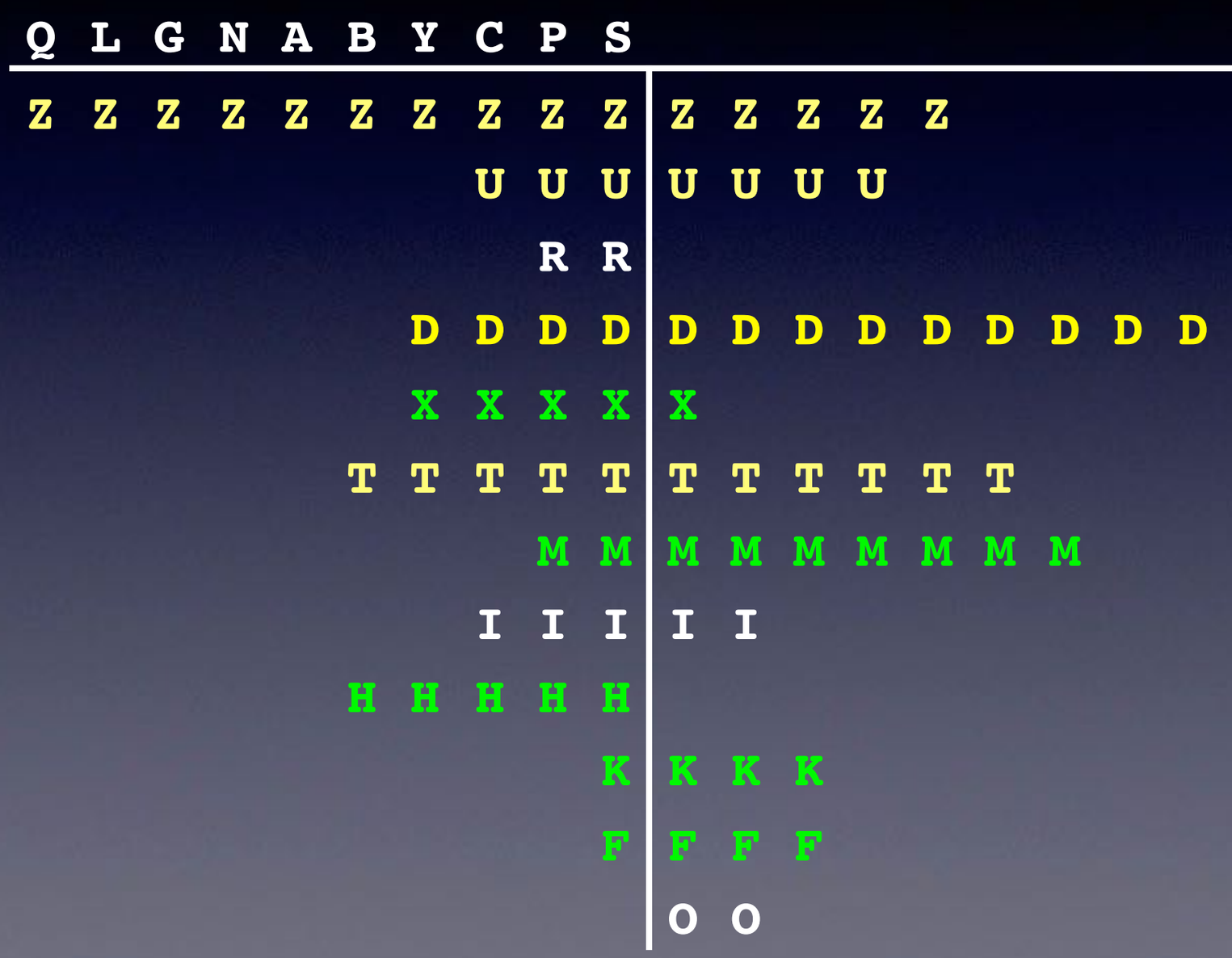
Q	L	G	N	A	B	Y	C	P	S					
Z	Z	Z	Z	Z	Z	Z	Z	Z	Z	Z	Z	Z	Z	Z
							U	U	U	U	U	U	U	U
								R	R					
						D	D	D	D	D	D	D	D	D
							X	X	X	X	X			
T	T	T	T	T	T	T	T	T	T	T	T	T	T	T
								M	M	M	M	M	M	M
							I	I	I	I	I			
H	H	H	H	H	H									
									K	K	K	K		
									F	F	F	F		
										O	O			

klinkers
links *en* rechts

A E I O
hoge frequentie

medeklinkers
links *of* rechts

Consonantlijn interpretatie



klinkers
links *en* rechts

A E I O
hoge frequentie

medeklinkers
links *of* rechts

H typisch voor n

H = n ?

Vooraf aan n vaak klinker & DTUZ = klinkers

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

ZH 8x TH 5x DH 1x KH 1x → H=n

Frequent digram KF

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

KF 11x *en* FK 0x → KF = th

KFD 7x KFZ 3x KFT 1x → D = e Z = a T = i,o

Samenvatting

K = t
F = h
D = e
Z = a
H = n

omdat
DTUZ klinkers

→ TU = i,o

omdat rs nog niet
en
IM hoge frequentie

→ IM = r,s

TU = io & IM = rs

```
KFDKTBDFZMEUBDKFDPZYIOMMZTXKUKZYGUR
theti.ehas.o.ethe.a.r.ssai.tota..o.
theti.ehar.o.ethe.a.s.rrai.tota..o.
theto.ehas.i.ethe.a.r.ssao.tita..i.
theto.ehar.i.ethe.a.s.rrao.tita..i.
```

```
BZHAKFTHCMURMFUDMZHXMFTNMZHXMDZYTHC
.an.thin.so.shoesan.shi.san.sea.in.
.an.thin.ro.rhoeran.rhi.ran.rea.in.
.an.thon.si.shiesan.sho.san.sea.on.
.an.thon.ri.rhieran.rho.ran.rea.on.
```

Keuze voor i,o & r,s

KFDKTBDFZMEUBDKFDPZYIOMMZTXKUKZYGUR

thetiehasoethearssaitotaoo

thetiehararoethearrraitotaoo

thetoehasiethearssaotitaoi

thetoehariethearsrraotitaoi

BZHAKFTHCMURMFUDMZHXMFTNMZHXMDZYTHC

anthinsoshoesanshisanseain

anthinrorhoeranrhiranreain

anthonsishiesanshosanseaon

anthonrirhieranrhoranreaon

T = i , U = o , I = r , M = s

KFDKTBDFZMEUBDKFDPZYIOMMZTXKUKZYGUR
theti ehas o ethe a r ssai tota o

BZHAKFTHCMURMFUDMZHXMFTNMZHXMDZYTHC
 an thin so shoesan shi san sea in

PZQUREZSSZCDMZHXGTHCMZHXPFAKFDMDZTM
 a o a a esan in san h theseais

SUTYTHCFUKZHXPFDKFDINTCMFZLDPTHCMSO
 oi in hotan hether i sha e in s

KPZTKZSTKKFDUAMKDIMEITDXSDRUIDPDFZL
t aita ittheo sters rie e ore eha

Wat is ZHX ?

```
KFDKTBDFZMEUBDKFDPZYIOMMZTXKUKZYGUR
theti ehas o ethe a r ssai tota  o

BZHAKFTHCMURMFUDMZHXMFTNMZHXMDZYTHC
 an thin so shoesan.shi san.sea in

PZQUREZSSZCDMZHXGTHCMZHXPFAKFDMDZTM
 a o  a  a esan. in san. h theseais

SUTYTHCFUKZHXPFDKFDINTCMFZLDPTHCMSO
 oi in hotan. hether i sha e in s

KPZTKZSTKKFDUAMKDIMEITDXSDRUIDPDFZL
t aita ittheo sters rie  e ore eha
```

X = d

KFDKTBDFZMEUBDKFDPZYIOMMZTXKUKZYGUR
theti ehas o ethe a r ssai tota o

BZHAKFTHCMURMFUDMZHXMFTNMZHXMDZYTHC
 an thin so shoesandshi sandsea in

PZQUREZSSZCDMZHXGTHCMZHXPFAKFDMDZTM
 a o a a esand in sand h theseais

SUTYTHCFUKZHXPFDKFDINTCMFZLDPTHCMSO
 oi in hotand hether i sha e in s

KPZTKZSTKKFDUAMKDIMEITDXSDRUIDPDFZL
t aita ittheo sters rie e ore eha

Woordherkenning

KFDKTBDFZMEUBDKFDPZYIOMMZTXKUKZYGUR
theti.ehas o ethe a r ssaidtota o

BZHAKFTHCMURMFUDMZHXMFTNMZHXMDZYTHC
 an thin.so shoesandshi.sandsea in

PZQUREZSSZCDMZHXGTHCMZHXPFAKFDMDZTM
 a o a a esand in sand h theseais

SUTYTHCFUKZHXPFDKFDINTCMFZLDPTHCMSO
 oi in hotand hether i sha e in s

KPZTKZSTKKFDUAMKDIMEITDXSDRUIDPDFZL
t aita ittheo.sters ried e ore eha

B=m, C=g, N=p, A= y

KFDKTBDFZMEUBDKFDPZYIOMMZTXKUKZYGUR
thetimehas o ethe a r ssaidtota o

BZHAKFTHCMURMFUDMZHXMFTNMZHXMDZYTHC
 an thingso shoesandships andsea in

PZQUREZSSZCDMZHXGTHCMZHXPFAKFDMDZTM
 a o a a esand in sand h theseais

SUTYTHCFUKZHXPFDKFDINTCMFZLDPTHCMSO
boilinghotand hether i sha e in s

KPZTKZSTKKFDUAMKDIMEITDXSDRUIDPDFZL
t aita itttheoysters ried e ore eha

Oplossing

KFDKTBDFZMEUBDKFDPZYIOMMZTXKUKZYGUR
thetimehascomethewalrussaidtotalkof

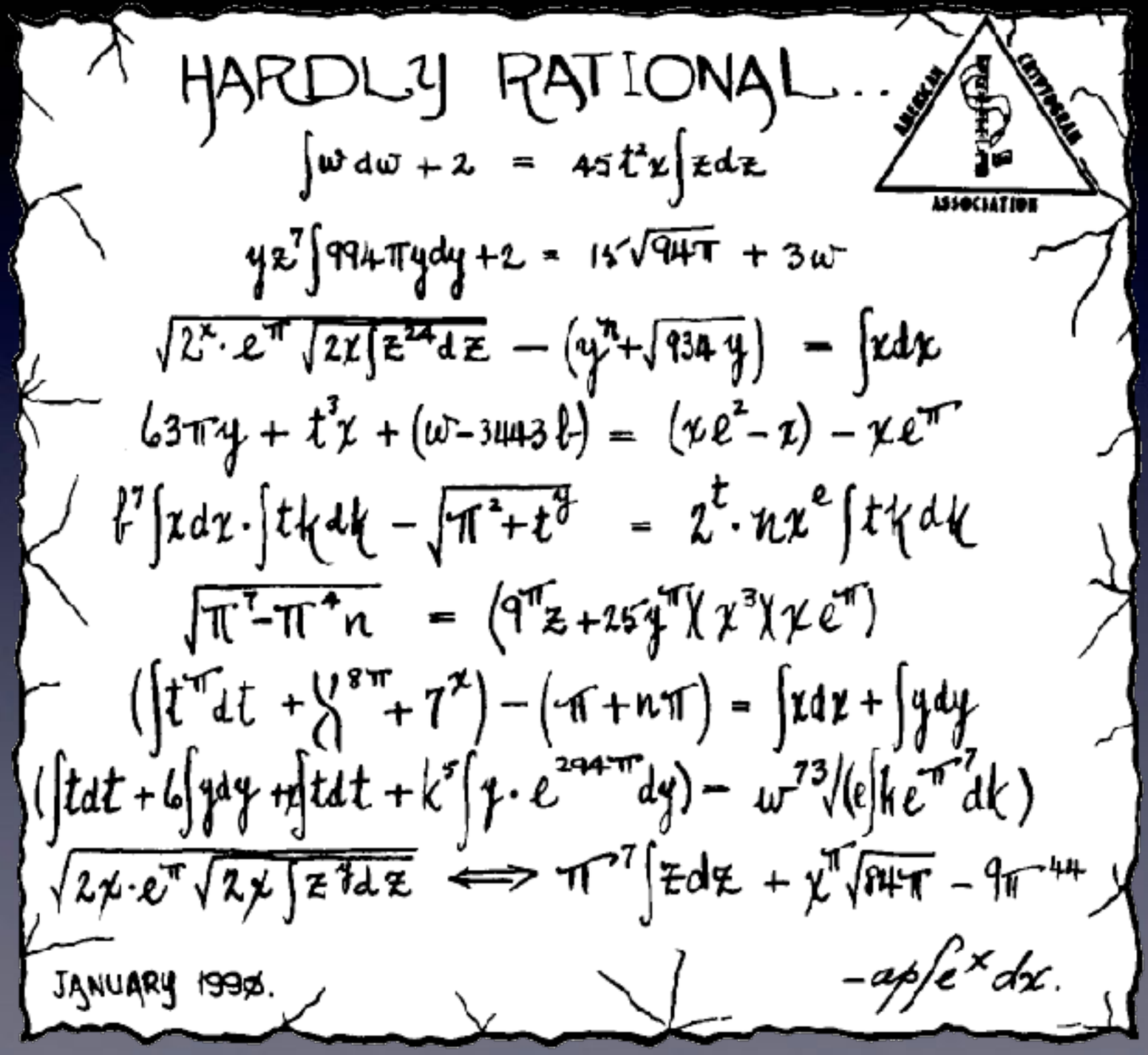
BZHAKFTHCMURMFUDMZHXMFTNMZHXMDZYTHC
manythingsofshoesandshipsandsealing

PZQUREZSSZCDMZHXGTHCMZHXPFAKFDMDZTM
waxofcabbagesandkingsandwhytheseais

SUTYTHCFUKZHXPFDKFDINTCMFZLDPTHCMSO
boilinghotandwhetherpigshavewingsbu

uit: Alice in Wonderland

Syllabus hoofdstuk 6



uit: ACA Cryptogram

Bonusopgaven aanpakken

- hoge letterfrequentie van etaonirsh
- contactgedrag = digramfrequenties
- begin- en eindletters van woorden
- classificatie klinkers-medeklinkers
- klinker-medeklinker wisseling
  niet - - - - - - of ++++++ maar +++-+ - - +
- letterpatroon
  bijvoorbeeld ABBCDDEE
- sleutelwoord in klaar- en/of cijferalfabet
  zie werkboek voor K1 en K2-type sleutel
- waarschijnlijke woorden
  hints in werkboek vercijferd met Caesar geheimschrift