Cursus Cryptografie

CRYPTOANALYSE

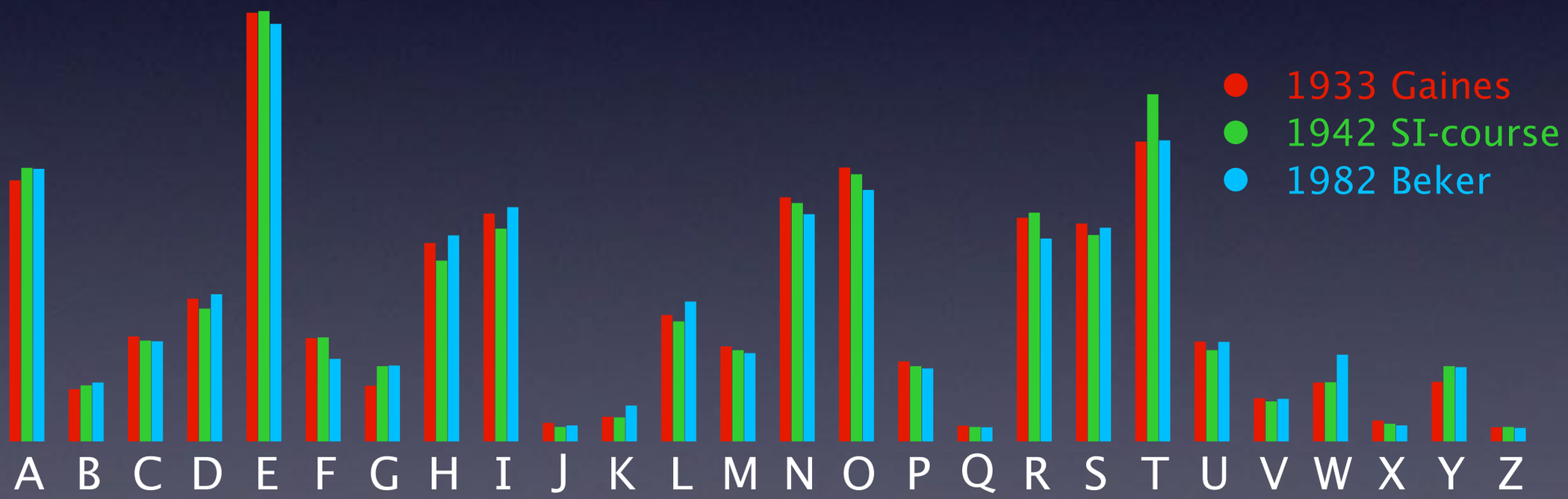
02-03-2017

Onderwerpen

- Monoalfabetische distributie
- Phi-test monoalfabeticiteit
- Periode bepalen
- Aantal letters bepalen
- Coïncidenties
- Chi-test distributie matching
- Voorbeelden

Monoalfabetisch

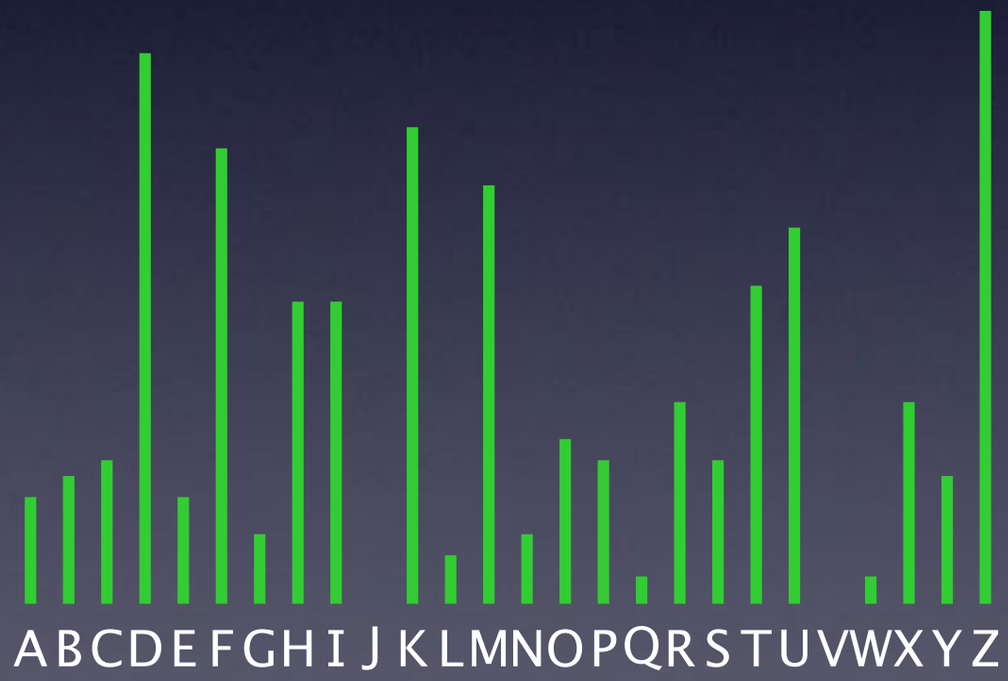
Centraal in de statistische cryptoanalyse is de letterdistributie



Polyalfabetisch

Doel polyalfabetische vercijfering: letterdistributie uitsmeren

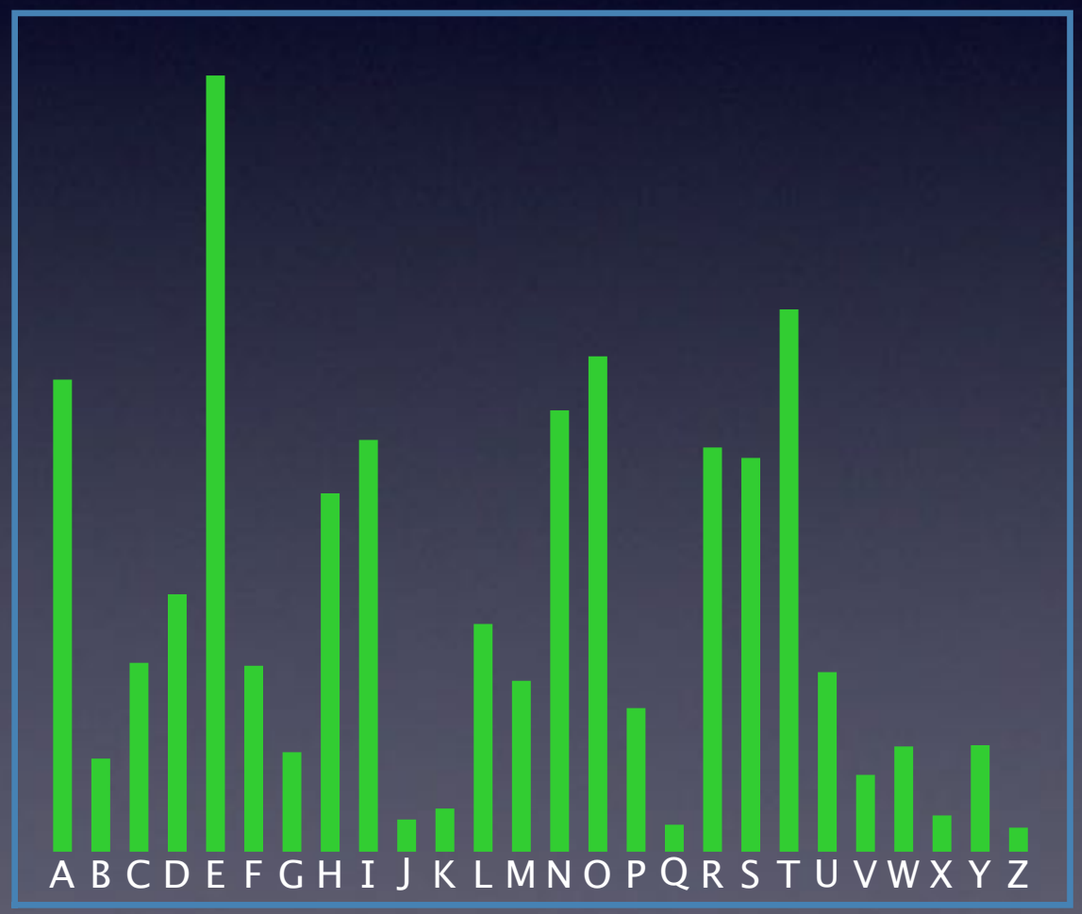
monoalfabetisch



polyalfabetisch

Tweede moment

Het tweede moment van de letterdistributie is het meest gebruikte instrument in de statistische cryptoanalyse



$$S_2 = p(A)^2 + \ldots + p(Z)^2$$

taal	S_2
• Engels	0.066
• Frans	0.078
• Duits	0.076
• Russisch	0.053
• Romaji	0.082
• random	0.038

Bepaal tweede moment

kans op bepaalde letter

$$p_i = \lim_{N \to \infty} \frac{f_i}{N} \quad \forall i = A, \ldots, Z \quad \text{met } N = \sum_{i=A}^{Z} f_i$$

tweede moment

$$S_2 = \sum_{i=A}^{Z} p_i^2$$

zuivere schatter Φ voor S_2

$$\Phi = \frac{\sum_{i=A}^{Z} f_i(f_i - 1)}{N(N-1)} \quad \text{met } N = \sum_{i=A}^{Z} f_i$$

Zuivere schatter

verwachtingswaarde $E(\Phi)$ uitrekenen

$$E(\Phi) = E\left(\sum_{i=A}^{Z} f_i(f_i - 1)\right) = \sum_{i=A}^{Z} E(f_i(f_i - 1)) = \sum_{i=A}^{Z} \left(E(f_i^2) - E(f_i)\right)$$

multinomiale verdeling voor kansen

$$p(f_A, f_B, \ldots, f_Z) = \frac{N!\, p_A^{f_A} p_B^{f_B} \ldots p_Z^{f_Z}}{f_A! f_B! \ldots f_Z!}$$

maak gebruik van

$$E(f_i) = Np_i \text{ en } var(f_i) = Np_i(1 - p_i) \text{ en } var(f_i) = E(f_i^2) - E(f_i)^2$$

Zuivere schatter

eliminatie van $E(f_i^2)$

$$E(\Phi) = \sum_{i=A}^{Z} \left(var(f_i) + E(f_i)^2 - E(f_i) \right)$$

substitutie van $E(f_i) = Np_i$ *en* $var(f_i) = Np_i(1 - p_i)$

$$E(\Phi) = \sum_{i=A}^{Z} \left(var(f_i) + E(f_i)^2 - E(f_i) \right)$$

resultaat

$$E(\Phi) = N(N-1) \sum_{i=A}^{Z} p_i^2 = N(N-1)S_2$$

Monoalfabeet

monoalfabetische substitutie =

```
ORDE LEIDT TOT ALLE DEUGDEN
WHZM VMQZU UWU YVVM ZMLXZMG
```

```
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 1       1 5             3 3 2 1 1 4
```

$\Phi_{CRYPTOGRAM} = 46$

$\Phi_{MONO} = 23x22x0,076 = 38 \pm 14$

$\Phi_{RANDOM} = 23x22x0,038 = 19 \pm 6$

Autoclaaf

klaartekst autoclaaf substitutie =

```
VYAND NADER TWATE RLINI ESTOP FORTA SPERE NPARA AT
KCNGD TOQZP TJDGE UPZGE ELXFA NBZXS LDTWS EIAJP EK
```

```
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
2 1 1 3 5 1 3   1 2 2 2   2 1 3 1   2 3 1   1 2   3
```

$\Phi_{CRYPTOGRAM} = 64$

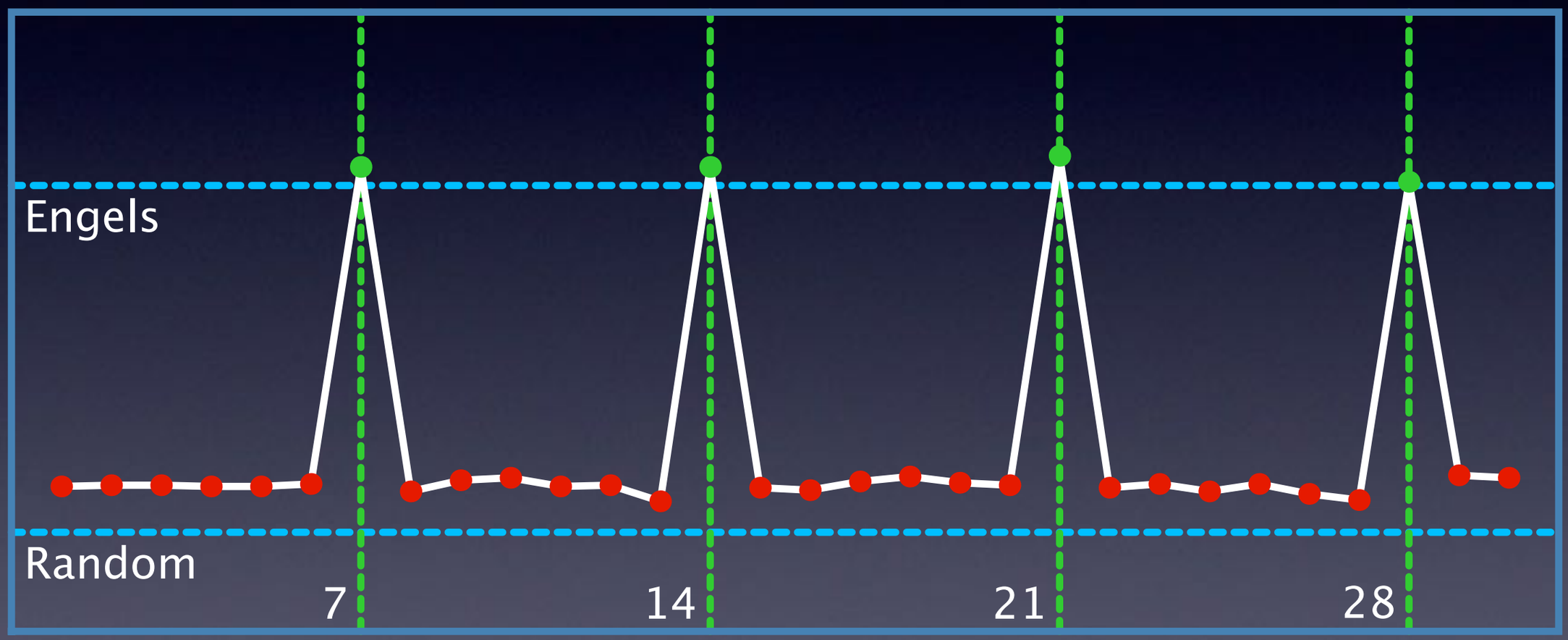
$\Phi_{MONO} = 42x41x0,076 = 131 \pm 32$

$\Phi_{RANDOM} = 42x41x0,038 = 65 \pm 11$

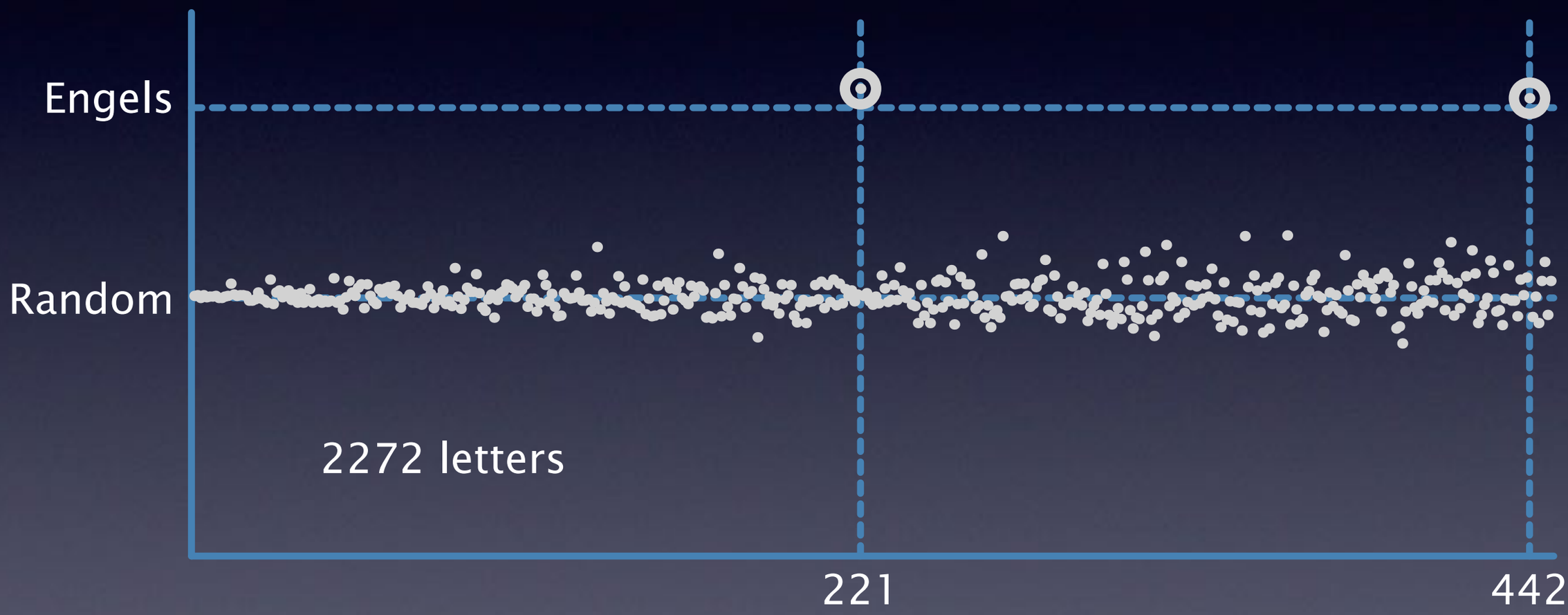
Periode polyalfabeet

1. veronderstel periode p
2. verdeel cryptogram in p groepen
3. bereken tweede moment voor alle groepen
4. bereken het gemiddeld tweede moment
5. test gemiddelde tegen monoalfabetische waarde
6. herhaal voor p = 1, 2, 3, enz.

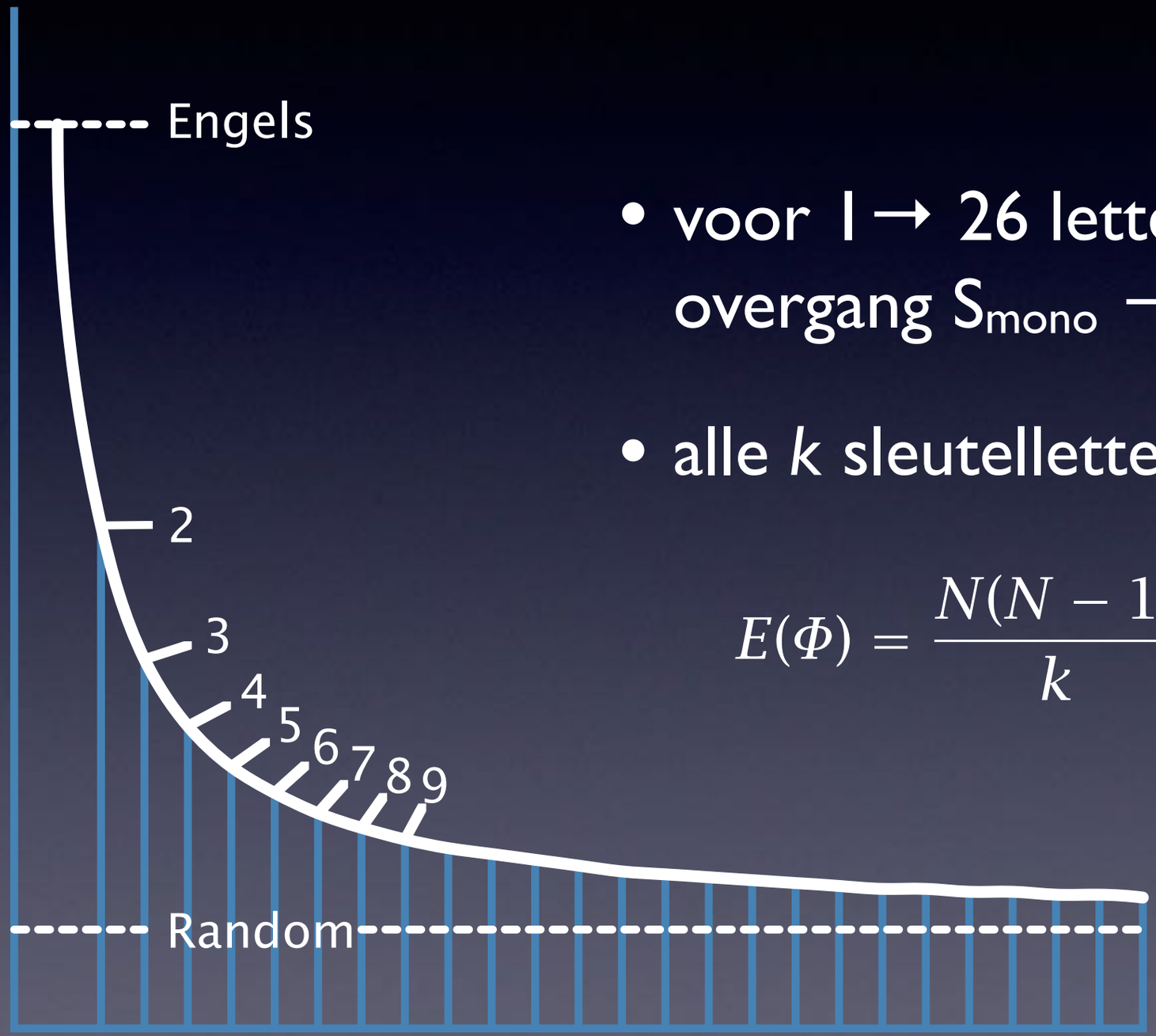
Periode Vigenère



Periode Kryha



Aantal sleutelletters



- voor $1 \rightarrow 26$ letters geleidelijke overgang $S_{mono} \rightarrow S_{26} > S_{random}$
- alle k sleutelletters verschillend

$$E(\Phi) = \frac{N(N-1)}{k}\left(S_2 + \frac{k-1}{26}\right)$$

Coincidenties

XWVVQBRTDDGZMBDEQPFMPMTUZQ…FVATFCKYZPJBMLFEPXZDODIUBILOAM
LBTNTIFYOIVTOZWHEBTMTDTINV…OVSANHWLQQDUFHXMIOUFFGMGXTQGON

PLANNENVANDEZEEROVERSVIELD…ORTEAFSTANDVANHETEILANDGEWORPE
ITTENVOUWDEKAARTOPENENLEGH…AATHETNOORDENMISSCHIENRONDKYKE

Poisson-verdeling met verwachting m en $\sigma = \sqrt{m}$

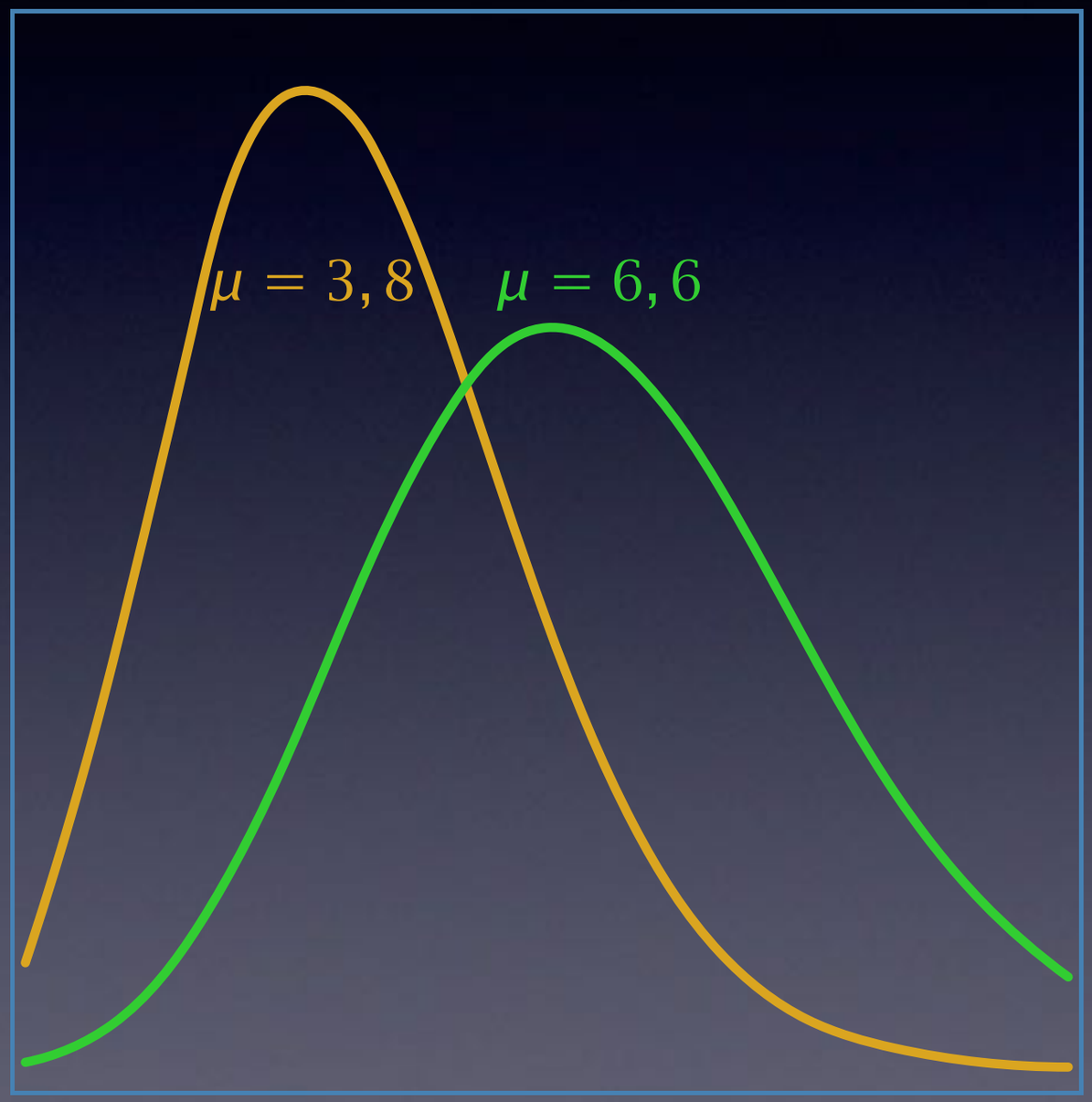
$$P(0) = e^{-m},\ P(1) = me^{-m},\ P(2) = \frac{m^2 e^{-m}}{2!} \cdots$$

Bij 100 letters coïncidentiekans = 100 $\times S_2$

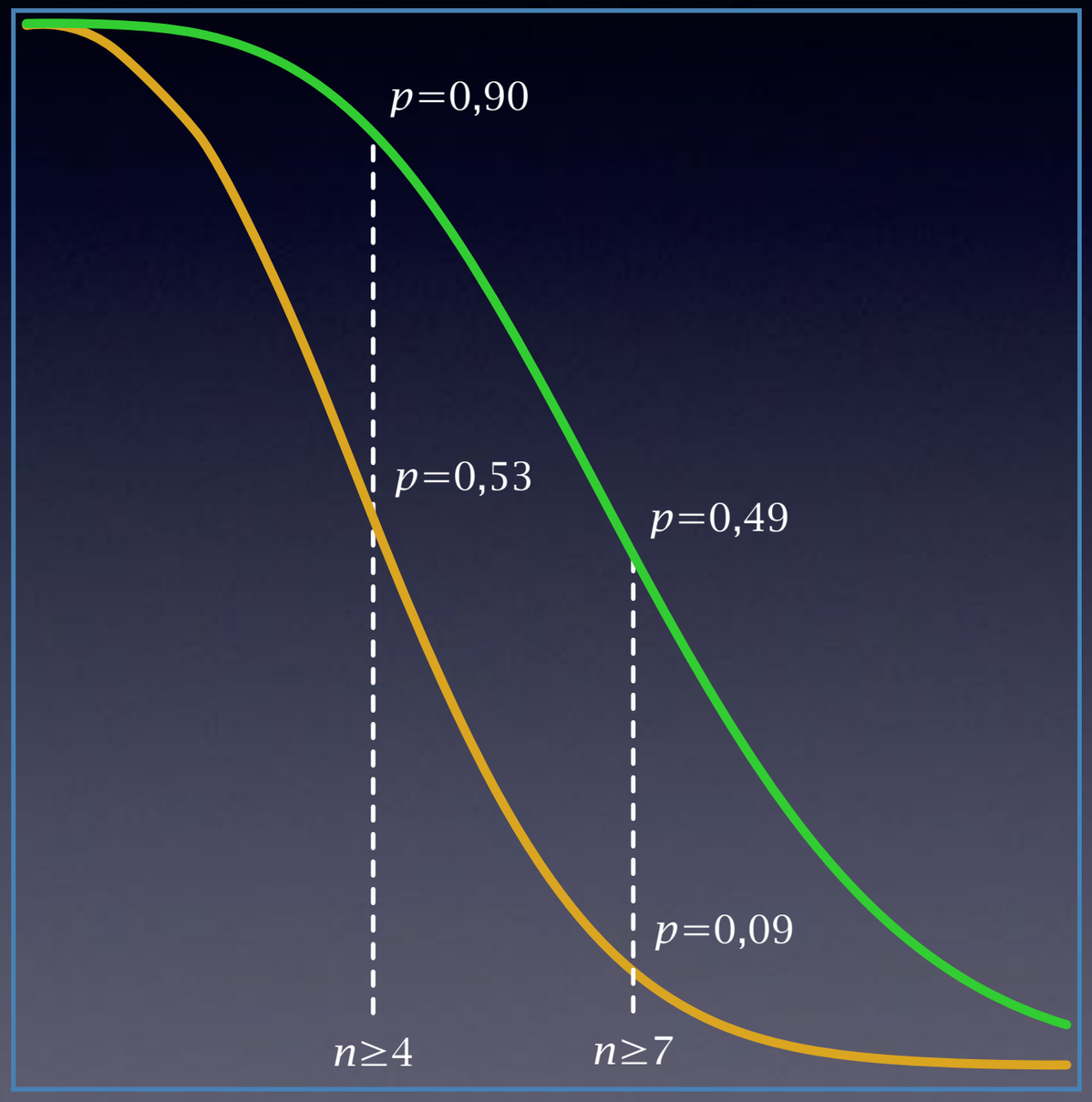
$m_{random} = 4 \pm 2$ $\quad$ $m_{monoalfabetisch} = 7 \pm 3$

Poisson verdeling

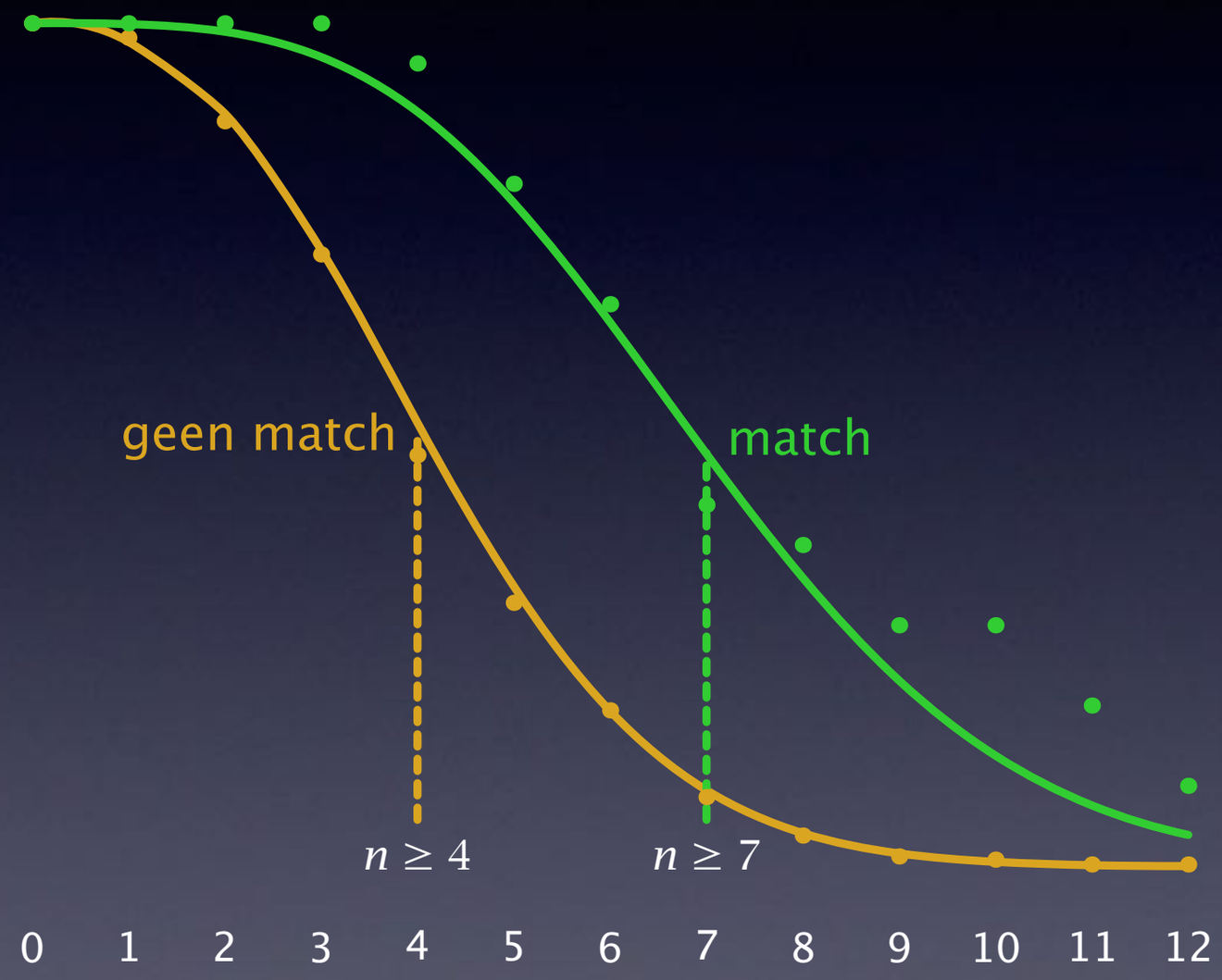
kans op n events



kans op n of meer events



Voorbeeld Vigenère



Coïncidenties cumulatief geteld
Vigenère 1673 letters
opgedeeld naar periode 7
100 letters per telling

525 geen match – 21 match

geen match – match		
# ≥ 7	43	9
# ≥ 12	1	2

Distributie match chi-test

meet overeenkomst tussen twee distributies

$$\chi = \sum_{i=A}^{Z} f_i f_i' \quad \text{met } N = \sum_{i=A}^{Z} f_i \text{ en } N' = \sum_{i=A}^{Z} f_i'$$

distributies hetzelfde

$$E(\chi) = NN' \sum_{i=A}^{Z} \frac{f_i f_i'}{NN'} = NN' \sum_{i=A}^{Z} p_i^2 = NN' S_2$$

distributies verschillend

$$E(\chi) = \frac{NN'}{n} \text{ met } n \text{ het aantal symbolen en } N = \sum_{i=A}^{Z} f_i$$

Chi-test voorbeeld

	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
f1:	1	4	0	3	0	1	0	0	1	0	0	1	0	0	1	0	0	3	2	2	1	0	1	3	0	2
f2:	0	2	0	0	0	3	0	0	1	0	1	0	0	1	1	0	0	3	1	1	0	0	0	0	1	2
f1f2:	0	8	0	0	0	3	0	0	1	0	0	0	0	0	1	0	0	9	2	2	0	0	0	0	0	4

som f1f2 = 30 0.667*26*17 = 29,5 0.038*26*17 = 17

match is waarschijnlijk

	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
f1:	1	4	0	3	0	1	0	0	1	0	0	1	0	0	1	0	0	3	2	2	1	0	1	3	0	2
f2:	2	0	0	0	3	0	0	1	0	1	0	0	1	1	0	0	3	1	1	0	0	0	0	1	2	0
f1f2:	2	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	3	2	0	0	0	0	3	0	0

som f1f2 = 10 0.667*26*17 = 29,5 0.038*26*17 = 17

match is onwaarschijnlijk

Voorbeeld match

Vigenère, 1673 letters, periode 7

- 21 matchende distributies
  verwachting $\chi_{21} = 3776 \pm 162$
  gevonden waarden 3599…4121
  $\chi = 3819 \pm 149$
- 525 niet-matchende distributies
  verwachting $\chi_{525} = 2197 \pm 361$
  gevonden waarden 1432…2909
  $\chi = 2132 \pm 303$

Resultaat chi-test

	12	13	14	15	16	17	23	24	25	26	27	34	35	36	37	45	46	47	56	57	67
A	369	434	485	574	357	260	410	375	276	439	298	307	396	374	347	443	357	306	363	372	520
B	362	355	499	312	341	373	374	302	316	315	430	370	416	296	281	304	327	286	337	332	444
C	350	508	318	322	305	415	411	318	335	348	350	381	498	380	372	298	362	365	336	335	323
D	368	331	291	441	307	443	298	348	310	388	398	500	389	374	355	438	325	479	382	395	252
E	275	314	400	731	411	453	434	372	353	646	454	392	364	396	481	393	381	348	324	503	382
F	329	236	650	418	420	401	374	342	327	370	372	366	367	387	390	311	397	301	355	365	408
G	420	344	434	381	383	369	666	348	514	391	353	353	448	259	511	342	625	438	367	269	408
H	748	387	396	211	430	304	409	492	428	300	290	479	463	295	213	251	404	408	690	440	404
I	379	415	249	356	280	445	332	360	409	348	407	401	301	351	274	302	325	315	403	360	399
J	402	398	349	359	312	317	260	423	417	354	371	302	254	488	442	413	309	313	365	348	226
K	242	274	365	338	431	377	409	422	459	373	523	255	277	426	630	446	445	409	336	302	343
L	383	360	387	323	702	462	313	441	401	383	370	304	437	474	398	392	428	417	482	377	376
M	345	426	345	336	409	405	403	385	367	293	430	401	410	352	366	394	362	378	384	418	663
N	466	723	383	471	410	312	351	428	407	383	254	431	569	411	321	455	387	377	396	342	352
O	300	439	450	409	223	219	280	355	281	343	318	528	273	412	402	450	275	426	320	368	345
P	344	330	360	412	351	364	448	281	294	452	346	305	325	355	451	413	249	273	255	449	311
Q	382	225	447	392	364	390	385	288	269	446	630	301	464	310	380	343	370	339	238	189	381
R	320	431	402	391	418	487	438	321	448	531	388	438	677	359	447	279	471	447	400	362	362
S	398	365	388	391	378	398	358	415	371	410	396	630	453	408	302	306	425	663	440	380	440
T	424	474	398	424	308	426	496	436	546	335	317	424	315	354	317	408	388	318	457	689	501
U	533	312	460	386	332	201	351	502	341	358	324	362	275	485	380	386	407	283	415	353	379
V	416	305	341	241	310	259	475	345	352	336	418	288	351	290	485	433	392	338	388	301	387
W	434	400	248	260	447	377	346	346	414	296	379	351	365	329	304	311	402	442	371	323	324
X	307	396	247	260	473	727	354	389	656	372	402	398	346	403	332	341	453	459	438	517	378
Y	413	444	311	424	500	411	295	594	371	453	362	388	326	608	391	436	354	428	433	408	345
Z	291	374	397	437	398	405	330	372	338	337	420	345	241	424	347	712	380	444	325	503	347

Voorbeelden Syllabus

- *Monoalfabeet*
  oplossing met consonantlijn
- *Vigenère*
  alfabet reconstructie met symmetrie in positie
  gemengd cijfertekst alfabet
- *Beaufort*
  alfabet reconstructie met isomorfen
  gemengd klaar- en cijfertekst alfabet
  decimatie van het alfabet