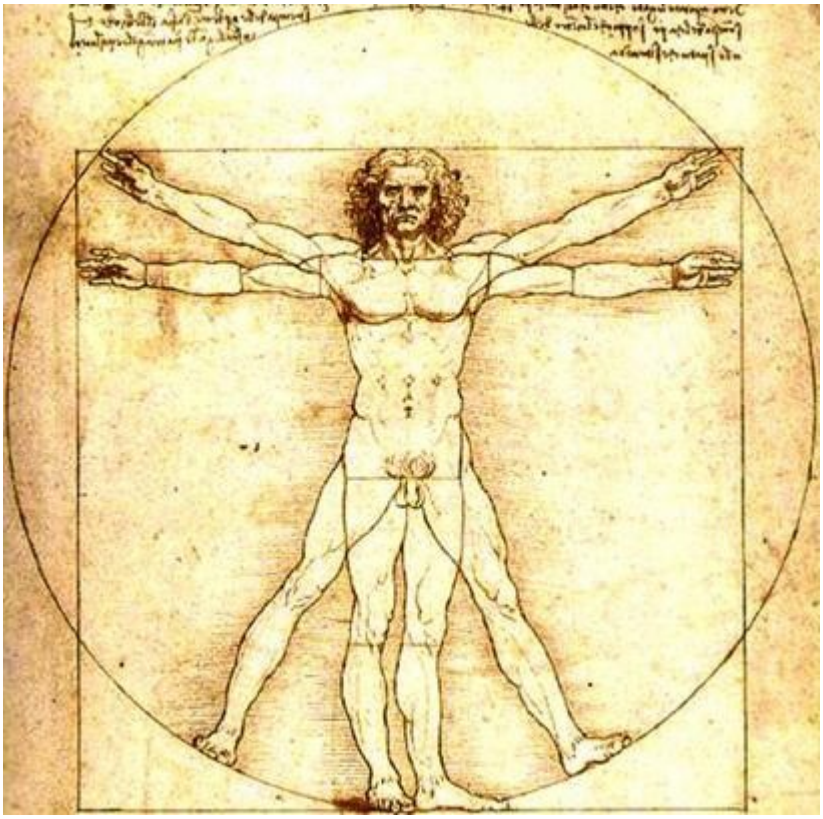
Uitwerking NBV Kerstpuzzel 2010



1
De tekst in de eerste opgave was:

```
363393939333966693336939363933339396933369393639363396669
363939639333963669669633396669666936339396393633936936969
333393693339669666963393693393666939633939666963639636393
369363396936936639333393393633966693339666936639333933933
696966696393963
```

De tekst is gecodeerd op een manier die op de (internationale) Morse code is gebaseerd. De 3 representeert '.' en 6 de '-' . Verder dient de 9 als scheiding tussen twee opeenvolgende letters.

Zo betekent 36339 de letter L, aangezien in Morse de L wordt gecodeerd als ".-.." .

De eerste vier letters uit de tekst worden gedecodeerd als:

```
363939393339
.-.. . . ...
  L  E E  S
```

De hele gedecodeerde tekst leest als volgt:

LEES OVER HET VERLOREN SYMBOOL EN LAAT HASMODAI JE DE OCCULTA PHILOSOPHIA TONEN

2
Het vierkant in de opgave is:

E U S Y M E W S T
E O T C F P N E 7
L P V E H A I U R
E E A E L A E O G
G L T A R I K E E
N E D T Z I R E N
P E R R E O G S N
D L K E D R E E L
E N A A R 6 S K 1

In het boek DE OCCULTA PHILOSOPHIA (hint uit opgave 1) worden verschillende magische vierkanten van verschillende grootte aan verschillende hemellichamen toegekend. Er wordt ook een 9-bij-9 vierkant in het boek met de maan geassocieerd en dit vierkant is hier gebruikt om de tekst te coderen. Ook HASMODAI is een hint naar dit vierkant: HASMODAI is een naam voor de "spirit of the moon" in het occulte.

Het magische vierkant van de maan wordt gegeven door:

37 78 29 70 21 62 13 54 5
 6 38 79 30 71 22 63 14 46
47 7 39 80 31 72 23 55 15
16 48 8 40 81 32 64 24 56
57 17 49 9 41 73 33 65 25
26 58 18 50 1 42 74 34 66
67 27 59 10 51 2 43 75 35
36 68 19 60 11 52 3 44 76
77 28 69 20 61 12 53 4 45

Dit magische vierkant heeft de eigenschap (net als ieder zogenaamd normaal magisch vierkant van 9-bij-9) dat de som van iedere rij, kolom en lange diagonaal precies 369 is – HASMODAI wordt om deze reden ook wel met het getal 369 aangeduid.

Een andere hint naar het gebruik van dit specifieke magische vierkant van de maan is het (gedeelte van een)

couplet aan het begin de kerstpuzzel. Dit komt uit het nummer LUNA SQUARE (maan vierkant) van de 80-er jaren band BOYTRONIC.

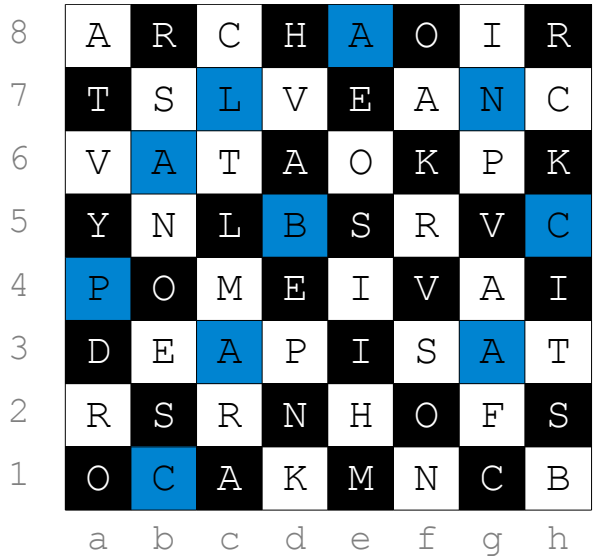
In het boek THE LOST SYMBOL van DAN BROWN (hint uit opgave 1) wordt een magisch vierkant (in dit geval een 8-bij-8 vierkant ooit gepubliceerd door BENJAMIN FRANKLIN) gebruikt om een boodschap te vercijferen op exact dezelfde manier als met het magische vierkant in deze opgave is gebeurd.

Het magische vierkant kan gebruikt worden voor het ontcijferen door de interpretatie dat de 37e letter van de verborgen boodschap de E is, de 78e letter de U is etc. Het herrangschikken van de 81 letters op deze manier levert op:

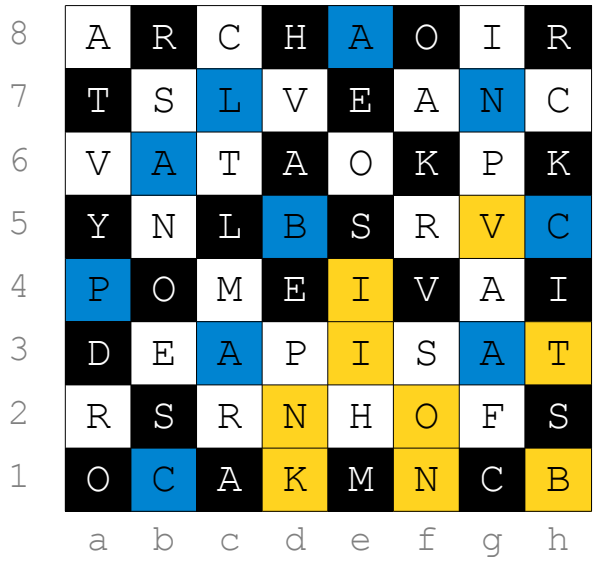
ZOEK TE PAARD 6 WERELDKAMPIOENEN SCHAKEN DE OVERIGE 17 LETTERS SUGGEREREN EEN PLAYFAIR SLEUTEL

3

Op het schaakbord moet gezocht worden naar schaakgrootmeesters. Als we met de C op het vak b1 (waar met schaken in het begin een wit paard staat) beginnen vinden we via negen paardensprongen de naam van oud wereldkampioen CAPABLANCA verscholen:



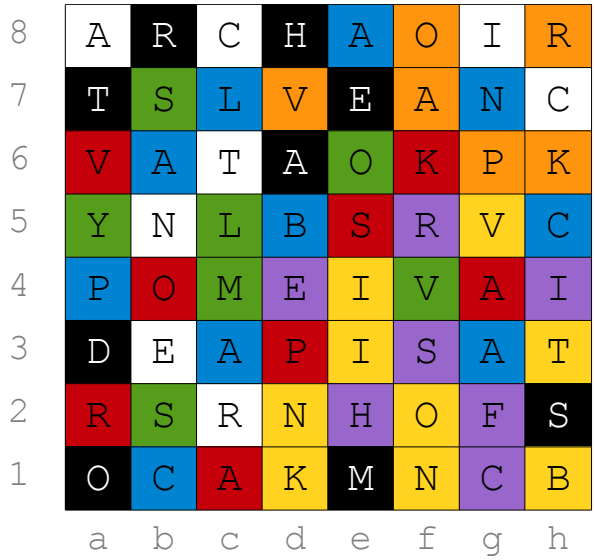
Als we vanuit de laatste A in CAPABLANCA doorgaan vinden we na wat puzzelen de naam van oud wereldkampioen BOTVINNIK:



Zo door gaan volgens het patroon hieronder aangegeven (waarbij we middels een paardensprong van de ene naam

naar de volgende komen) vinden we achtereenvolgens de volgende zes schaakgrootmeesters (in chronologische volgorde van het moment dat ze wereldkampioen werden):

CAPABLANCA (blauw), BOTVINNIK (geel), SMYSLOV (groen), FISCHER (paars), KARPOV (oranje), KASPAROV (rood)



De 17 overgebleven letters (die niet deel uitmaken van de namen van de schaakgrootmeesters) zijn hierboven overgebleven in zwarte of witte vakken en vormen samen de hint voor de gezochte PLAYFAIR sleutel:

ARCHITECT ANDERSOM

4

Uit opgave 2 hebben we dat het PLAYFAIR systeem gebruikt is. De hint ARCHITECT slaat op VITRUVIUS – een beroemde Romeinse architect. De tekening op het voorblad van de kerstpuzzel is namelijk de beroemde tekening van de VITRUVIUS MAN van LEONARDO DA VINCI.

Vul nu het PLAYFAIR vierkant met als sleutelwoord VITRUVIUS maar dan ANDERSOM, dus SUIVURTIV, dan levert dit:

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

De vercijferde tekst is:

QFPEH FABMT PBKSR TBMBD ECPOA CSKFE CESGV PPBKS GLUFD UNPLE TKQKC YNEGL TQHLM BDKMY PVTKX BXNHS LHKB

GLBN HFP QPO AIVU HTEC SIP AFSU ZBMF NPH VPAU LEU THOC LTK CYPV

Ontcijferen we dit dan krijgen we:

WELK GETAL ANDERS DAN ACHT ONTBREEKT HIERONDER EN WAAR MOET DEZE VOLGENS LEONARDO WORDEN INGEVOEGD

ENIG GEL ZON BUIS ECHT RUM DEUR WANG MOK ROUW ETS ACHT ODE VOOR

De veertien gegeven woorden hebben de eigenschap dat je er een enkele letter voor kunt zetten zodat er een nieuw Nederlands woord ontstaat.

Bij sommige woorden kan dit met verschillende letters (zoals bij ECHT, ROUW, ACHT of ODE), maar bij de meeste is er maar een enkele mogelijkheid (zoals (E)GEL, (O)ZON,

(A)BUIS, (D)RUM, (O)DEUR, (A)MOK of (I)VOOR).

Er zijn verchillende getallen die deze eigenschap ook hebben: (K)NUL, (B/N/G/H)EEN, (Z)ELF en (N/Z/W)ACHT (maar deze doet niet mee omdat er gevraagd wordt om een getal anders dan ACHT).

De vraag is nu welke getal ontbreekt en op welke plek hoort deze thuis. De LEONARDO uit de hint verwijst naar LEONARDO DA VINCI, van wie zoals gezegd de tekening van de VITRUVIUS MAN is die voorop de kerstpuzzel staat.

Het idee is nu dat je met de vijftien letters die je er voor zet, een zinnig en relevant woord vormt.

Wat puzzelen moet opleveren dat als je voor EEN een N plakt, je LEONARDO DA VINCI kunt spellen met de vijftien letters die voor de woorden kunnen worden geplakt:

(L)ENIG (E)GEL (O)ZON **(N)EEN** (A)BUIS (R)ECHT (D)RUM (O)DEUR (D)WANG (A)MOK (V)ROUW (I)ETS (N)ACHT (C)ODE (I)VOOR

De EEN ontbreekt dus en hoort tussen ZON en BUIS.

5

De tekst van het eerste gedeelte is:

NMREZ ILMEI OGRIO EZINE NNNEO IEENE LEEIE ILEZI LEOGN EOIRG RNOGL INNZM RANEO EEGRI ZILIN EOIEE NELGZ NNERG OGNEZ N

Het lastige van opgave 5 is wellicht dat er geen hint is gegeven - noch over het gebruikte systeem, noch over de gebruikte sleutel - en dat er dus geanalyseerd moet worden.

Wat opvalt is dat er maar 10 verschillende letters voorkomen. Dit suggereert dat niet elke letter maar ieder paar van letters een originele letter codeert. Als je de vercijferde tekst opdeelt in 48 bigrammen krijg je:

NM RE ZI LM EI OG RI OE ZI NE NN NE OI EE NE LE EI EI LE ZI LE OG NE OI RG RN OG LI NN ZM RA NE OE EG RI ZI LI NE OI EE NE LG ZN NE RG OG NE ZN

Dan valt verder op dat de eerste letter uit een bigram altijd komt uit de verzameling

N,R,Z,L,E,O

en de tweede letter altijd uit de verzameling

M,E,I,G,N,A

Hiermee zijn dus 36 mogelijke bigrammen te maken, waarvan er 21 daadwerkelijk voorkomen (met het bigram NE dat negen keer voorkomt als duidelijke uitschieter).

Verder valt op dat met de letters N,R,Z,L,E,O het woord LORENZ gemaakt kan worden en met de letters M,I,A,E,G,N het woord ENIGMA – beiden belangrijke Duitse cryptoapparaten uit de tweede wereldoorlog.

Het gebruikte vercijfermechanisme is onderstaand vierkant:

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

Om een letter te coderen zijn de letters uit het hoofd van de kolom en kop van de rij waar de letter zich bevindt achter elkaar gezet. Zo is de A gecodeerd als LE en de 2 als NM.

Ontcijferen levert de volgende tekst op:

2 CRYPTOBREKENDE APPARATEN UIT MK3 6EB VORMEN DE SLEUTEL

Het tweede gedeelte van de opgave is

VNESA HNDKS EAO8T NEOWN 1DEEE IVEOE GKETE E1TVR G3ASW RLIBN P0GLE VEHIT D6IOE HG

Een frequentie-analyse (veel E's en geen Q of X) van deze tekst doet vermoeden dat het gebruikte cryptosysteem geen substitutie is maar een transpositie (door elkaar husselen van de letters). Waarschijnlijk de meest gebruikte vorm van transpositie is een kolomtranspositie. Uit de hint van het eerste gedeelte volgt dat er twee sleutels zijn. Dit alles suggereert het proberen van een dubbele kolomtranspositie.

MK3 6EB uit de hint is de postcode van BLETCHLEY PARK.

De twee meest beroemde cryptobrekende apparaten van BLETCHLEY PARK waren waarschijnlijk de BOMBE (waarmee naar ENIGMA instellingen werd gezocht) en de COLOSSUS (waarmee naar LORENZ SZ 40/42 instellingen werd gezocht).

Om te ontcijferen verdelen we de tekst over vijf

kolommen, waarbij we boven de kolommen de letters van het woord BOMBE schrijven.

De volgorde waarin de kolommen gevuld worden wordt gedicteerd door de lexicografische volgorde van de letters in het codewoord BOMBE. De B komt het eerst, dus de eerste 14 letters VNESAHNDKSEAO8 komen in de eerste kolom (doordat de vercijferde tekst uit 67 = 13*5 + 2 letters bestaan de eerste twee kolommen onder de eerste B en de O uit 14 letters en de laatste drie kolommen uit 13 letters). De volgende 13 letters TNEOWN1DEEEIV komen onder de tweede B enz.

B	**O**	**M**	**B**	**E**
1	**5**	**4**	**2**	**3**
V	L	G	T	E
N	E	3	N	O
E	V	A	E	E
S	E	S	O	G
A	H	W	W	K
H	I	R	N	E
N	T	L	1	T
D	D	I	D	E
K	6	B	E	E
S	I	N	E	1
E	O	P	E	T
A	E	0	I	V
O	H	G	V	R
8	G			

Lezen we de tekst per rij uit:

VLGTE NE3NO EVAEE SESOG AHWWK HIRNE NTL1T DDIDE K6BEE SINE1 EOPET AE0IV OHGVR 8G

Vervolgens doen we hetzelfde met deze tekst en het tweede

codewoord COLOSSUS. Nu verdelen we de tekst over 8 kolommen. Omdat de tekst uit 67 = 8*8 + 3 letters bestaat, bestaan de eerste drie kolommen uit 9 letters, en de overige 5 kolommen uit 8 letters. De eerste kolom die gevuld moet worden is die van de C. Deze kolom moet 9 letters bevatten, dus VLGTENE3N. Zo verder gaan levert op:

C	**O**	**L**	**O**	**S**	**S**	**U**	**S**
1	**3**	**2**	**4**	**5**	**6**	**8**	**7**
V	O	O	R	D	E	V	O
L	G	E	N	D	E	O	P
G	A	V	E	I	S	H	E
T	H	A	N	D	I	G	T
E	W	E	T	E	N	V	A
N	W	E	L	K	E	R	E
E	K	S	1	6	1	8	0
3	H	E	T	B	E	G	I
N	I	S					

Als we nu per rij uitlezen, levert dit de originele tekst op:

VOOR DE VOLGENDE OPGAVE IS HET HANDIG TE WETEN VAN WELKE REEKS 161803 HET BEGIN IS

6

In de hint uit de vorige opgave wordt gevraagd van welke reeks 161803 het begin is. Hiermee wordt de decimale ontwikkeling van de gulden snede bedoeld:

1,61803398...

Bekijk de grijze letters op de eerste twee pagina's van de kerstpuzzel. Dit zijn:

Woord	**letter(s)**
years	S
magic	M
rich	I
it	T
he	H
way	Y
cryptische	C
opgaven	O
deze	DE
ontcijferd	N
kunnen	U
vorige	G
ontcijferde	C
zijn	J
wellicht	L
wat	A
makkelijker	K
gedeelte	T
tweede	E
gedeelte	GL
wat	W
lastiger	GR

uiteindelijke	K
eerste	RE
juist	U
tijd	J
geval	A
dingt	N
Behalve	H
Kijk	K
lossen	L
computer	R
gebruikt	G
CrypTool	C
gespeeld	GL

Dit levert de volgende verborgen boodschap op:

SMITHY CODE NUGCJ LAKTE GLWGR KREUJ ANHKL RGCGL

De SMITHY CODE is een code gebruikt door rechter SMITH om als grap een vercijferde boodschap te verstoppen in zijn vonnis in een rechtzaak over het boek THE DA VINCI CODE van DAN BROWN (rechter SMITH gebruikte *italic* letters in plaats van grijze letters).

De SMITHY CODE gebruikt een VARIANT BEAUFORT vercijfer mechanisme. Dit is (nagenoeg) het omgekeerde van het VIGENERE systeem. Als we de sleutel als een reeks getallen voorstellen, dan is het ontcijferalfabet dat bij getal n hoort het originele alfabet ABCD...XYZ geroteerd naar links over (n-1) posities. In de SMITHY code wordt een sleutelreeks met periode 8 gebruikt die afgeleid is van de FIBONACCI reeks. De eerste acht FIBONACCI getallen zijn

1,1,2,3,5,8,13,21

Rechter SMITH gebruikte de reeks getallen

1,1,25,3,5,8,13,21

Hieronder staan de ontcijfer-alfabetten voor de gebruikte acht sleutelgetallen.

	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	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
3	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B
5	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D
8	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G
13	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L
21	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T
25	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X

Een letter F in de vercijferde tekst wordt met sleutel-getal 5 dus ontcijferd tot de letter J. Ontcijferen we nu de boodschap NUGCJ LAKTE GLWGR KREUJ ANHKL RGCGL, dan levert dit op:

C:	N	U	G	C	J	L	A	K	T	E	G	L	W	G	R	K	R	E	U	
K:	1	1	25	3	5	8	13	21	1	1	25	3	5	8	13	21	1	1	25	

P:	N	U	E	E	N	S	M	E	T	E	E	N	A	N	D	E	R	E	S	

C:	J	A	N	H	K	L	R	G	C	G	L									
K:	3	5	8	13	21	1	1	25	3	5	8									

P:	L	E	U	T	E	L	R	E	E	K	S									

Dit levert dus als verborgen ontcijferde boodschap:

NU EENS MET EEN ANDERE SLEUTELREEKS

Het idee is nu om VARIANT BEAUFORT te gebruiken voor het ontcijferen van de tekst in opgave 6, maar dan met als sleutelreeks de reeks waarvan 161803 het begin is; de decimale ontwikkeling van de gulden snede.

De decimale ontwikkeling van de gulden snede begint als volgt:1,6180339887498948482045868343656381177203091798057628621576286213 54..

We maken weer een VARIANT BEAUFORT ontcijfer tabel, maar nu met de sleutelgetallen K = 0,1,..,9

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

Ontcijfering van de tekst uit de opgave levert nu op:

C: SKEXM KCLXX HGGGY BLMTZ OPAWV FCBLC AOYGT WIIQE MQSLF
K: 16180 33988 74989 48482 04586 83436 56381 17720 30917

P: SPEEL METEE NJONG ESPAA NSEDA MEENH ETANT WOORD OPALL

C: WLPLY ZMWVL BMNA
K: 98057 62862 1354

P: ESOPE ENDAM BORD

Oftewel:

SPEEL MET EEN JONGE SPAANSE DAME EN HET ANTWOORD OP ALLES OP EEN DAMBORD

7

De hint DAMBORD refereert aan het (STRADDLE) CHECKERBOARD systeem. Voor (een eenvoudige instantiatie van) dit systeem is een woord van acht verschillende letters nodig en twee getallen onder de tien. Het woord van acht letters is gegeven, namelijk JONGE SPAANSE DAME, ofwel SENORITA.

Het ANTWOORD OP ALLES verwijst naar THE HITCHIKERS GUIDE TO THE GALAXY, waar THE ANSWER TO THE ULTIMATE QUESTION IN LIFE, THE GALAXY, EVERYTHING wordt gegeven: 42. Hiermee kunnen we het checkerboard vullen:

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

De tekst uit de opgave valt nu uiteen in:

```
45  1  8  0 26  0  8  1  1 49  7  0  0  7 41  7 48  7  9
 9  3  0  1  3 42  1 47 48  9  6  1  8  1 47  0  8 40  1
23  9  8 45  1  8 24  5  5  6 42 20  6  7  1 49 44  1  8
 9 48
```

Dit ontcijfert tot:

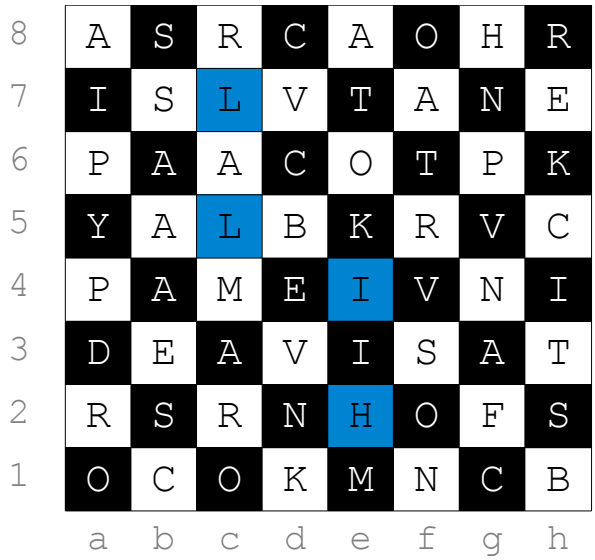
```
 H  E  T  S  Y  S  T  E  E  M  I  S  S  I  C  I  L  I  A
 A  N  S  E  N  D  E  K  L  A  R  E  T  E  K  S  T  B  E
 V  A T   H  E  T  W  O  O  R  D  P  R  I  E  M  G  E  T
 A  L
```

Oftwel:

HET SYSTEEM IS SICILIAANS EN DE KLARE TEKST BEVAT HET WOORD PRIEMGETAL

8

We weten het gebruikte systeem niet, maar de hint is SICILIAANS. Dit refereert naar de Siciliaanse schaakopening, die begint met de zetten e2-e4 en c7-c5. Als we de vakjes e2,e4,c7,c5 op het schaakbord van opgave 3 bekijken zien we hier de naam van het gebruikte systeem: HILL.



Aangezien het aantal letters 78 = 2*3*13 een veelvoud van zowel twee als drie is, is het niet meteen duidelijk of een 2-bij-2 of een 3-bij-3 matrix gebruikt is. Proberen een 2-bij-2 matrix te achterhalen levert niets op (CrypTool kan dit automatisch gegeven de informatie dat PRIEMGETAL in de klare tekst voorkomt, aangezien PRIEMGETAL uit voldoende letters bestaat).

Voor het eenduidig achterhalen van een 3-bij-3 matrix is PRIEMGETAL te kort (hiervoor zijn 12 achtereenvolgende letters nodig). We moeten dus echt aan het werk. Er rest niets anders dan alle mogelijke startposities van de vercijfering van PRIEMGETAL af te lopen, de bijbehorende ontcijfermatirx te achterhalen, de rest van de tekst te ontcijferen, en kijken of er iets zinnigs uit komt.

De vercijfering van PRIEMGETAL blijkt dan op positie 39 te beginnen. Delen we de vercijferde tekst op in

trigrammen dan levert dit (met de vercijfering van PRIEMGETAL vetgedrukt):

ABH QBI ZIR RJH IPY APW BUN MUP JKI MBB KGK VKF LN**E**
MJQ AAE KKT EUX GPV CYD MQC AUM ORS EFW QFO UJT TYQ

De negen letters MJQ AAE KKT moeten dus ontcijferen als RIE MGE TAL.

Nu is het zaak de ontcijfermatrix

$$\begin{matrix} a & b & c \\ d & e & f \\ g & h & i \end{matrix}$$

te achterhalen. Als we de codering A=0, B=1, .., Z=25 aanhouden, dan zijn we dus op zoek naar negen getallen a,b,c,d,e,f,g,h,i zodat:

$$\begin{aligned} a*12 + b*9 + c*16 &= 17 \pmod{26} \\ d*12 + e*9 + f*16 &= 8 \pmod{26} \\ g*12 + h*9 + i*16 &= 4 \pmod{26} \end{aligned}$$

(MJQ = 12,9,16 moet ontcijferd worden als RIE = 17,8,4) en:

$$\begin{aligned} a*0 + b*0 + c*4 &= 12 \pmod{26} \\ d*0 + e*0 + f*4 &= 6 \pmod{26} \\ g*0 + h*0 + i*4 &= 4 \pmod{26} \end{aligned}$$

(AAE = 0,0,4 moet ontcijferd worden als MGE = 12,6,4) en:

$$\begin{aligned} a*10 + b*10 + c*19 &= 19 \pmod{26} \\ d*10 + e*10 + f*19 &= 0 \pmod{26} \\ g*10 + h*10 + i*19 &= 11 \pmod{26} \end{aligned}$$

(KKT = 10,10,19 moet ontcijferd worden als TAL = 19,0,11)

Dit systeem heeft een enkele oplossing (modulo 26) in de vorm van

```
a b c     8 9 3
d e f  =  3 0 8
g h i     1 6 1
```

Het is uiteraard geen toeval dat de oplossing voor a,b,..,i bestaat uit de eerste negen getallen uit de decimale ontwikkeling van de gulden snede, maar dan andersom a la het gebruik van SUIVIRTIV als PLAYFAIR sleutel in opgave 4.

Nu de decryptiematrix bepaald is, kan de rest van de tekst ontcijferd worden. Bijvoorbeeld het trigram ABH = 0,1,7 ontcijferen levert:

```
8*0 + 9*1 + 3*7 = 30 =  4 (modulo 26)
3*0 + 0*1 + 8*7 = 56 =  4 (modulo 26)
1*0 + 6*1 + 1*7 = 13 = 13 (modulo 26)
```

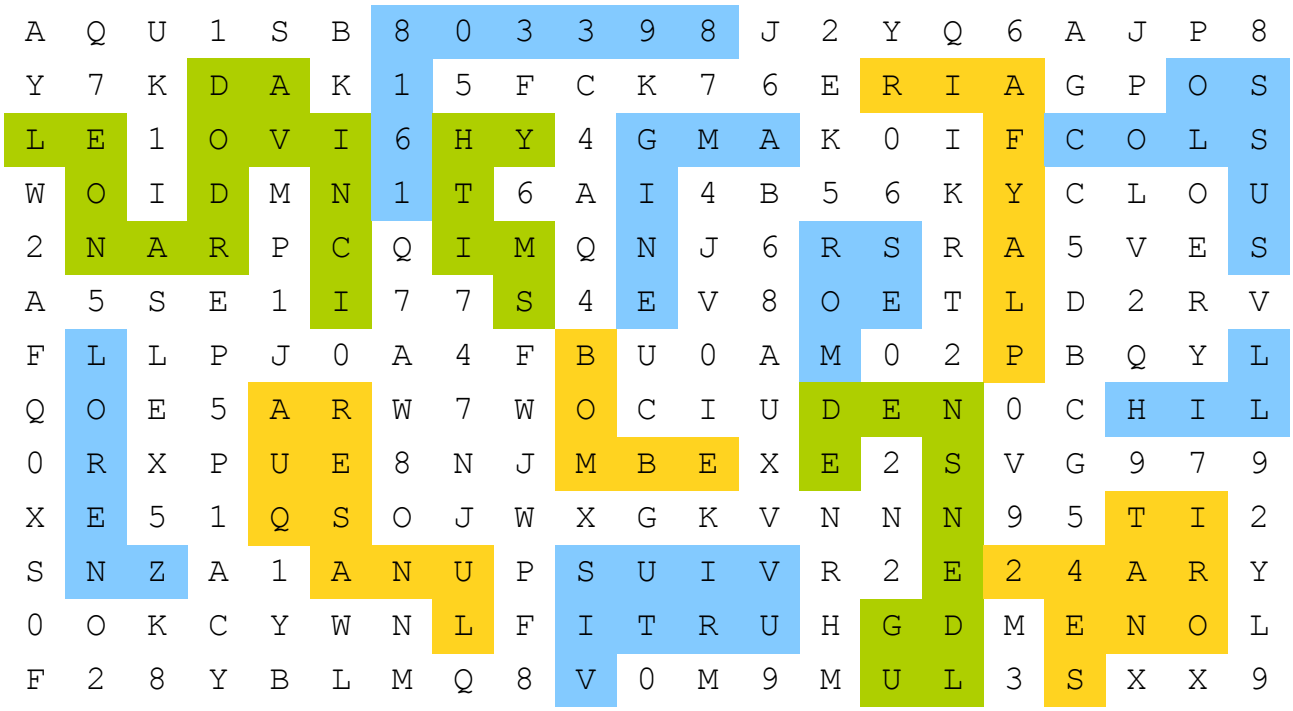
en dus is EEN de ontcijfering van ABH. Zo verder gaan levert de complete ontcijferde tekst:

EEN FIELD MEDALIST UIT DE JAREN ZESTIG EN ZIJN PRIEMGETAL VORMEN HET MAGISCHE EN GEHEIME PAD

De field medalist (equivalent van de Nobelprijs voor de wiskunde) waaraan gerefereerd wordt is GROTHENDIECK (kreeg de medaille toegewezen in 1966). Een legendarische anecdote rond GROTHENDIECK is dat hij ooit 57 = 3*19 als voorbeeld van een priemgetal gaf. Sindsdien staat 57 bekend als het GROTHENDIECK priemgetal.

9

Wat op te merken valt is dat een heleboel woorden die belangrijk zijn (geweest) in deze kerstpuzzel in de rechthoek zijn terug te vinden:



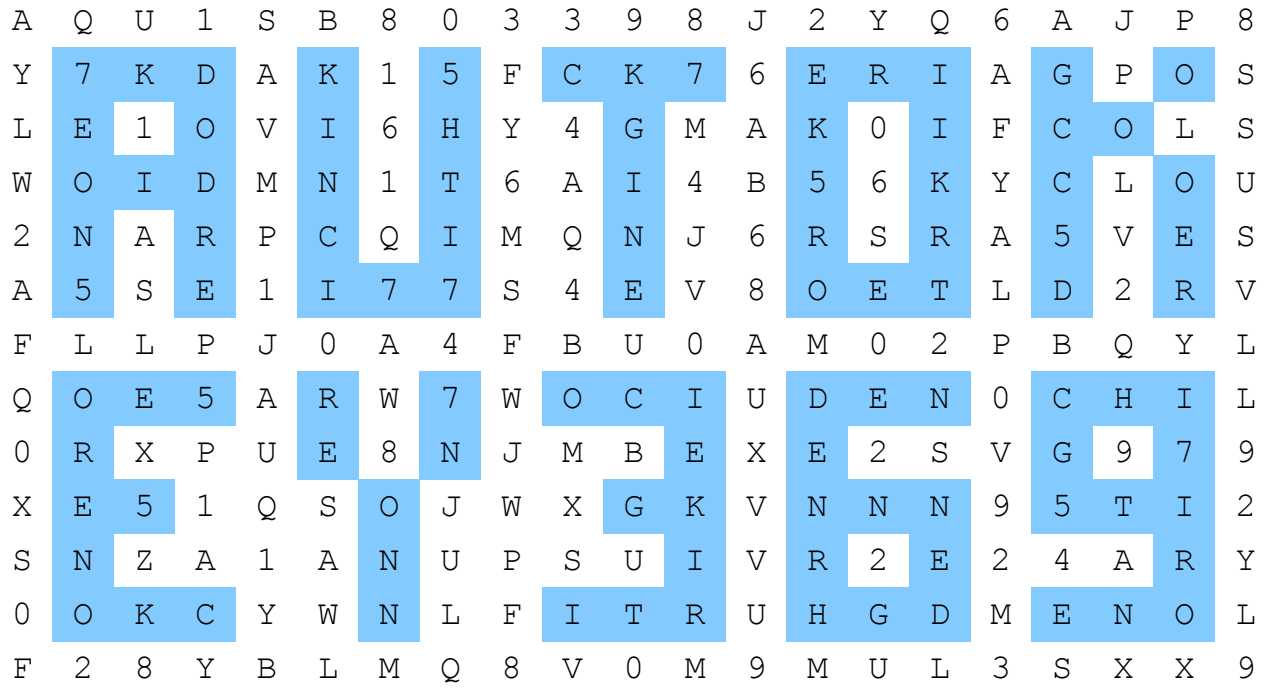
Namelijk de volgende woorden zijn terug te vinden:

MORSE LUNASQUARE 161803398 LORENZ ENIGMA BOMBE COLOSSUS PLAYFAIR LEONARDODAVINCI SMITHY VITRUVIUS HILL GULDENSNEDE SENORITA42

Een aardigheid, maar tevens bedoeld de oplettende puzzelaar het idee aan te reiken dat er in het rechthoek gezocht moet worden naar de oplossing.

De hint HET MAGISCHE EN GEHEIME PAD slaat op het stuk tekst van LUNA SQUARE waarmee de kertspuzzel begint, te weten HE KNOWS THE MAGIC THAT MAKES IMAGES.. AND HE'S THE ONE WHO KNOWS THE SECRET WAY. Dit suggereert dat GROTHENDIECK en 57 samen afbeeldingen kunnen maken.

En inderdaad, als we alle letters en cijfers van GROTHENDIECK en 57 inkleuren, dan zien we het volgende:



Hiermee hebben we de laaste hint te pakken: AUTOKEY 369.

Uiteraard niet geheel toevallig is 369, zoals eerder opgemerkt, de som van ieder rij, kolom en lange diagonaal in het magische vierkant uit opgave 2 en wordt ook wel HASMODAI (spirit of the moon) genoemd, zoals in de hint uit opgave 1.

Het gebruikte systeem is de VIGENERE TEXT AUTOKEY variant, met als sleutelwoord HASMODAI. Ontcijferen we de text hiermee dan vinden we

IN ONDERSTAANDE REEKS ONTBREEKT WELK LAND JEMEN MALAWI SIERRA LEONE SLOWAKIJE EGYPTE DUITSLAND COLOMBIA PARAGUAY LESOTHO ETHIOPIE

De truc zit in de vlaggen van de betrokken landen. Van elk land bestaat de vlag uit drie horizontale strepen in drie verschillende kleuren. De volgorde van de landen wordt bepaald doordat de onderste kleur op de vlag van een land overeenkomt met de bovenste kleur van de vlag van het volgende land. Dit geeft de volgende tabel, met een gat tussen SIERRA LEONE en SLOWAKIJE.

LAND	VLAG
JEMEN	
MALAWI	 (tot juni 2010)
SIERRA LEONE	
?	
SLOWAKIJE	
EGYPTE	
DUITSLAND	
COLOMBIA	
PARAGUAY	
LESOTHO	
ETHIOPIE	

Er is een land waarvan de vlag uit drie horizontale strepen bestaat, waarvan de bovenste blauw en de onderste wit, namelijk ESTLAND met de volgende vlag:

Enige onbedoelde moeilijkheid zat in het feit dat MALAWI nadat de puzzel gemaakt was maar voordat deze uitkwam, de nationale vlag had gewijzigd, waardoor deze nu rood-zwart-groen als patroon had. Gelukkig bleek de opgave toch op te lossen, gezien de inzendingen..

De volledige oplossing van de NBV kerstpuzzel 2010 was dus:

Eerste gedeelte
EEN, en deze moet tussen ZON en BUIS worden ingevoegd

Tweede gedeelte
ESTLAND