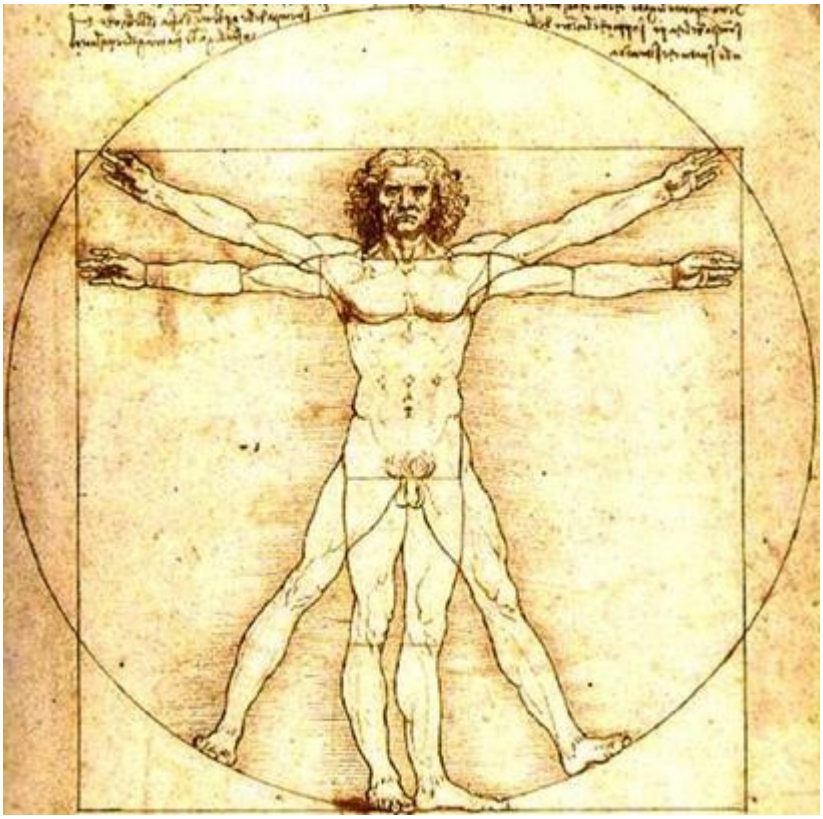
Solution NLNCSA XMas Puzzle 2010



1

The text in the first exercise was:

```
3639393696339369633396669336969693333939363396669333969333
3963669669633396669363393696396339633939693333936933396 6
9666963393693396639336933963393963669666933696933339363966
6693369663933339633939666963639636393369363396936636933
3393393633966693339666936639333393393 6
```

The code used is based on (international) Morse code. The 3 represents a '.' and 6 represents a '-'. For example 363 encodes the letter R, since in Morse the R is coded as ".-." . The 9 is used to seperate two consecutive letters.

For example, the first four letters are encoded as:

```
363939369639
.-. . .- -..
 R  E  A  D
```

The complete decoded text reads:

READ ABOUT THE LOST SYMBOL AND LET HASMODAI GUIDE YOU THROUGH DE OCCULTA PHILOSOPHIA

2

The square in the exercise is:

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

In the book DE OCCULTA PHILOSOPHIA (first hint from exercise 1) different magic squares of different sizes are related to various celestial bodies. The following 9-by-9 magic square is related to the moon (where HASMODAI is the spirit of the moon):

```
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
```

In this magic square the sum of each row, column and long diagonal equals 369 (note the number 369 also represents HASMODAI).

A second reference to this particular magic square is given at the very start of this years Xmas puzzle. It starts with part of the lyrics from the 80s song LUNA SQUARE by BOYTRONIC.

In THE LOST SYMBOL by DAN BROWN (second hint from exercise 1) a magic square is used to encode a secret message (the magic square used there is an 8-by-8 square published by BENJAMIN FRANKLIN). Here the 9-by-9 magic

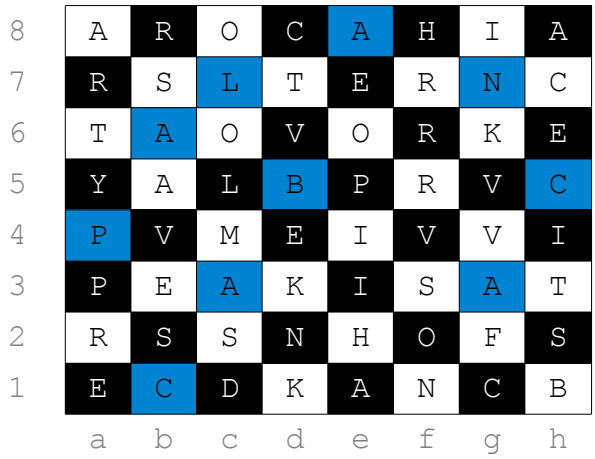
square of the moon is used to encode the first square in the exercise.
Decryption can be performed by setting the 37^{th} letter of the plain text to an P, the 78^{th} letter in the plaintext to a R and so on. This gives:

TAKE A KNIGHT AND FIND THE 6 CHESS WORLD CHAMPIONS THE 17 REMAINING LETTERS SUGGEST A PLAYFAIR KEY

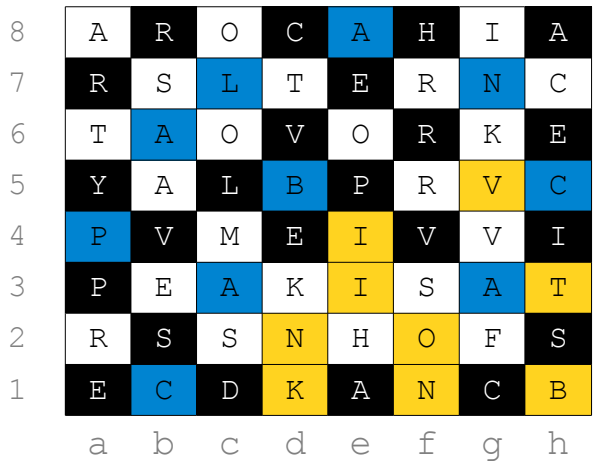
3

In the original version of the XMAS Puzzle 2010 the contents of the squares f5 and h6 are mixed up. Apologies for anyone who spend too much time because of this, although judging from the submissions it seemed not to have hindered most of you. In the text below the corrected chessboard is used.

If we start at the C at the square b1 (where at the start of a chess game a white knight resides) and use a chess knight to hup to consecutive letters we find we can make the name of the former chess world champion CAPABLANCA:



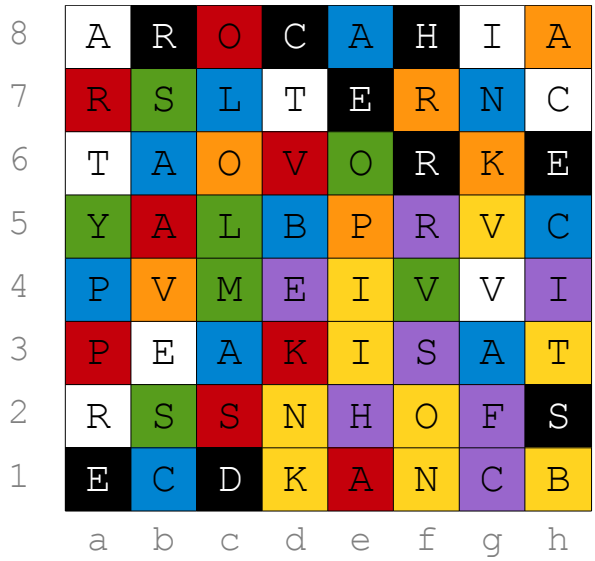
Continuing from the last letter A of CAPABLANCA a chess knight allows us to jump to the letters of the former chess world champion BOTVINNIK:



We find we can construct in this way the names of the

following six chess world champions (in chronological order):

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



The seventeen letters not used (that are on the chessboard above still in black or white squares) constitute the hint for the PLAYFAIR key used in the next exercise:

ARCHITECT REVERSED

4

From excercise 2 we have the hint ARCHITECT REVERSED to make a PLAYFAIR key. Here ARCHITECT refers to VITRUVIUS, the famous Roman architect. He extensively made use of the golden ratio in his work and the drawing by LEONARDO DA VINCI included in the introduction of this year's puzzle is based on the golden ratio and named after the architect: the VITRUVIUS man.

Fill the PLAYFAIR square with the keyword SUIVURTIV (VITRUVIUS, but then REVERSED):

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

The encrypted text is:

YFVBG OAWTG SVULV UUVXN TGMPU FPBBD HYDKB XEBPM HLMBD KMYKF SKVEM VPTSB TGBXT LSDKT

HSKS SHVZ UDXNK LDUA BXNKS UDX QPOF TVE DVLVV LNUE TMTL FDU SIVE TKTM

If we decrypt this we get:

WHICH NUMBER IS MISSING BELOW AND ACCORDING TO LEONARDO WHERE SHOULD IT BE INSERTED

EVER VERY RANGE PART ANGER RAW ZONE ASH CROSS OMIT SLAM EAR RUSH DEAL

All fourteen words have the property that a single letter can be prepended to form a new English word. There are numbers which have this property too: (N)ONE, (W)EIGHT. The question remains which one should be inserted where.

The idea is to prepend letters in such a way that the

prepended letters together form a sensible and appropriate word. It turns out that by prepending an N before ONE and inserting it between RANGE and PART one is able to form LEONARDO DA VINCI with the prepended letters:

(L)EVER (E)VERY (O)RANGE **(N)ONE** (A)PART (R)ANGER (D)RAW (O)ZONE (D)ASH (A)CROSS (V)OMIT (I)SLAM (N)EAR (C)RUSH (I)DEAL

Hence the number ONE should be inserted between RANGE and PART.

5

The text of the first part of the exercise is:

NMREZ ILMEI OGRIO EZINE LENNR NOILN LILER EONRN OINEL GZEZI RILIL INNZM RANEO EZERI ZILIO GONNE OINEZ GOGNN NELM

It might be difficult that no clues are given for the used cipher nor key. A little analysis is needed. Notice only 10 different letters appear in the text. This suggests information is encoded not is asingle letter, but perhaps in pairs of letters (bigrams). Breaking up the ciphertext in bigrams gives:

NM RE ZI LM EI OG RI OE ZI NE LE NN RN OI LN LI LE RE ON RN OI NE LG ZE ZI RI LI LI NN ZM RA NE OE ZE RI ZI LI OG ON NE OI NE ZG OG NN NE LM

Also notice that the first letter of each bigram is always from the set

N,R,Z,L,E,O

and the second letter is always from the set

M,I,E,G,N,A

Out of the 36 bigrams that can be formed in this way 21 actually occur. This all suggests each possible bigrams encodes a single letter (and perhaps also a digit).

Moreover the letters N,R,Z,L,E,O spell the word LORENZ and the letters M,I,A,E,G,N spell the word ENIGMA – two important German cryptodevices from the second world war.

The used system employs the following square:

	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

A letter or digit from the square is encoded by concatenating the head of the corresponding colomn and row. For example, the bigram EI encodes the letter P and NM encodes the number 2.

Decryption gives:

2 CRYPTOBREAKING MACHINES FROM MK3 6EB FORM THE NEXT KEY

The second encrypted part reads:

FCESE FN3WR RTNET 1NOHX TMTWI SEORS TETII EUH6H SOE0K TEEAC ENG1X CIWB8 OHQIH ICT

A frequency analysis indicates that a substituion cipher is unlikely and that rather a transposition cipher might be used. From the first part we know two keys are used. It makes sense to try and decrypt with these two keys and a double columnar transposition as educated guess for the used cipher.

MK3 6EB is postal code of BLETCHLEY PARK. Probably the two best known cryptanalytic machines from BLETCHLEY PARK are the BOMBE (on which part of the ENIGMA keyspace was exhausted) and the COLOSSUS (on which part of the LORENZ SZ 40/42 keyspace was exhausted).

To start the decryption we start with the word BOMBE and write the ciphertext in five colomns below the letters of

the word BOMBE. We do this by filling the colums below in the order of the alphabetical order of the letters in the word BOMBE. Since the ciphertext contains 68 = 13*5 + 3 letters, the columns below B,O and M will contain 14 letters and the columns below B and E will contain 13 letters.

This way the first 14 letters FCESEFN3WRRTNE appear below the first B. The next 13 letters T1NOHXTMTWISE appear below the next B and so on. This gives:

B	**O**	**M**	**B**	**E**
1	**5**	**4**	**2**	**3**
F	X	S	T	O
C	C	O	1	R
E	I	E	N	S
S	W	0	O	T
E	B	K	H	E
F	8	T	X	T
N	O	E	T	I
3	H	E	M	I
W	Q	A	T	E
R	I	C	W	U
R	H	E	I	H
T	I	N	S	6
N	C	G	E	H
E	T	1		

Next we read out the text rowwise:

FXSTO CCO1R EIENS SW0OT EBKHE F8TXT NOETI 3HEMI WQATE RICWU RHEIH TINS6 NCGEH ET1

Then we do the same with this text and the second keyword COLOSSUS. Since the text contains 68 = 8*8 + 4 letters the first four colomns will contain 9 letters, and the

rightmost four columns will contain 8 letters. The columns below the C will be filled with the first 9 letters FXSTOCCO1. The next 9 letters REIENSSW0 appear below the L. Continuing this way gives:

C	**O**	**L**	**O**	**S**	**S**	**U**	**S**
1	**3**	**2**	**4**	**5**	**6**	**8**	**7**
F	O	R	T	H	E	N	E
X	T	E	X	E	R	C	I
S	E	I	T	M	I	G	H
T	B	E	N	I	C	E	T
O	K	N	O	W	W	H	I
C	H	S	E	Q	U	E	N
C	E	S	T	A	R	T	S
O	F	W	I	T	H	1	6
1	8	0	3				

Again reading out this text rowwise reveals the plaintext:

FOR THE NEXT EXERCISE IT MIGHT BE NICE TO KNOW WHICH SEQUENCE STARTS OF WITH 161803

6

The hint of the previous exercise refers to a sequence that starts with 161803. The sequence meant is the decimal progression of the golden ratio:

1,61803398...

Note the golden ratio is a key theme in the drawing of VITRUVIUS man by LEONARDO DA VINCI which was included. The question is how to use this sequence.

Notice the letters in grey in the introduction of the XMas puzzle:

Woord	**letter(s)**
years	S
magic	M
rich	I
it	T
he	H
way	Y
unofficial	C
of	O
order	DE
an	N
to	O
decrypted	Y
For	R
decryption	N
prove	R
key	K
into	O
The	TH
consists	C

solution	L
look	K
Ultimately	M
provide	V
Kudos	K
parts	R
kindly	K
solving	G
drawn	W
cooperation	O
exercises	X
deadline	EAE
Solutions	N
clue	E
CrypTool	C

This gives as a hidden message:

SMITHY CODE NOYRN RKOTH CLKMV KRKGW OXEAE NEC

The SMITHY CODE was a cipher used by judge SMITH to encrypt a secret message hidden in his ruling in a case concerning plagiarism in THE DA VINCI CODE by DAN BROWN.

The hint from the first exercise TRUST YOUR JUDGEMENT TO FIND THE RIGHT CODE LATER ON was referring to the code from the judgement by judge SMITH.

The SMITHY CODE uses a VARIANT BEAUFORT cipher. When the key sequence is represented by integers, the decryption alphabet corresponding to integer n is the original alphabet ABCD...XYZ rotated to the left over (n-1) positions. In the original SMITHY code a key sequence of period 8 is derived from the FIBONACCI numbers. The first eight FIBONACCI numbers are:

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

Judge SMITH used the sequence:

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

Below are the eight corresponding decryption alphabets:

	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
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
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

For example, the letter F gets decrypted to a J if the key is the number 5. Decrypting the message

NOYRN RKOTH CLKMV KRKGW OXEAE NEC

this way gives:

```
C:  N  O  Y  R  N  R  K  O  T  H  C  L  K  M  V  K  R  K
K:  1  1 25  3  5  8 13 21  1  1 25  3  5  8 13 21  1  1
```

```
P:  N  O  W  T  R  Y  W  I  T  H  A  N  O  T  H  E  R  K

C:  G  W  O  X  E  A  E  N  E  C
K: 25  3  5  8 13 21  1  1 25  3
```

```
P:  E  Y  S  E  Q  U  E  N  C  E
```

Or:

NOW TRY WITH ANOTHER KEY SEQUENCE

The idea is now to use this VARIANT BEAUFORT with as key sequence the decimal progression of the golden ratio.

The decimal progression of the golden ratio starts with:
1,6180339887498948482045868343656381177203091798057628621354486 22..

First we construct the ten decryption alphabets corresponding with the ten possible key digits 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

Decrypting the text from the exercise now gives:

C: PGARX GRZTR IRFZK MTKBR IIWWT TLARC AVLLW ELNNF TFJYN
K: 16180 33988 74989 48482 04586 83436 56381 17720 30917

P: PLAYW ITHAY OUNGS PANIS HLADY ANDTH EANSW ERTOE VERYT

C: ZBOCI IZVCD CIAOY HVQC
K: 98057 62862 13544 8622

P: HINGO NACHE CKERB OARD

Or:

PLAY WITH A YOUNG SPANISH LADY AND THE ANSWER TO EVERYTHING ON A CHECKERBOARD

7

The hint CHECKERBOARD refers to the (STRADDLE) CHECKERBOARD system. For (a very basic variant of) this system a word of eight different letters is needed together with two digits below 10. The eight letter word is given: YOUNG SPANISH LADY or SENORITA.

The ANSWER TO EVERYTHING refers to THE HITCHIKERS GUIDE TO THE GALAXY, in which THE ANSWER TO THE ULTIMATE QUESTION IN LIFE, THE GALAXY, EVERYTHING is given: 42. We can thus fill the checkerboard:

	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	-	-

The text from the exercise breaks up as

```
 8 45  1  0 26  0  8  1 49  7  0  0  7 41  7 48  7  9  3
 9  3 42  8 45  1 20 48  9  7  3  8  1 25  8 41  5  3  8
 9  7  3  0  8 45  1  8  1  6 49 20  6  7 49  1  3 22 49
40  1  6
```

which decrypts as

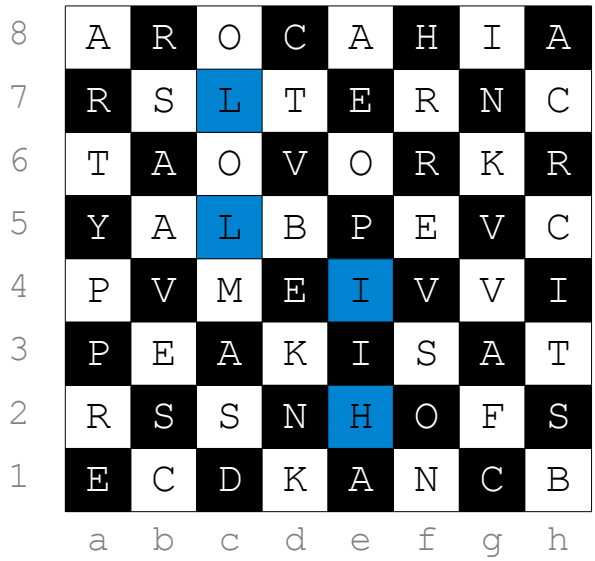
```
 T  H  E  S  Y  S  T  E  M  I  S  S  I  C  I  L  I  A  N
 A  N  D  T  H  E  P  L  A  I  N  T  E  X  T  C  O  N  T
 A  I  N  S  T  H  E  T  E  R  M  P  R  I  M  E  N  U  M
 B  E  R
```

or:

THE SYSTEM IS SICILIAN AND THE PLAINTEXT CONTAINS THE TERM PRIME NUMBER

8

The system used is (by the hint from the previous exercise) SICILIAN. This refers to the sicilian chess opening, which starts off with the moves e2-e4 and c7-c5. If we highlight the four squares e2,e4,c7,c5 on the chessboard from exercise 3, we see the letters in these squares spell out HILL – the used system here is the HILL cipher.



Since the numbers of letters 78 = 2*3*13 the dimensions of the matrix are not clear yet but it seems likeley either a 2-by-2 or a 3-by-3 matrix has been used. Testing for a 2-by-2 matrix is helped by the knowledge that PRIME NUMBER is part of the plain text (hint from the previous exercise). There is no 2-by-2 matrix which will decrypt with PRIME NUMBER being part of the plain text (CryptTool for instance can test this automatically for you).

Now we try to recover a 3-by-3 matrix. We will have to guess where the encryption of PRIME NUMBER starts, recover the decryption matrix and decrypt the remainder of the text to see if the decrypted text makes sense. As it turns out, the encryption of PRIME NUMBER starts at position 35.

Dividing the text in trigrams gives (with the encryption

of PRIME NUMBER in bold) gives:

XBF TOE OTF ZFF FOU SPI LON GJP UTA UZZ BAH B**KI MKK**
EZO QAB KRY PQA JMC HPT LON MQC YYO XAV KFD DXL AZD

Hence the 3-by-3 decryption matrix we want decrypts the nine letters MKK EZO QAB into IME NUM BER.

Denote the decryption matrix by

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

using the encoding A=0, B=1, .., Z=25 we are looking for nine integers a,b,c,d,e,f,g,h,i such that:

$$\begin{aligned} a*12 + b*10 + c*10 &= 8 \pmod{26} \\ d*12 + e*10 + f*10 &= 12 \pmod{26} \\ g*12 + h*10 + i*10 &= 4 \pmod{26} \end{aligned}$$

(MKK = 12,10,10 should decrypt to IME = 8,12,4)

and:

$$\begin{aligned} a*4 + b*25 + c*14 &= 13 \pmod{26} \\ d*4 + e*25 + f*14 &= 20 \pmod{26} \\ g*4 + h*25 + i*14 &= 12 \pmod{26} \end{aligned}$$

(EZO = 4,25,14 should decrypt to NUM = 13,20,12)

and:

$$\begin{aligned} a*16 + b*0 + c*1 &= 1 \pmod{26} \\ d*16 + e*0 + f*1 &= 4 \pmod{26} \\ g*16 + h*0 + i*1 &= 17 \pmod{26} \end{aligned}$$

(QAB = 16,0,1 should decrypt to BER = 1,4,17).

This linear system has a solution that is given (modulo 26) by:

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

By no concidence the integers a,b,..,i are the first nine integers (but reversed as was VITRIVIUS when used as PLAYFAIR key in exercise 3) in the decimal representation of the golden ratio.

Now the other trigrams can be decrypted. For example, XBF = 23,1,5 decrypts as

```
8*23 + 9*1 + 3*5 = 208 =  0 (modulo 26)
3*23 + 0*1 + 8*5 = 109 =  5 (modulo 26)
1*23 + 6*1 + 1*5 =  34 =  8 (modulo 26)
```

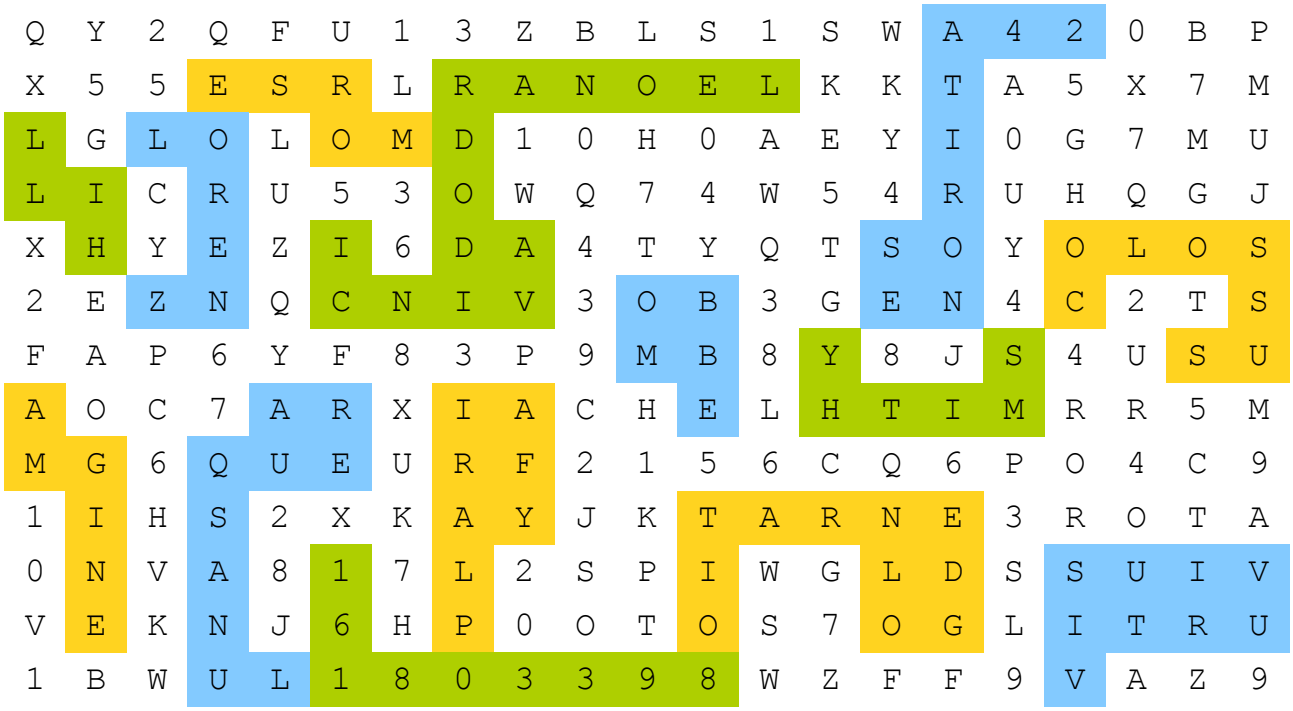
and so XBF decrypts to AFI. Continuing this way gives:

A FIELD MEDALIST FROM THE SIXTIES AND HIS PRIME NUMBER TOGETHER FORM THE MAGIC AND SECRET WAY(X)

The FIELD MEDALIST that is referred to is GROTHEDIECK (awarded the medal in 1966). A legendary anecdote has GROTHENDIECK give 57 = 3*19 as an example of a prime number. SInce then, 57 is known as the GROTHENDIECK prime.

9

In the rectangle we can actually discover many words that have played an important role in this years puzzle:



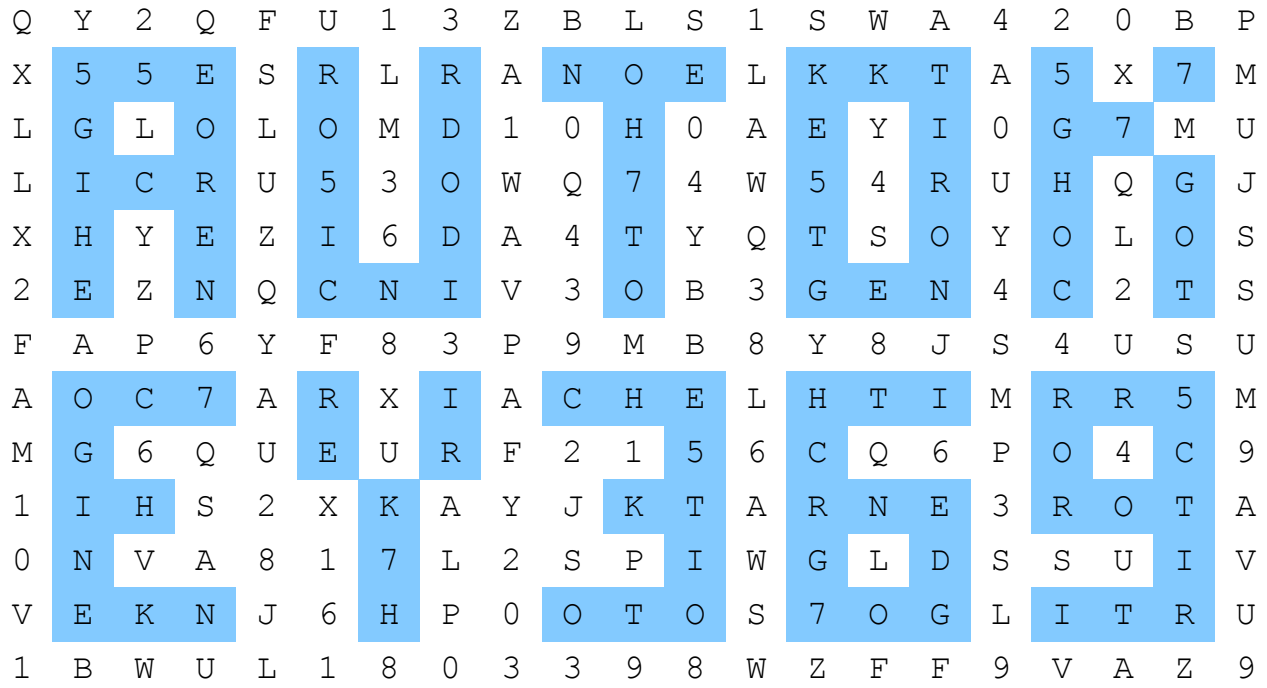
The hidden words are:

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

This observation may not lead directly to the solution but suggests maybe the solution can be found in a similar way.

The hint THE MAGIC AND SECRET WAY refers to part of the LUNA SQUARE songtext from the start of the Xmas puzzle: HE KNOWS THE MAGIC THAT MAKES IMAGES.. AND HE'S THE ONE WHO KNOWS THE SECRET WAY. It suggests that GROTHENDIECK and 57 together can make images.

Indeed if we colour the letters and numbers from GROTHENDIECK and 57 we immediately see the hidden message:



The recovered message is AUTOKEY 369.

The last part of this year's puzzle is encrypted in the VIGENERE TEST AUTOKEY system, in which the VIGENERE key is extended with the plaintext. The hint 369 hints at the key used in the system: as recovered from exercise 1 the number 369 represents the 'spirit of the moon': HASMODAI. Decrypting with HASMODAI as key now gives the final riddle to solve:

WHICH COUNTRY IS MISSING FROM THIS LIST RUSSIA SYRIA GERMANY ECUADOR HUNGARY GABON LESOTHO SIERRA LEONE SLOVENIA SERBIA

The solution to this riddle lies in the national flags of these countries: all flags consist of three horizantal stripes. The order in which these countries are listed is such that the lower clour in the flag of a counrty matches the upper colour in the flag of the next country on the list. If we list the countries in this way we see a gap between SIERRA LEONE and SLOVENIA:

Country	Flag
RUSSIA	
SYRIA	
GERMANY	
ECUADOR	
HUNGARY	
GABON	
LESOTHO	
SIERRA LEONE	
?	?
SLOVENIA	
SERBIA	

There is one country whose natinal flag consists of three horizontal stripe with the upper colour blue and the lower colour white: ESTONIA, with the following flag:

The complete solution of the NLNCSA XMas Puzzle 2010 is thus:

First part
ONE, which should be inserted between RANGE and PART.

Second part
ESTONIA