MysteryTwister C3
A CRYPTO CHALLENGE BY CRYPTOOL

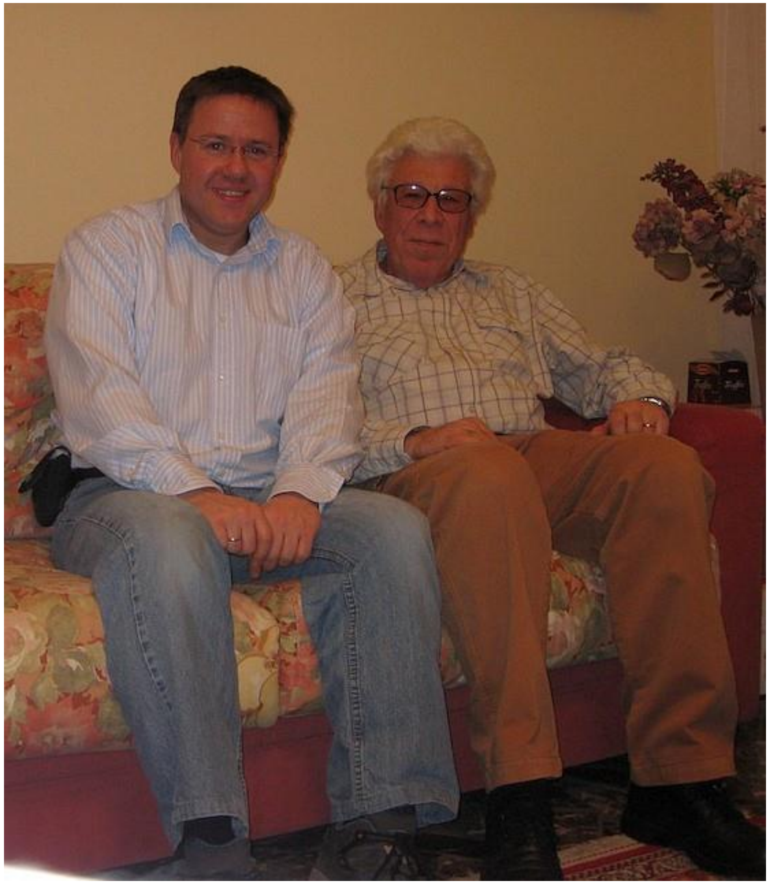
NOTES OF AN ITALIAN SOLDIER 1944-1945

Secret notes kept by an Italian Professor

Tobias Schrödel

In the beginning of October 2009, I visited my friend Prof. Filippo Sinagra in Venice, Italy. We happen to have the same hobby: collecting books and machines related to cryptology.

Filippo has a wonderful collection, including tons of books and crypto machines, such as the Swiss NEMA, some Hagelin machines, and various special parts like the rotors of a Russian Fialka.



His goal is to keep historic documents and inventions available to the future. He is author of “Dalla Scitala all’Enigma etc. etc…”, a wonderful composite of 2,300 pages filled with descriptions and documents related to cryptology.

After sharing our recent acquisitions, taking pictures of every new item, and eating a wonderful dinner cooked by his wife Gianna, Filippo presented me a set of old photocopies.

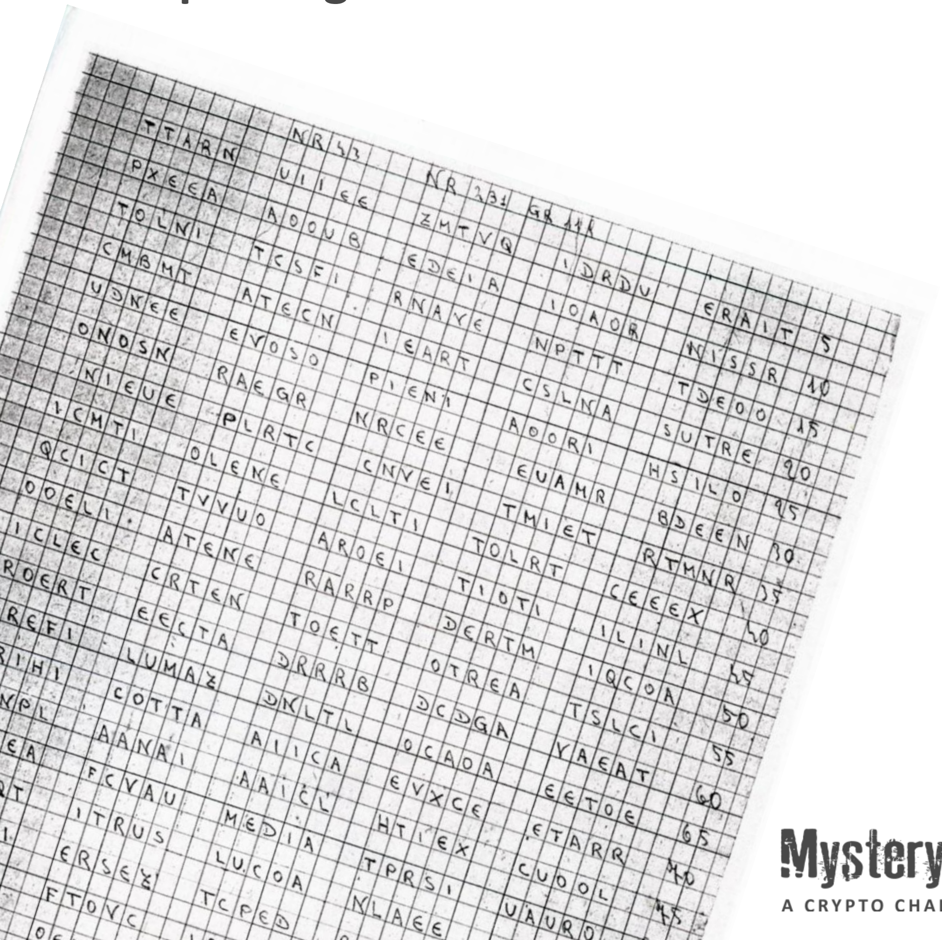
The pages are full of handwritten, uppercase letters in groups of five.

They were written between 1944 and 1945, when Italy was divided into two parts. The northern part was occupied by the German Nazis and Mussolini’s fascists, while in the south Italian partisans fought together with the Allied forces.

One of the partisans was Antonio Marzi. He was recruited by the Regia Marina in 1944. Marzi was trained in using the radio, so he was employed as a “radiotelegrafista”. As his work was quite important, Marzi was soon parachuted into action in Udine.

During his work, he made notes about the military operations, his observations, and his feelings and fears during the days and nights in combat.

Anticipating the possibility of becoming a prisoner of war, Marzi enciphered his notes. Although not a cryptograph, he was clever enough to find a secure enciphering method that could be used with just pencil and paper.



```
        NR 43   NR 231 GR 118
TTARN   UIIEE   ZMTVQ   IDRDU   ERAIT   5
PXEEA   AOOUB   EDEIA   IOAOR   NISSR   10
TOLNI   TCSFI   RNAYE   NPTTT   TDEOO   15
CMBMT   ATECN   IEART   CSLNA   SUTRE   20
UDNEE   EVOSO   PIENI   AOORI   HSILO   25
ONOSN   RAEGR   NRCEE   EUAMR   BDEEN   30
NIEUE   PLRTC   CNVEI   TMIET   RTMNR   35
ICMTI   OLENE   LCLTI   TOLRT   CEEEX   40
QCICT   TVVUO   AROEI   TIOTI   ILINL   45
OOELI   ATENE   RARRP   DERTM   IQCOA   50
ICLEC   CRTEN   TOETT   OTREA   TSLCI   55
ROERT   EECTA   DRRRB   DCDGA   YAEAT   60
REFI    LUMAZ   DNLTL   OCAOA   EETOE   65
RIHI    COTTA   AIICA   EVXCE   ETARR   70
NPL     AANAI   AAICL   HTIEX   CUOOL   75
EA      FCVAU   MEDIA   TPRSI   UAURO
RT      ITRUS   LUCOA   NLAEE
I       ERSEZ   TCPED
        FTOVC
```

Antonio Marzi used a double columnar transposition and – in addition – added some K, X, Y, J and W's to confuse possible cryptanalysts.

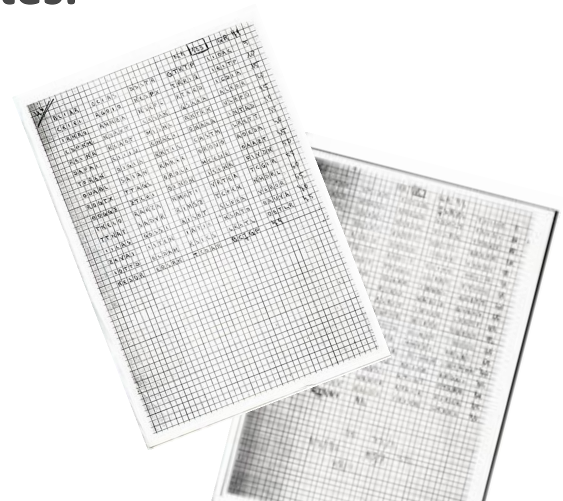
The columnar transposition was probably performed by using the alphabetical order of the letters of one to three codewords that came from an Italian poem.

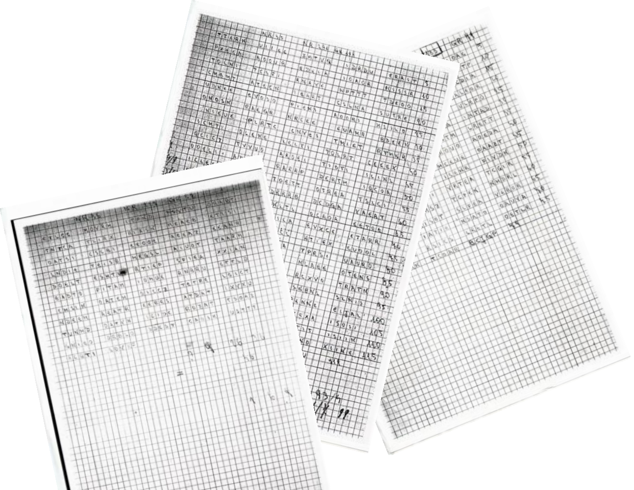
Almost 60 years later, Marzi wrote a letter to Prof. Sinagra and asked for assistance, as he was not able to decipher his own papers.

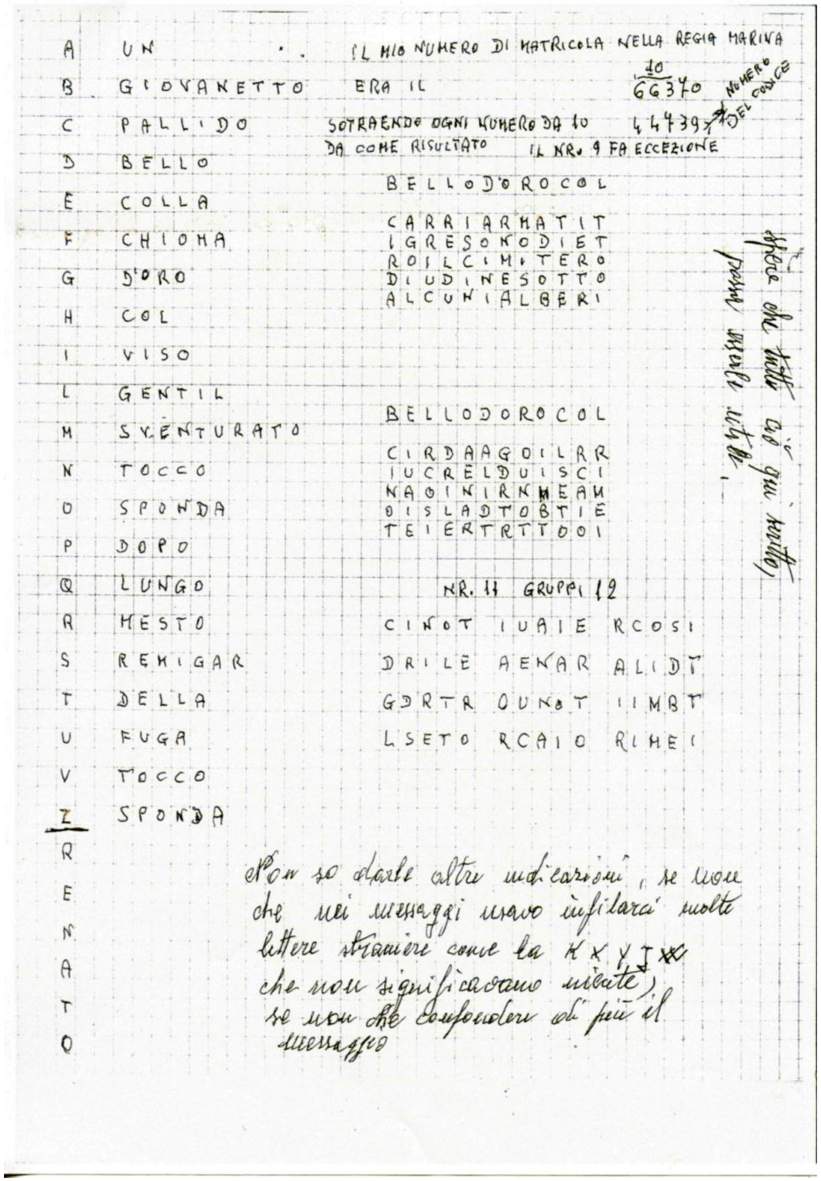
Sinagra visited him in Rome in 2003 and was able to gather some important information regarding the encryption. He learned how the codeword was defined, as well as how the double transposition was performed.

Reversing the transposition should have revealed a text in Italian, but it did not. Marzi’s memory must have been wrong in at least one of the cipher steps or he mixed up the sequence.

Antonio Marzi died in 2007 at the age of over 80 years. He never read his own notes.







A	UN	. . IL MIO NUMERO DI MATRICOLA NELLA REGIA MARINA
B	GIOVANETTO	ERA IL 10 66370 NUMERO DEL CODICE
C	PALLIDO	SOTRAENDO OGNI NUMERO DA 10 44739
		DA COME RISULTATO IL NR. 9 FA ECCEZIONE
D	BELLO	
E	COLLA	
F	CHIOMA	
G	D'ORO	
H	COL	
I	VISO	
L	GENTIL	
M	SVENTURATO	
N	TOCCO	
O	SPONDA	
P	DOPO	
Q	LUNGO	
R	MESTO	
S	REMIGAR	
T	DELLA	
U	FUGA	
V	TOCCO	
Z	SPONDA	

BELLOD'OROCOL

```
CARRIARMATIT
IGRESOKODIET
ROILCIMITERO
DIUDINESOTTO
ALCUNIALBERI
```

BELLODOROCOL

```
CIRDAAGOILRR
IUCRELDUISCI
NAOINIRNMEAM
OISLADTOBTIE
TEIERTRTTOOI
```

NR. 11 GRUPPI 12

```
CINOT IUAIE RCOSI
DRILE AENAR ALIDT
GDRTR OUNOT IIMBT
LSETO RCAIO RIMEI
```

R
E
N
A
T
O

Spero che tutto ciò qui scritto,
possa essere utile,

Non so darle altre indicazioni, se non
che nei messaggi usavo infilarci molte
lettere straniere come la K X Y J W
che non significavano niente),
se non che confondere di più il
messaggio

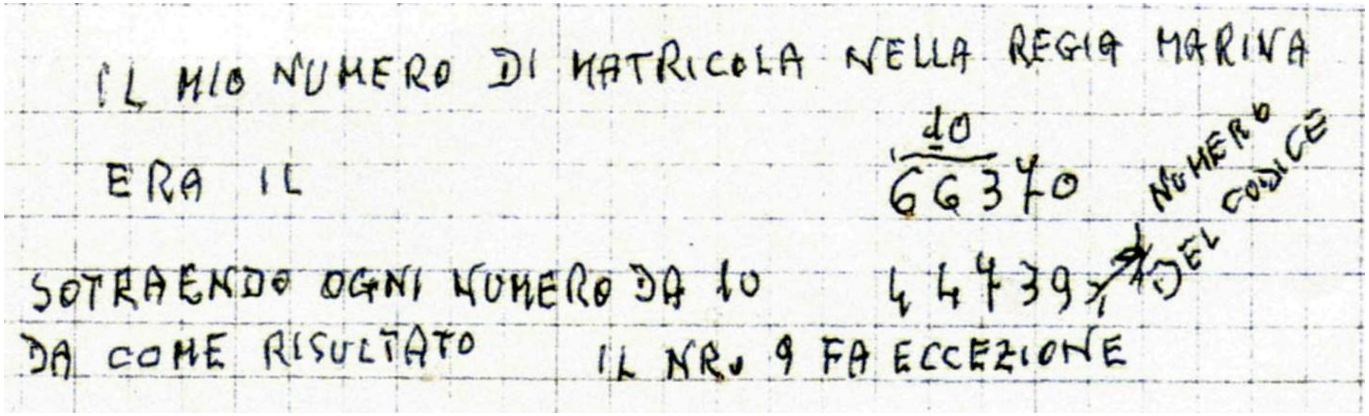
Thanks to Filippo Sinagra, over 230 pages with encrypted information about WWII and the Italian resistance are still available to posterity.

With the information he saved, it should be possible to decipher some or all of the sheets.

On the left is the most important document. Marzi wrote down the poem for the codewords, a sample encipherment and also some other information.

The matricalulation number of Marzi at the Regia Marina, 66370, has something to do with the code.

Subtracting every single number from 10 (where the zero is an exception as it becomes nine) derives the code number 44739.



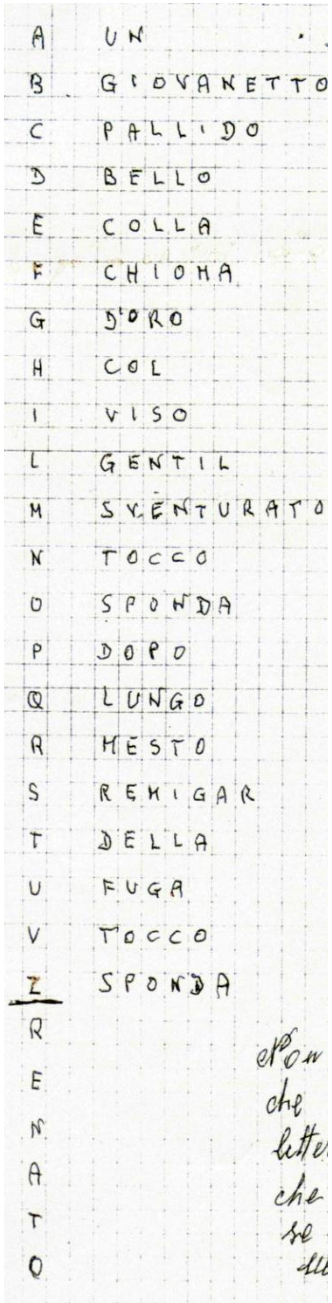
IL MIO NUMERO DI MATRICOLA NELLA REGIA MARINA

ERA IL 10
66370

NUMERO DEL CODICE

SOTRAENDO OGNI NUMERO DA 10 44739

DA COME RISULTATO IL NR. 9 FA ECCEZIONE



A	UN
B	GIOVANETTO
C	PALLIDO
D	BELLO
E	COLLA
F	CHIOMA
G	D'ORO
H	COL
I	VISO
L	GENTIL
M	SVENTURATO
N	TOCCO
O	SPONDA
P	DOPO
Q	LUNGO
R	MESTO
S	REMIGAR
T	DELLA
U	FUGA
V	TOCCO
Z	SPONDA
R	
E	
N	
A	
T	
O	

Non
che
lette
che
se
su

This is the poem, which is about a beautiful young man.

Marzi uses the words BELLO, D‘ORO and COL for the following example. These are the fourth, seventh and eighth words from the list.

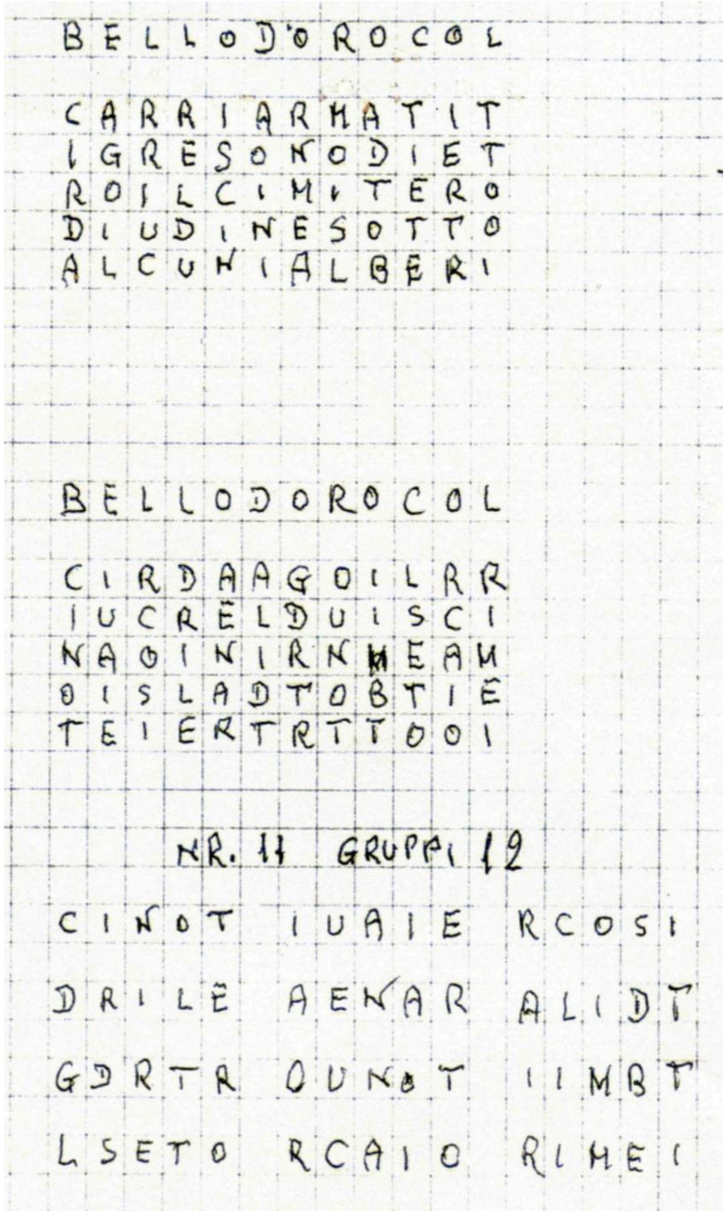
The sequence could somehow be derived from the code number that was previously calculated. More details are not known.

This is probably the most helpful part of the notes.

In both steps, Marzi transfers the columns to rows.

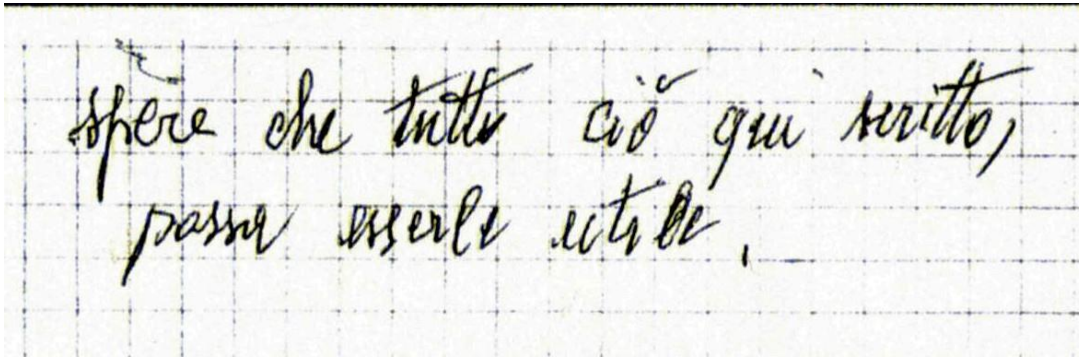
What is missing is a sort order after one or both of the transposition steps.

Historically this would be done by sorting the codeword and the respective columns alphabetically.

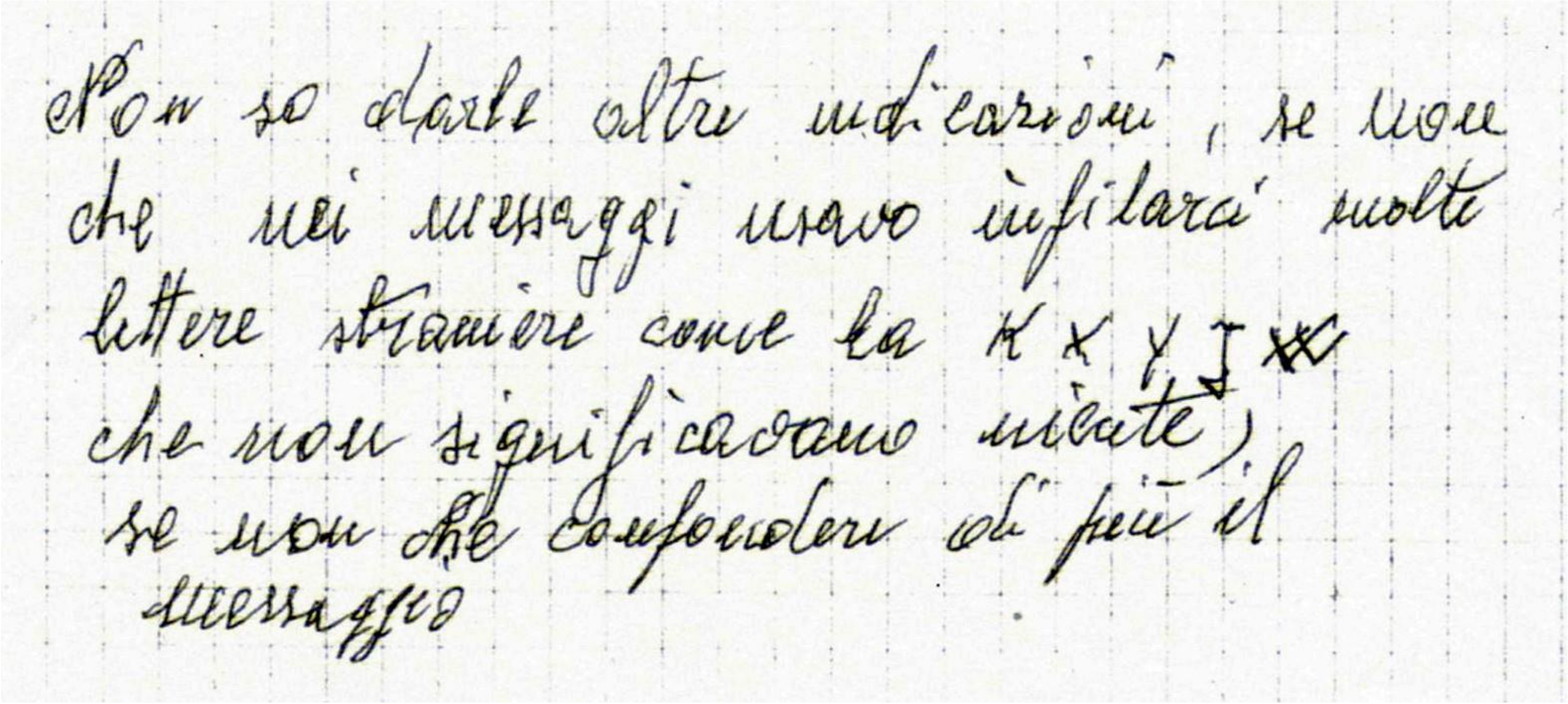


```
B E L L O D'O R O C O L

C A R R I A R H A T I T
I G R E S O N O D I E T
R O I L C I M I T E R O
D I U D I N E S O T T O
A L C U N I A L B E R I


B E L L O D O R O C O L

C I R D A A G O I L R R
I U C R E L D U I S C I
N A O I N I R N M E A U
O I S L A D T O B T I E
T E I E R T R T T O O I

      NR. 11   GRUPPI 12

C I N O T   I U A I E   R C O S I

D R I L E   A E N A R   A L I D T

G D R T R   O U N O T   I I M B T

L S E T O   R C A I O   R I H E I
```

Some additional notes:



Spero che tutto ciò qui scritto,
possa esserle utile.



Non so darle altre indicazioni, se non
che nei messaggi usavo infilarci molte
lettere straniere come la K X Y J W
che non significavano niente,
se non che confondere di più il
messaggio

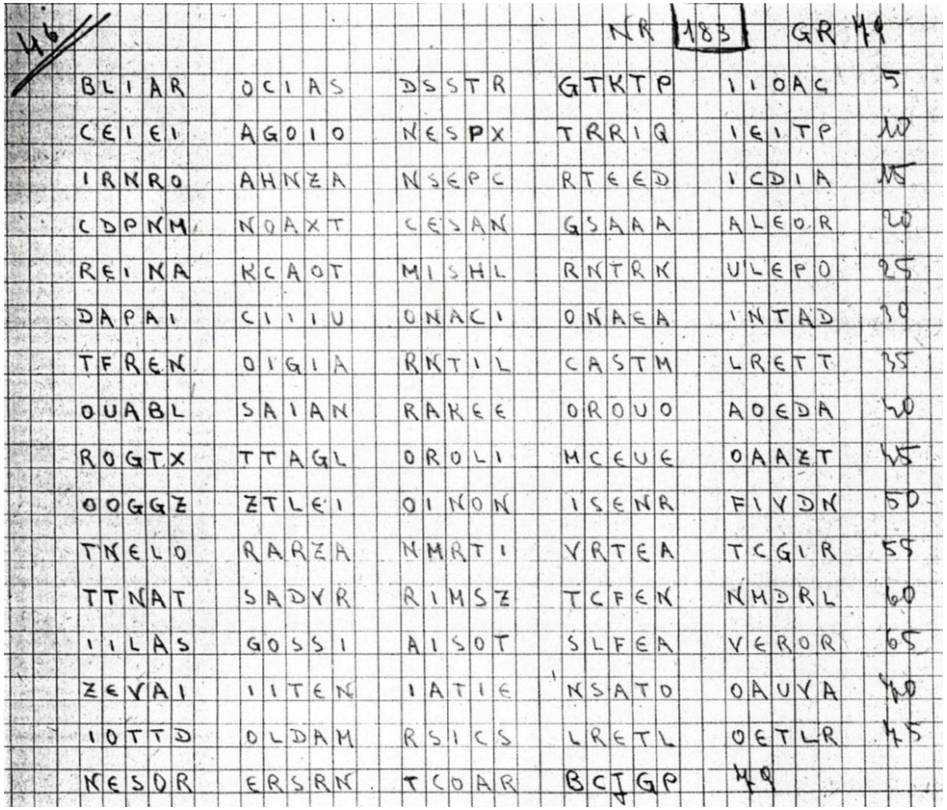
The goal of this challenge is to find out the technique that Marzi used to encrypt his messages and thus to propose a comprehensible method to decipher at least one of his messages.

Attached are three sample messages; more are available by request.

Sample #1

In case you need more example pages or you find the solution, please contact Tobias Schrödel from the Mystery Twister Team.
schroedel@sichere.it

If you have additional questions about Marzi and the meeting in Rome, please contact Professor Filippo Sinagra directly.
cryptosite@yahoo.it

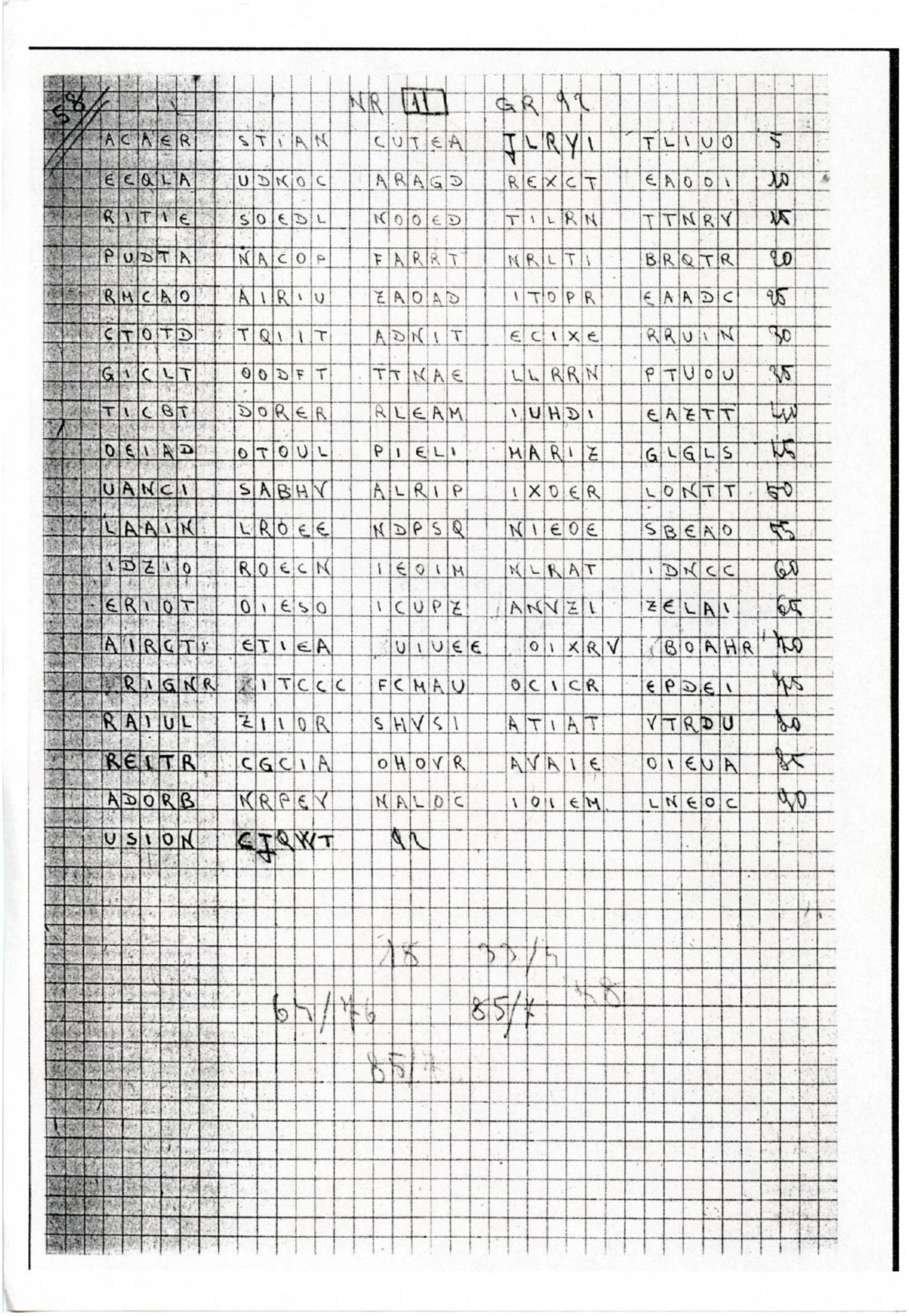


46 NR 183 GR 49

BLIAR	OCIAS	DSSTR	GTKTP	IIOAC	5
CEIEI	AGOIO	NESPX	TRRIQ	IEITP	10
IRNRO	AHNZA	NSEPC	RTEED	ICDIA	15
CDPNM	NOAXT	CESAN	GSAAA	ALEOR	20
REINA	KCAOT	MISHL	RNTRK	ULEPO	25
DAPAI	CIIIU	ONACI	ONAEA	INTAD	30
TFREN	OIGIA	RNTIL	CASTM	LRETT	35
OUABL	SAIAN	RAKEE	OROUO	AOEDA	40
ROGTX	TTAGL	OROLI	MCEUE	OAAZT	45
OOGGZ	ZTLEI	OINON	ISENR	FIYDN	50
TNELO	RARZA	NMRTI	YRTEA	TCGIR	55
TTNAT	SADYR	RIMSZ	TCFEN	NMDRL	60
IILAS	GOSSI	AISOT	SLFEA	VEROR	65
ZEVAI	IITEN	IATIE	NSATO	OAUYA	70
IOTTD	OLDAM	RSICS	LRETL	OETLR	75
NESDR	ERSRN	TCOAR	BCJGP	49	

MysteryTwister C3
A CRYPTO CHALLENGE BY CRYPTOOL

Sample #2



58

NR 41 GR 92

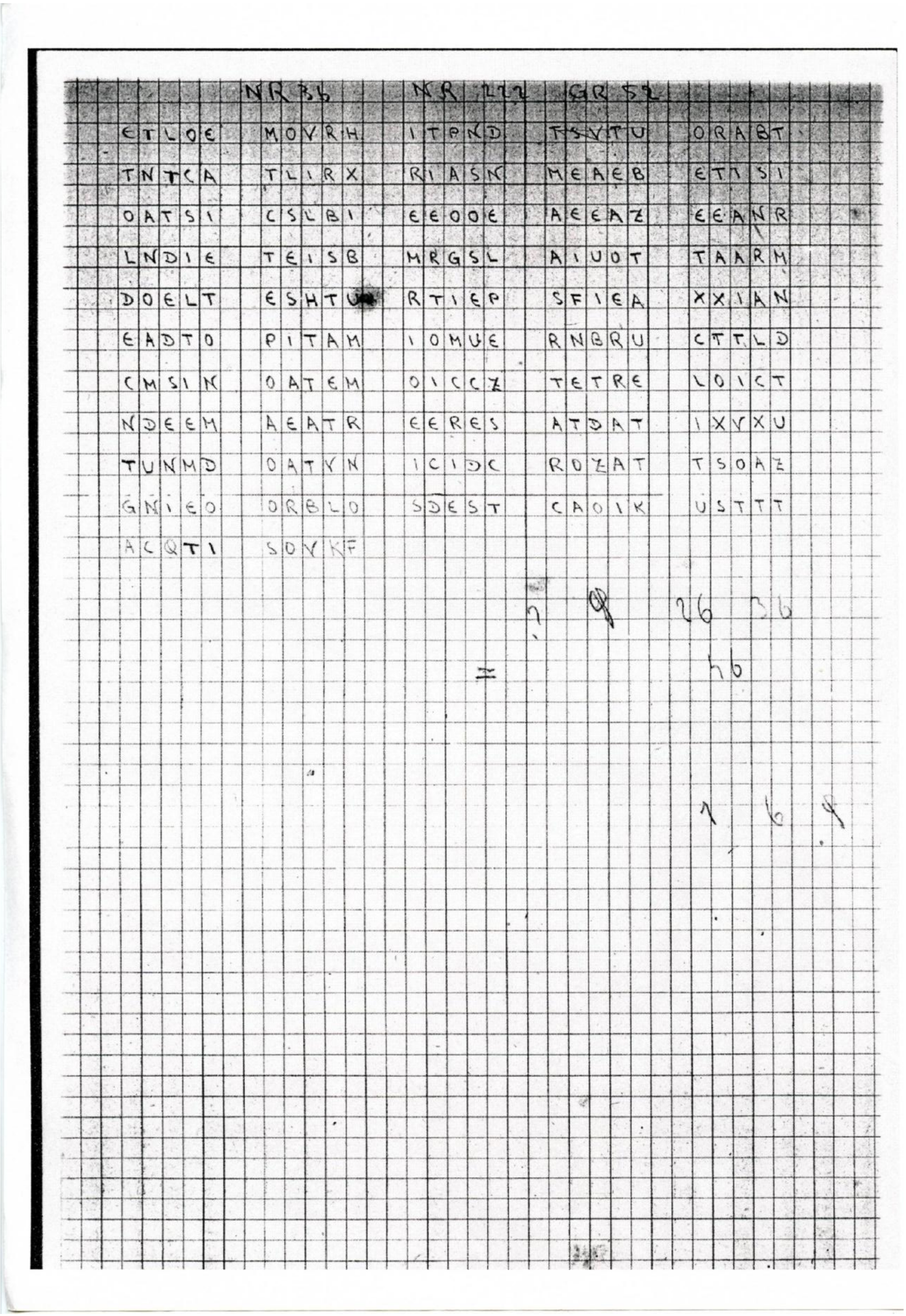
ACAER	STIAN	CUTEA	JLRYI	TLIUO	5
EEQLA	UDKOC	ARAGD	REXCT	EAOOI	10
RITIE	SOEDL	KOOED	TILRN	TTNRY	15
PUDTA	NACOP	FARRT	NRLTI	BRQTR	20
RMCAO	AIRIU	ZAOAD	ITOPR	EAADC	25
CTOTD	TQIIT	ADKIT	ECIXE	RRUIN	30
GICLT	OODFT	TTKAE	LLRRN	PTUOU	35
TICBT	DORER	RLEAM	IUHDI	EAZTT	40
OEIAD	OTOUL	PIELI	MARIZ	GLGLS	45
UANCI	SABHY	ALRIP	IXOER	LONTT	50
LAAIN	LROEE	NDPSQ	NIEOE	SBEAO	55
IDZIO	ROECN	IEOIM	NLRAT	IDNCC	60
ERIOT	OIESO	ICUPZ	ANVZI	ZELAI	65
AIRGT	ETIEA	UIUEE	OIXRV	BOAHR	70
RIGNR	KITCCC	FCMAU	OCICR	EPDEI	75
RAIUL	ZIIOR	SHVSI	ATIAT	VTRDU	80
REITR	CGCIA	OHOVR	AVAIE	OIEUA	85
ADORB	KRPEY	NALOC	IOIEM	LNEOC	90
USION	CJQWT	92			

18 33/5

65/46 85/7 48

85/7

Sample #3



```
         NR 36     NR 222     GR 52
ETLOE    MOVRH     ITPND      TSVTU     ORABT
TNTCA    TLIRX     RIASN      MEAEB     ETTSI
OATSI    CSLBI     EEOOE      AEEAZ     EEANR
LNDIE    TEISB     MRGSL      AIUOT     TAARM
DOELT    ESHTU     RTIEP      SFIEA     XXIAN
EADTO    PITAM     IOMUE      RNBRU     CTTLD
CMSIN    OATEM     OICCZ      TETRE     LOICT
NDEEM    AEATR     EERES      ATDAT     IXVXU
TUNMD    OATYN     ICIDC      ROZAT     TSOAZ
GNIEO    ORBLO     SDEST      CAOIK     USTTT
ACQTI    SOVKF
```

7 8 26 36

46

=

7 6 8

MysteryTwister C3

A CRYPTO CHALLENGE BY CRYPTOOL