New Findings in a WWI Notebook of Luigi Sacco

Paolo Bonavoglia
former teacher of Mathematics
Convitto Nazionale Marco Foscarini,
Cannaregio 4942, I 30121 Venezia, Italy
paolo.bonavoglia@liceofoscarini.it

Abstract

A small size booklet was found by the author among the papers of Luigi Sacco, his grandfather, founder and chief of the Italian Army cryptographic office (a.k.a. *Reparto crittografico*) during WW1. This paper presents a new research, still work in progress, about new cryptograms found in the booklet containing historical links to events of WW1.

1 The booklet

The booklet has 160 pages, mostly handwritten, some left blank. The cover has the date 18 July 1916, the last pages are dated November 1916. Therefore, the book covers the very beginning of the Italian cryptographic office in WW1.

The first part looks like an exercise book with examples and explanations. The following pages have a mix of German language cryptograms, mainly transposition ciphers.

A paper about this booklet has been already published on-line by the author (Bonavoglia 2018). Recent research has produced more interesting results.

2 Are these real WW1 cryptograms?

This is the first question arising from this booklet. Are all these cryptograms real war messages? Or are only examples, exercises?

Examining the pages, the most likely hypothesis is there both are true. A first good criterion is language; several cryptograms at the beginning are in French; since France was an ally of Italy, it looks very likely these are mere exercises. And the text states clearly these are examples taken from Valerio (the French treatise of cryptography which Sacco used extensively).

And most other messages are in German and this is a first clue in favor of the hypothesis that these cryptograms are real WW1 messages. Most cryptograms have names of persons or places of the war on the eastern front, mainly on the Rumanian theatre, which is consistent, both in space and time, with the conjecture that these German messages were intercepted by Sacco's radio stations in the Italian Friuli region, not so far from the Danube region. They could also come from other Italian intercepting stations, a good candidate is for instance the one in Lecce, not far from the Danube region.

3 A transposition cryptogram

A particularly interesting transposition cipher appears in the following couple of pages[1] :

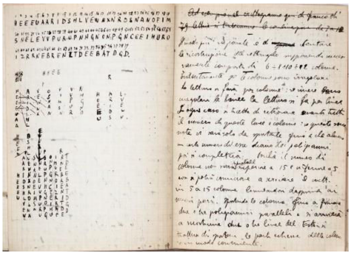
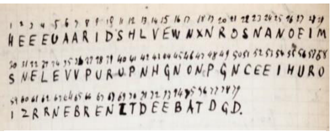


Figure 1 : The couple of pages.



```
HEEEUAARIDSHLVEWNXNRDSNANOFIM
SNELEVVPURUPNHGNONPGNCEEIHURO
IZRRNEBRENZTDEEBATDGD.
```

Figure 2 : The cryptogram of 79 letters on top of the left page.

[1] Only a few pages have a date; these are between a page dated 24-09-1916 and one dated 11-10-1916; this should be a good clue about the date.

In the right page Sacco writes down a possible strategy to decrypt it: he tries to arrange the text in 6 8 10 12 columns rectangles in the hypothesis of an irregular rectangle. No solution is given.

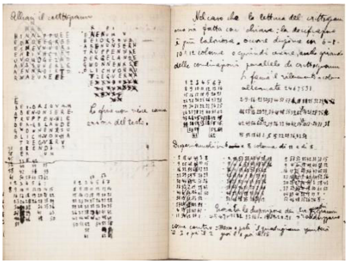


Figure 3 : The second couple of pages.

Two pages forward we find another couple of pages with a slightly different cryptogram, a few letters changed with similar letters, e.g. *L* → *V, H* → *E, N* →*W*. It's likely Sacco found some transcription errors from the original.

Finally, Sacco finds a solution which has strange errors in the last lines.

The decrypted text is:

```
BEI ORSOVA HABEN UNSERE TRUPPEN
WIEDER GELANDE GWONNEN X
SUDLICH VON HATZEG VERVEREN DIE
RUME
```

Taking the X as a separator, and GWONNEN for GEWONNEN we have a text sounding good in German, except for the last line:

Bei Orsova haben unsere Truppen wieder Gelande gewonnen. Sudlich von Hatzeg ververen die Rume.

But *Ververen die Rume* has no meaning in German, and Sacco writes near this solution: "The end does not work for errors in the text". Quite puzzled by these strange final errors I supposed there was some mistake in the cryptogram, maybe a handwriting problem, and made a few attempts; I restored the D present in the first cryptogram and for some reason removed from the second and changed it in O. So we have this 80 letters cryptogram:

```
HEEEU AARID SHLVE WNXNR OSNAN
OEIMS NELEV VDURU PENHG NONPG
NCEEI EUROI ZRRNE BREWL TOEEB
ATDGD
```

The decrypted text is:

Bei Orsova haben unsere Truppen wieder Gelände gewonnen. Sudlich von Hatzeg verloren die Rumen.[2]

and at last the final words make sense!

This text is interesting because of the geographic names: Orsova and Hatzeg are Rumanian cities by the Danube; and in September 1916 the German Army under General Falkenhayn launched a counter offensive between Orsova and Hatzeg against the Rumanian Army to regain the ground lost in August and early September when Romania declared war to Austria-Hungary and occupied regions near Transylvania.

This gives a good accordance of times between these cryptograms of Sacco's notebook, and historical events of WW1. Another clue in favor of the idea that these cryptograms are real WW1 encrypted messages which Sacco decrypted and used to find a method for decrypting transposition ciphers.

4 Solved transposition cryptograms

These two pages[3] of the booklet have a lot of decrypted transposition cryptograms of various kinds.

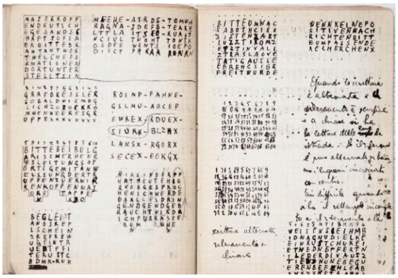


Figure 4 : A few have the original cryptogram, many only the final solved rectangle.

Here is the first, top left, a simple transposition cipher with alternate up and down writing; the original cryptogram is also shown on the right.

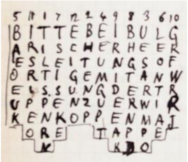
The decrypted text is:

[2] English: At Orsova our troops have gained ground again. South of Hatzeg lost the Rumanians

[3] These pages are between a page dated 11-10-1916 and one dated 17-10-1916.

Major Koppen deutsche Gesandtschaft Sofia erbitte Draht Antwort welche Formationen dort unterstellts in[4]

Another cryptogram is an irregular rectangle key transposition, much more difficult to break.



```
5 11 1 7 12 2 4 9 8 3 6 10
B I T T E B E I B U L G
A R I S C H E R H E E R
E S L E I T U N G S O F
O R T I G E M I T A N W
E I S S U N G D E R T R
U P P E N Z U E R W I R
K E N K O P P E N M A J
  O R E     T A P P E
    K         K D O
```

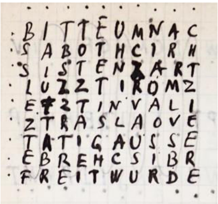
Figure 5 : The original cryptogram is missing, but of course it can easily be reconstructed.

The decrypted text is:

Bitte bei Bulgarischer Heeresleitung sofortige mit Anweisung der Truppen su erwirken Koppen Major Etappen Kdo[5]

Who was this Major Koppen, named twice here? I could find an answer only in the German Wikipedia[6]; he was a chief of staff at the High Command of the German Army.

A third cryptogram is shown hereafter.



```
B I T T E U M N A C
S A B O T H C I R H
S I S T E N Z A R T
L U Z Z T I R O M Z
E T Z T I N V A L I
Z T R A S L A O V E
T A T I G A U S S E
E B R E H C S I B R
F R E I T W U R D E
```

Figure 6 : A simple transposition, with alternate direction of writing, left-right, right-left.

Not very hard to break, in spite of some typos like *Artz* instead of *Arzt*.

The decrypted text finally is:

Bitte um Nachricht ob Assistenzarzt Moritz zuletzt in Valievo[7] *als Arzttatig aus Serbischer befreit wurde*[8]

5 October '16: three grille cryptograms

Near the end of the booklet, October 19169, a few grilles appear; Sacco only presents them together with some conjecture about a possible solution, but no solution is given.

In the following couple of page, Sacco displays two 8x8 grilles, both unsolved, the second incomplete.

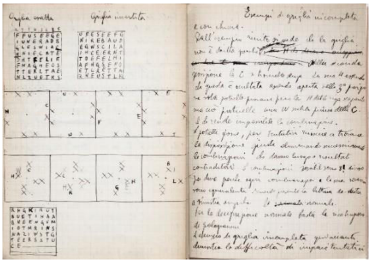


Figure 7 : A couple of pages with grilles.

Here is the first grille; Sacco, searching for the digraph 'CH' very common in German, thought it was a double transposition grille and tried a permutation of the columns shown on the right, under the label "*Griglia invertita*":[10]

5.1 Decrypted texts

In 2017 a challenge was launched on the *Cryptograms & Classical Ciphers* Facebook group and both grilles were decrypted with the aid of dedicated software**.**

The Fleissner 7x7 grille[11], with a black case in the middle is shown in the following figure.

At first look the X and Y on the bottom left could be nulls to fill the grille; and this was a first aid for the cryptanalyst. At last the raw decrypted text is[12] :

[4] English: Major Koppen asks the German Embassy in¨ Sofia a wired answer, which formations are placed there.

[5] English: You are asked to get by the Bulgarian Army Command the disposition of the troops. Major Koppen, Stage (rear) command.

[6] Wikipedia is not the best source for serious research and its reliability is variable; but in this case it was the only source I could find about this Major Koppen; and, after all, I just needed a confirmation he was a real German military officer.

[7] Valjevo is a city of Serbia.

[8] English: Please let us know if the assistant physician Moritz recently in Valjevo as aid physician has been released.

[9] these pages have a beginning date, 17-10-1916; the next is dated 20-10-1916.

[10] under these two grilles he showed some unfinished and unsuccessful trials.

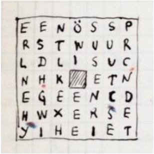
[11] See (Bauer 1997) p. 96,97.

[12] The cryptogram was decrypted by Barth Wenmeckers with a hill cipher algorithm and independently by the author with a computer aided software implemented *ad hoc*.

```
ESWURDENDREIPUNKTEGESEHEN
OTLLICHWEITESRSSUCHENXY
```

There are a few typos and some extra S; the spaced and cleaned text is:

Es wurden drei Punkte gesehen östlich weiter suchen XY[13]



E	E	N	Ö	S	S	P
R	S	T	W	U	U	R
L	D	L	I	S	U	C
N	H	K	▨	E	T	N
E	G	E	E	N	C	D
H	W	X	E	K	S	E
Y	I	H	E	I	E	T

Figure 8 : The 7x7 grille

The 8x8 grilles were also decrypted; here is the first:

Feuer eingestellt feindliche Fahrzeuge abgewandte ausser Sicht Flotten K[ommando?][14]

And here is the decrypted text of the second 8x8 grille, which happened to be encrypted with the same grille:

Krieg Ministerium ist ersucht beantragtes Guthaben von Zw[15]

6 Open questions

A few questions remain unanswered:

Bauer in his book[16], writes that the German Army "early in 1917 suddenly introduced turning grilles with denotations like ANNA (5x5), BERTA(6x6), CLARA(7x7), DORA(8x8), EMIL(9x9), FRANZ(10x0)." Are these grilles the first of this kind? A few months earlier that reported by Bauer? Why this small difference?

Did Sacco manage to solve these grilles in the following months? At the end of October 1916, he moved to Rome, and his booklet ends in the same days. We simply do not know. The answer could be in the notebooks and papers of Sacco in his Rome office, but all these papers were likely destroyed or lost.

Could these cryptograms be Austrian rather than German? The first two cryptograms look like Navy messages and could come from the Austrian fleet in the Adriatic Sea; not very likely from German ships in the Black Sea.

7 Conclusion

As already stated, the booklet has 160 pages, there are still a lot of pages to be studied; these are the more interesting found so far, but there is always the possibility of something more important to be found.

Other pages are about the Austrian diplomatic code, Austrian and German Navy codes, and others, but no complete cryptograms with decrypted texts are given.

I'm publishing the whole booklet on the web, so any researcher will be able to examine it.

Acknowledgements

I wish to thank Cosmo Colavito, engineer and telecommunications historian, for help about Italian Army history in WW 1, and Diana Schindler, for help in translating German cryptograms.

References

Friedrich L. Bauer. 1997. *Decrypted Secrets*. Springer, Berlin, D. ISBN: 3-540-24502-2

Paolo Bonavoglia. 2017. *A 1916 World War I notebook of Luigi Sacco*. Cryptologia, 42:3, 205-221 DOI:10.1080/01611194.2017.1362064

Yves Gylden. 1933. *The contribution of the cryptographic bureaus in the world war*. Signal Corps Bulletin 75 and 81, Washington, DC.

David Kahn. 1967. *Codebreakers*. Scribner, New York, NY. ISBN: 978-0-684-83130-5

Luigi Sacco. 1947.*Manuale di Crittografia*.
Ist. Poligrafico dello Stato, Roma, Italy.

Luigi Sacco. 1977. *Manual of Cryptography* Laguna Hills, Aegean Park Press, (English translation).

[13] English: Three points were seen eastwards, seek further XY.

[14] English: Ceased fire, enemy vehicles got out of sight. Fleet Command.

[15] English: The War Ministry is requested of the required balance by Zw

[16] (Bauer, 1997) pag. 96; see also (Kahn, 1967) pag. 308.