Deciphering German Diplomatic and Naval Attaché Messages from 1914-1915

George Lasry
University of Kassel
Germany
george.lasry@gmail.com

Abstract

In World War One (WW1), the German diplomatic services and the Imperial Navy employed codebooks as the primary means for encoding confidential communications over telegraph and radio channels. The Entente cryptographic services were able to reconstruct most of those codebooks, to obtain copies of others, and to overcome various enhancements introduced by the Germans.

A collection of diplomatic and naval attaché cryptograms from and to the German consulate in Genoa, dating from the late 19th Century to 1915, has been preserved and is held in German archives.[1]

In this article, the author describes the process of identifying the encoding methods, of reconstructing the 18470 diplomatic codebook, and of recovering the superencipherment applied to the German Navy's Verkehrsbuch.

The vast majority of the messages can now be read in clear. Before the war, the communications are mainly about routine consular matters. From the summer of 1914, they reflect the sequence of events leading to war, including the declarations of war. The messages also describe the crucial role played by the German consulate in collecting naval intelligence, and in assisting the German warships Goeben and Breslau in their escape to the Dardanelles in August 1914.

1 Overview

Collections of original encrypted messages are hard to find. As a standard security procedure, it was not allowed to keep records in their encoded form. Diplomatic archives in most cases do not contain original cryptograms. Furthermore, signal intelligence and codebreaking agencies which intercept enemy communications also have a policy of not preserving the original cryptograms. As a result, the discovery of a collection of such documents is a rare event and can be of significant value for cryptology history research and general historians. For example, hundreds of Enigma cryptograms from 1941 and 1945 were decrypted in 2005, shedding new light on German communication procedures and on the fate of resistance leaders who died in Nazi concentration camps (Sullivan and Weierud, 2005). In 2016, a collection of ADFGVX cryptograms from the Eastern Front of WW1 was deciphered, providing new insight into events which occurred towards the end of the war (Lasry et al., 2017).

The Politisches Archiv des Auswärtigen Amtes (PA AA), the political archives of the German Foreign Office in Berlin, holds a series of documents recording communications to and from the German consulate in Genoa (Genova), a port in northwestern Italy (PAAA, c 1915). The records cover the period from 1867 to 1915, most of them from 1914 until May 1915, at the time Italy left the Triple Alliance and declared war on the Austro-Hungarian Empire. While a large part of the documents consists of non-encrypted plaintexts, hundreds of them consist of original cryptograms, encoded using several types of diplomatic and naval codebooks.

This article describes the process of recovering the original plaintexts and analyzing their contents. It is structured as follows: In Section 2, we provide an introduction to codebooks, as well as a description of the main German diplomatic and naval codebooks used in WW1. In Section 3, we describe, step-by-step, the process of identifying the various encryption methods, of recon-

[1] RAV Genua - Records from the German General Consulate in Genoa. Politisches Archiv des Auswärtigen Amtes.

structing one of the codebooks, and of recovering the superencipherment key for another codebook. In Section 4, we provide preliminary findings about the contents of the messages. In Section 5, we briefly assess the cryptographic weaknesses of WW1 German codebooks and procedures.

2 German WW1 Code Books

A codebook is essentially a dictionary of words and other entities that may be encoded using a code, such as a 5-digit number, or a 4-letter code. In this section, the various types of codebooks are described, focusing on diplomatic and naval codebooks used by the German Empire in WW1.

2.1 One-Part Codebooks

The *one-part codebook* is the most convenient form of a codebook. Compiling such a codebook is a relatively simple process. The codebook entries appear in alphabetical order. Numerical codes are assigned to each entry in the same order. It is easy to search for a word and its corresponding numerical code while enciphering a message, or to search for a numerical code while deciphering an encoded message. Therefore, the same physical copy of the codebook can be used for both enciphering and deciphering.

Like any other form of enciphering using substitution, codebooks may be reconstructed by adversaries using frequency analysis. The most frequent codes are most likely to represent the most frequent words of the language. To reduce the frequency of the most common codes, codebook compilers also included expressions and even full sentences as entries in the book. Furthermore, they assigned multiple codes for the most heavily used words. Those measures were not always effective, as they often depended on the operator choices for encoding sentences instead of single words, and for not always selecting the same numerical code for a common word. The main weakness of one-part codebooks is the strong relationship between the alphabetic location of words and their corresponding numerical codes. If two numerical codes are close to each other, and the meaning of the first word is known, it might be possible to guess the meaning of the second word, as it is alphabetically close to the first one.

2.2 Two-Part Codebooks

To achieve better cryptographic security, there should ideally not be any relationship between the (alphabetical) order of the words and the numerical order of the corresponding codes. While doing so increases the cryptographic security of a codebook, at the same time, it is not possible anymore to use the same codebook for both enciphering and deciphering. Two versions of the codebook are required, the first one in alphabetical order for enciphering, and the second one in numerical order for deciphering, in other words, a *two-part codebook*.

At first, the designers of German codebooks introduced two-part codebooks in which they scrambled the order of the pages, but the numerical codes for words within a page (usually 100 per page) were still ordered according to the alphabetical order of the words. As a result, numerically close codes could still be guessed. Worse, new codebooks were often no more than a copy of a previous codebook (possibly already reconstructed by the enemy) in which only the original pages had been reshuffled, but not the words inside each page. To reconstruct such a codebook, it was enough to map each page from the previous version to the corresponding page in the new version. For that purpose, the knowledge of the meaning for only a few tens of codes (in the new codebook version) was usually sufficient.

To achieve a purely random ordering, 'hat codes' (also known as 'lottery codes') were introduced during the war. Their name is derived from the manual methods used in WW1, such as mixing paper strips inside a hat, and extracting them randomly and assigning them numerical codes, so that the numerical codes have no relation to the alphabetical order of the words. Reconstructing a hat code by codebreaking agencies required a significantly larger and longer effort, including extensive trial-and-error. In general, cryptanalysts could never reconstruct such a codebook in its entirety.

2.3 Superencipherment

Physical copies of a codebook may always fall into the enemy's hands, and while harder with hat codebooks, reconstruction by analytical means is still possible. Therefore, codebooks should not be used for an extended period of time. On the other hand, compiling a new codebook and distributing its physical copies was often difficult, especially to embassies in countries without a border with Germany, such as Spain. To increase the security of existing codebooks without replacing them, German cryptographers often applied a *superencipherment* (an additional encipherment) on the numerical codes. Methods of superencipherment either consisted of transpositions (changing the order of the digits in the numerical code), substitutions (replacing a digit with another digit), or additives (some number mathematically added to the numerical codes). At first, superencipherment methods were simple or used over a long time span, allowing Room 40, the section in the British Admiralty responsible for cryptanalysis, to recover the keys on a regular basis.[2]

Toward the end of the war, the Germans introduced more sophisticated methods, but often made the severe mistake of communicating the details of a new superencipherment method in a message encoded with a previous version, already known to Room 40.[3]

2.4 German Diplomatic Code Books

Germany started the war with several families of diplomatic codebooks in place, mainly the 13040 and the 18470 families. A family of codebooks includes several codebooks derived from one another. Those first German diplomatic codebooks usually consisted of the following sections:

- **Dreinummerheft**(3-digit code): This section was common to all codebooks in the 18470 and 13040 families. The prewar 18102 codebook also used the same Dreinummerheft codes. The Dreinummerheft consists of 3-digit codes, from 000 to 999. They represent numbers (000 to 500, 00 to 99) and dates (January 1 to December 31). The mapping follows an almost predictable pattern. As a result, to fully reconstitute the Dreinummerheft, an adversarial code-breaking organization such as Room 40 needed to know the meaning of only a few of the Dreinummerheft codes.

- **Places**: A set of pages (randomly numbered) dedicated to names of cities, countries, nationalities, and foreign government institutions. Each page contains 100 entries.

- **Words and Expressions**: A set of pages (randomly numbered) dedicated to words, expressions and some full sentences. Each page contains 100 entries.

- **Persons**: A set of pages dedicated to names of persons, and entities such as banks and commercial shipping lines. Those pages, randomly numbered, were sparsely populated (usually only ten names out of the possible 100 in a page).

- **Supplement**: A set of pages with additional names and places, with numerical codes randomly assigned.

Except for the Dreinummerheft, which consists of 3 digits, the numerical codes have 4 or 5 digits. The three leftmost digits (for a 5-digit code) or the two leftmost digits (for a 4-digit code) represent the page number. The second digit to the right represents the *block* number. Each page has ten blocks (from 0 to 9), each block containing ten words. For example, code `10275` corresponds to the word *Dampfer* (steamer), and it is the sixth word (the last digit is 5, we start counting from 0) in block 7 of page 102. The order of the pages (the page numbers) does not correspond to the alphabetical order of the words they contain. Furthermore, the order of the 10-word blocks inside a page does not correspond to the alphabetical order of their contained words. However, all the 100 words inside a page are always relatively close alphabetically. Also, the ten words inside each block are in alphabetical order. While those codebooks are nominally two-part codebooks, it is still possible to deduce the meaning of one numerical code based on the meaning of another code on the same page or block.

The 18470 and its derivatives, such as the 12444, the 1777, and the 2310, were fully recovered by Room 40, aided by the capture of codebook 3512 in Persia in 1915. Interestingly, it seems that Room 40 never shared their copy of the captured codebook 3512 with their US counterparts, despite closely cooperating in various domains. Room 40 was able to analytically reconstruct most parts of the 13040 codebook (which was used to encipher the famous Zimmerman Telegram), as well as its derivatives, the 5950 and the 26040 (the 13040 superenciphered using

[2] (Gannon, 2010), p. 130.

[3] (Gannon, 2010), p. 261, footnote 20.

a constant additive).[4,5]

The German diplomatic services also developed a series of two-part hat codes, such as the 5300, 6400, 7500, 8600, and 9700 codebooks. Room 40 was able to recover large parts of those codes, and in particular, codebook 7500, used to encipher one of the versions of the Zimmerman Telegram.[6]

Interestingly, despite the capture of a copy of the 3512 codebook, and the publication of the Zimmermann Telegram, the German diplomatic cryptographers never realized that both the 18470 and 13040, and their relatives, had been compromised. In a report from April 1917, Herman Stützel, a German Navy cryptographer, describes how he was able to decipher messages encoded with the 18470 codebook, only from intercepted communications. He was also able to decipher messages encoded with the 5300 hat code with various superencipherment methods (Stützel, 1969). Ironically, Room 40 intercepted and deciphered a message containing the report. The reaction of the German diplomatic services to the report is unknown. The Imperial Navy swiftly reacted, implementing a series of new complications on top of their naval attaché codes (see Section 2.5).

2.5 Naval Code Books

At the outset of the war, the Navy had several codebooks in use for various purposes, including the *Signalbuch der Kaiserlichen Marine (SKM)*, used mainly for signaling and communications between ships, and the *Handelsverkehrsbuch (HVB)*, for communications with merchant ships. For communicating with naval attachés, the Imperial Navy also employed the *Satzbuch (SB)*, as well as the *Verkehrsbuch (VB)*. The SKM, HVB, SB, and VB were all one-part codebooks. The VB and the SB were usually superenciphered, but at the beginning of the war, the keys were not frequently changed. The German Navy was slow to realize that copies of its books had fallen into enemy's hands, early on in the war. Later on, the Navy implemented various methods for superencipherment, and also introduced new codebooks such as the *Flottenfunkspruchbuch (FFB)*, which replaced the SKM in 1917.

The main codebook for communicating with naval attachés, the Verkehrsbuch, maps words and entities into groups of 5 digits. It consists of several sections, for words and expressions, for names of places and ships, as well as for indicating positions of ships on maps. The Stützel report (see Section 2.4) caused great alarm at the German Admiralty, and the Navy introduced new, more complex superencipherment methods. Based on the voluminous numbers of transcripts in British National Archives in Kew, which also mention the types of code and superencipherment, those probably did not pose serious problems to Room 40's codebreakers. Using decrypts from the traffic between Berlin and the naval attaché in Madrid, Room 40 was able to unravel and prevent various plots and espionage activities conducted from the German embassy in Madrid.[7]

3 Deciphering the Genoa Cryptograms

In this section, we present the step-by-step process of deciphering the majority of the cryptograms in the Genoa collection. We describe the processes of classifying the various types of cryptograms, of reconstructing a diplomatic codebook, of identifying the superencipherment method for a naval attaché code, and of recovering its key. This detective work also required the retrieval and survey of a multitude of documents from archives in Germany, the UK, and the US, with the assistance of leading experts. The work continued with building a computerized database of the cryptograms, successfully deciphering most of them, and validating the decryptions with newly found documents.

3.1 Classifying the Cryptograms

At first, we obtained six files from the RAV Genua collection at the PA AA, containing both plaintexts and cryptograms.[8,9,10,11,12,13]

After analyzing the structure of the cryptograms, we were able to divide them into four categories:

[4] (Gannon, 2010), p. 130.

[5] (Gannon, 2010), p. 205.

[6] (Gannon, 2010), p. 131.

[7] (Gannon, 2010), Chapter 13 - The Spanish Interception.

[8] PA AA - RAV Genua 09, Acten betreffend Ziffern 1867-1908.

[9] PA AA - RAV Genua 10, Chiffrierwesen 1898-1913.

[10] PA AA - RAV Genua 11, Sammlung der Chiffres 1889-1908.

[11] PA AA - RAV Genua 12, Sammlung der Chiffres mit Ausschluss der Korrespondenz mit den Marinebehörden, Bd. 2, 1904-1914.

[12] PA AA - RAV Genua 13, Chiffrierte Telegramme 1914-1915

[13] PA AA - RAV Genua 14, Telegramme in Chiffre. 1914-1915.

- **Sequences of letters**: Two messages from 1897 and 1898, each composed of series of letters, from a to z. After a quick analysis, we identified the encryption method to be Vigenère, and we deciphered the two cryptograms. The German plaintexts contain references to another cipher system, as well as new keywords for that system, for which there are no corresponding cryptograms in the Genoa collection.

- **5-digit codes with indicator 1847X:** A set of messages composed of groups of 3, 4, or 5 digits, from December 1913 to mid-1915. Those cryptograms have an indicator of the form 1847X (18470 to 18479, usually 18470) as one of the first groups.

- **5-digit codes with indicator 1810X:** A set of messages composed of groups of 3, 4, or 5 digits, from 1898 to November 1913. Those cryptograms have an indicator of the form 1810X (18100 to 18109, usually 18102) as one of the first groups.

- **10-letter codes:** A set of nine messages from August 1914, composed of groups of 10 letters each, sent between the Kaiserliche Marine Admiralsstab (German Imperial Navy Admiralty), German warships Goeben and Breslau, and the German consulate in Genoa.

3.2 Deciphering Diplomatic Codebook 18470 Cryptograms

Following the successful decryption of the Vigenère messages, we first analyzed the cryptograms with the 1847X indicators. In the archive records, a few hundred of them are available. Although plaintexts also appear in the original records, we could not match any of them to a corresponding cryptogram with a 1847X indicator. We found a key document on the subject, *Studies in German Diplomatic Codes Employed during the World War*, written by Charles J. Mendelsohn, and compiled into a War Department report in 1937 (Mendelsohn, 1937). The first of its three sections is named *Code 18470 and Its Derivatives*. It describes the structure of codebook 18470, based on a 1918-19 study by Mendelsohn and a team of cryptographers at the Military Intelligence Division of the General Staff in Washington. The study also includes a few original messages encoded using 18470, as well as the German meaning for the codes in those cryptograms. With those, we were able to reconstruct about 10% of the 18470 codebook and to produce fragmentary decryptions for some of the messages in the Genoa files.

In codebook 18470, while the pages are scrambled, the words inside each page (such as the words with codes between 12100 and 12199) are alphabetically close. Based on this, we tried to guess assignments for unknown numerical codes in pages for which we had other known assignments. A team of linguists investing time on the problem would probably have been able to reconstruct large parts of the codebook and decipher most of the cryptograms, given the availability of hundreds of them. However, such resources were not available to the author. To progress, either a copy of the codebook, or some plaintexts matching the cryptograms were required. A search for matching plaintexts in archives produced only a single message, dated August 1, 1914, sent by the German consul in Genoa, von Herff, to the German Foreign Office. [14]

It reads as follows:

```
Nummber 7.  Im hiesigen Hafen
liegende englische Dampfer der White
Star Line und British India Company
'Celtic' und 'Malda' sind von ihren
Gesellschaften angewiesen möglichst
rasch auslaufen und westlisch.[15]
```

The plaintext is a report about British ships leaving Genoa westbound. Using the date, the message length, and the correspondents, we were able to locate the original ciphertext in the Genoa files.[16]

The code corresponding to the word *Dampfer* (steamer), `10275`, also appears in Mendelsohn's study and has the same meaning. Other codes correspond to words or expressions located in alphabetical positions as expected from Mendelsohn's interpretation of the 18470 code. Based on this, we were able to conclude that not only the messages with the 1847X indicators were indeed encoded with the 18470 codebook, but that they

[14] PA AA, R 19875, Bl. 31. Generalkonsul von Herff an das Auswärtige Amt.

[15] 'In local port anchored steamers of the White Star Line and British India Company 'Celtic' and 'Malda' have been instructed by their companies to leave port as soon as possible and (sail) westbound.'

[16] PA AA - RAV Genua 13, Chiffrierte Telegramme 1914-1915, p. 6.

were encoded without any additional encipherment. This finding was an important step. But while the plaintext also provided the meaning for a few additional codes, this was not enough to progress with the decryption of other 18470 messages in the collection.

We started to look for copies of original codebooks. Copies of various WW1 German codebooks are available at the British National Archives at Kew, including naval codes such as the SKM, captured in 1914 from the German warship Magdeburg. The archives also include a version of code 13040, reconstructed via cryptanalysis by Room 40, and used to encode the (in)famous Zimmermann Telegram in 1917. The successful decipherment of the Zimmermann Telegram, along with German pursuance of unrestricted submarine warfare, contributed to the entry of the United States into the war. However, neither the 18470 codebook, nor the 18102 appear in British, German, or US archives.

In his study, Mendelsohn described how the 18470 codebook was part of a larger family of codes, including the 12444, the 1777, and the 2310 codebooks, all derived from the same division of words and expressions to pages, the pages being reshuffled differently. We could not find any of the 18470 derivatives listed by Mendelsohn in US, British, or German archives. Further research in the British National Archives at Kew produced another document, *The Political Branch of Room 40*, which mentions two other codebooks, 89374 and 3512, captured by the British in Persia in 1915. According to this report, an analysis by the Political Branch led to the conclusion that those two codes stem from the same source, albeit reordered differently.[17]

Several recent papers also link those two codebooks to the 18470 family, and this assumption was strengthened by the fact that Mendelsohn mentions there existed at least one member of that family, unknown to him (Freeman, 2006; Kelly, 2013). Fortunately, a copy of the 3512 codebook is available at Kew.[18]

After obtaining a photocopy of the 3512 codebook, we needed to establish the precise relationship between the 3512 and the 18470, using the known numerical codes from Mendelsohn. Eventually, and after an extensive trial-and-error process, we were able to reconstruct almost the entire mapping between the codebooks. While some random elements of the mapping created some challenges, the compilers of the 18470 derivatives (including the 3512) had applied several regular patterns in the process, which helped us significantly (and also weaken the security of the codebook). After the mapping was established, we wrote a special software and used it to decrypt all the messages encoded with 18470, except for a few names which appear in a special supplement of the codebooks (and for which there is no conversion formula or pattern).

3.3 Diplomatic Codebook 18102 Cryptograms

After successfully reconstructing codebook 18470, we turned to the 1810X cryptograms. Several plaintexts from October and November 1913 announce the transition from the 18102 codebook to the 18470 codebook, and an order to destroy all physical copies of the 18102. Unfortunately, we were unable to find copies of the 18102 codebook in any of the relevant British, German or US archives. An analysis of the ranges of pages showed that the 18102 code could not have been a derivative of the 18470. Codebook 18102 might still be a derivative of the 13040 codebook, as the 13040 was also in use before the war, but there is no evidence in that direction, and further work is needed to check this hypothesis. Lacking a corresponding plaintext for any of the 18102 messages, or a derivative of this code, we were neither able to reconstruct the codebook, nor to decipher any of the cryptograms. Since the 18102 and the 18470 share the encoding of numbers and dates (Dreinummerheft), it might be possible to look for matching plaintext-ciphertexts in the files based on the message serial numbers.

3.4 Deciphering Naval Codebook Cryptograms

The last category is comprised of only nine cryptograms, sent in August 1914, and involving Navy recipients or senders. They consist of 10-letter codes, such as `DUMOSEPIRE` or `CLYHMUIMUS`, with the prefix (the first five letters) of one of the 10-letter codes often used as the prefix in another 10-letter code, or the suffix (the last 5 letters) of one code often used as the suffix of another code. A likely codebook candidate appeared to be the

[17] (ADM, 223) ADM 223/773, George Young, Political Branch of Room 40, Section ‘89374 and 3512’.

[18] (HW, 7) HW 7/26 German Codebook Number 3512.

HVB, used for communicating with German merchant ships. While the HVB is primarily a 4-letter code, each code also has a 10-letter equivalent, composed of a combination of a 5-letter prefix and a 5-letter suffix. However, none of the HVB prefixes or suffixes seemed to match any of those found in the Genoa cryptograms. The HVB also had an optional substitution superencipherment.[19]

This substitution preserves the vowel-consonant structure of the original ten letters, and since this characteristic can be used to validate possible outputs, we were able to rule out the possibility that the cryptograms were encoded with HVB with substitution.

The next obvious candidate was the VB, intended for naval and military attaché communications. The VB consists of 5-digit codes. With the assistance of other scholars, the author was able to obtain a photocopy of the VB, as well as a copy of a VB supplement.[20,21]

The supplement describes a mapping of 5-digit VB codes to 5-letter prefixes (representing the first three digits) and 5-digit suffixes (representing the last two digits). Those prefixes matched those found in the Genoa files. Therefore, we were able to map all the 10-letter codes in the collection, into their 5-digit equivalents. However, none of these 5-digit codes would map to words or expressions in VB which have a logical or relevant meaning, indicating that some form of superencipherment had been employed. After all, naval communications were deemed to be more sensitive than regular diplomatic communications. There was no clue, however, about the specific type of superencipherment employed here. At this stage, the research had reached a dead end regarding the 10-letter cryptograms.

After several months of extensive research, we found in the British National Archives at Kew a message sent on August 3, 1914, to the Goeben warship by the Admiralty in enciphered VB. The file consists of a log of English transcripts (translations) of VB messages from 1914, intercepted and deciphered by Room 40. The message from August 3, 1914, is the only one in the file for which the cryptogram is also available. The German plaintext was also available from other sources (Lorey, 1928). Unfortunately, we could not (yet) draw any conclusions from this sample alone.[22]

A breakthrough came from a review of the messages sent in the 18470 codebook, which by then we were already able to decipher. A message from Berlin was sent in 18470 code to Genoa on August 1, 1914, with the following instructions:

```
Nummer 9 unter Bezugnahme auf Telegr.
Nummer 10.  Schlüsselzahlen zu Marine
Chiffres lauten:  Schlüssel B: 469,
reserve B: 718.  Auswärtig.  Amt.[23]
```

In a serious breach of security, this message specifies the primary key (469) as well as the reserve key (718) for the Navy's cipher. We hypothesized that those could be the key for some superencipherment. The next step was to look for references to any of the two keys, hoping this might help to identify the type of superencipherment. We were unable to find any reference to key 469. However, the author vaguely remembered a mention of key 718, in the multitude of archive files already reviewed. Luckily, an extensive survey of all the material gathered so far resulted in the (re)discovery of a reference to key 718, in Mendelsohn's study (Mendelsohn, 1937). The third chapter lists several methods for the superencipherment of codes. One of them is based on *sliders* (*Schieber* in German), which consist of a set of three substitution slides. Those slides map some of the digits of the 5-digit codes to other digits according to some random pattern. A 3-digit key specifies the starting position of each one of the three sliders. Mendelsohn provides the ordering for a set of 3 sliders used before the war and until 1917, described in Table 1 (Mendelsohn, 1937). In this example, the sliders are set to key 718, and are to be applied on the second, third, and fourth digits (the first and last digits are kept unchanged).

Interestingly, the example given by Mendelsohn uses key 718 which happens to be the reserve naval key mentioned in the 18470 message. This was a clear indication that the 10-letter cryptograms might have been superenciphered using

[19] (ADM, 137) ADM 137/4320, Chiffresschlüssel H.V.B. 1913.

[20] (ADM, 137) ADM 137/4374, Verkehrsbuch (VB) 1908.

[21] (ADM, 137) ADM 137/4314, Verkehrsbuch Supplement.

[22] (ADM, 137) ADM 137/4065, Log of intercepted German signals in Verkehrsbuch code from various sources 1914-1915, entry 113.

[23] 'Number 9 with reference to telegram number 10. The keys for Marine cipher are: Key B: 469, reserve B: 718. Foreign Office.'

Original Digit	Second Digit Becomes	Third Digit Becomes	Fourth Digit Becomes
0	7	1	8
1	0	9	3
2	9	4	4
3	2	6	6
4	6	2	5
5	3	7	2
6	5	3	7
7	8	5	1
8	1	0	9
9	4	8	0

Table 1: Slider for VB

sliders. Next, we tried to decode some of the 10-letter cryptograms using the sliders with key 718, but this failed to produce any plausible plaintext. Another option was key 469. We tested that slider key on one of the cryptograms and obtained a few German words related to *Kohle* (coal), a topic very much relevant to the escape of the Goeben. When applying the sliders with key 469 to other cryptograms, we could finally recover plausible plaintexts. To further validate those findings, we tried to apply the same slider method to the message from August 3, 1914, sent from the Admiralty to the Goeben. While this message could not be deciphered using key 469, further analysis showed that another key was applied, namely 5288, with the 3rd slider (at key position 8) also being applied to the fifth digit (in addition to being applied to the fourth digit). This message reads as follows:

```
August 3 Bündnis geschlossen mit
Türkei Goeben Breslau sofort gehen
nach Konstantinopel bescheinigen.
```
[24]

We had thus achieved a complete solution for the elusive 10-letter naval cryptograms in the Genoa collection. We were now certain that those consisted of VB codes superenciphered with sliders, using key 469.

3.5 New Genoa Files

Our project did not end here. One year after successfully deciphering the cryptograms in the first six files, we were able to obtain three new files from the Genoa collection in the PA AA. Two of them included plaintexts, many of which could be matched to original 18470 cryptograms based on their serial numbers. The matching could not be done before as the serial numbers appear encoded in the cryptograms. Further analysis showed that those new files include plaintexts for about 40% of the 18470 cryptograms, and it was possible to validate that they had been (mostly) corrected deciphered.[25,26]

A third file contained messages from 1910 encoded using VB with sliders. Surprisingly, those could be decrypted using slider key 469, which indicates that this key was in effect for several years and until the war broke, highlighting a severe breach of security.[27]

Those decryptions further confirmed the correctness of our solutions for the 1914 naval messages in the collection.

4 The Contents of the Cryptograms

The ”RAV Genua - Generalkonsulat Genua” collection at the PA AA covers the period from 1867 to May 24, 1915, when the German consulate was closed after Italy entered the war on the side of the Entente powers. It also covers the period from 1921, after the consulate reopened, until the end of World War 2. Our research focuses on the first period, and especially on the years 1913, 1914, and 1915. The records cover a wide area of topics, including administrative and legal matters (such as passports and visas), protocol, local politics, naval intelligence, economy, trade, and shipping.

Of particular interest are the decryptions related to three subjects, namely the declarations of war in summer 1914, the role played by the consulate in gathering naval intelligence, and its role in assisting the Goeben and Breslau warships to escape to the Dardanelles. The latter event had a significant impact on the war in the Mediterranean Sea and the Middle East.

4.1 No War Without Declaration

World War I was one of the last modern, major military conflicts in Europe which started with formal declarations of war, by all parties involved. Countries felt obliged to formally declare war, as part of an official international protocol defined

[24] ‘August 3: Alliance with Turkey concluded. Goeben and Breslau should at once sail to Constantinople.’

[25] PA AA - RAV Genua 74, Kriegsgefahr 1914-1915.

[26] PA AA - RAV Genua 77, Krieg, Militärsachen 1914-1915.

[27] PA AA - RAV Genua 68, Chiffres nach d. Marine 1907-1914.

at The Hague Peace Conference of 1907, and for internal legal and political reasons. With a formal declaration, a country could start mobilizing its army. Also, military and merchant navy ships had to be informed that they should leave hostile ports, to avoid being seized. As this was usually done before issuing the formal declaration of war, any signs of movement of ships in times of crisis might indicate an upcoming declaration of war. The Genoa collection includes a series of messages informing the consulate of the various declarations of war, and of their impact such as the freedom of movement of German nationals. From the first declaration of war between Russia and the Austro-Hungarian Empire, and throughout August 1914, the tensions escalate, and this is reflected in the communications. For example, on August 2, 1914, the following message is sent from the German Foreign Office to Genoa:

```
Nummer 8.  Durch allerhöchst
kabinettsorder ist Mobilmachung
angeordnet.  Bitte deutsche Schiffe
im dortig Amtsbezirk ohne rücksicht
auf Geheimhaltung weiter warnen
und Dienstpflicht zur Rückkehr
auffordern.  Jagow.[28]
```

4.2 Naval Intelligence

A large number of cryptograms relate to naval intelligence collected mainly from public sources, such as newspapers, or German nationals returning from British and French colonies. Movements of ships, including warships as well as merchant ships transporting troops, are routinely reported. An example of such a report is given in Section 3.2.

4.3 Assistance to the Goeben and Breslau Warships

The most interesting findings in the decrypted records are about the extensive assistance given by the German consulate in Genoa (as well as other German representations in the region), to the German warships Goeben and Breslau in their escape to the Dardanelles, in August 1914. To extend its presence and influence in the Mediterranean Sea, the German Empire had before the war sent to the region one of her most modern warships, the battle cruiser Goeben, together with the light cruiser Breslau, under the command of Rear Admiral Souchon. Given the vast superiority of the British and French fleets in the Mediterranean Sea, those two lone ships were threatened to be isolated, captured or destroyed, as the war broke out. Souchon was first ordered to escape via the Gibraltar straights but instead decided to attack French facilities in North Africa. After the attack, with the westbound route being blocked, he was ordered to reach the Dardanelles, following the signing of an alliance between the Ottoman Empire and the German Empire in the beginning of August 1914. To successfully escape vastly superior enemy forces, the Goeben needed large quantities of coal, required to reach higher speeds. Supply of coal in sufficient quantities could only be found in Italy or obtained from German merchant ships. For that purpose, the German Foreign Office instructed its local representations to assist the Goeben and Breslau to secure large quantities of coal. This effort is reflected in several messages, encrypted with the 18470 codebook, as well as with the VB with superencipherment. For example, the following message was sent on August 1, 1914, from von Herff, the consul in Genoa, to Rear Admiral Souchon:

```
Goeben - Messina.  Auf Ersuchen von
Breslau:  Kohlendampfer ist nicht
vorhanden.  Deutsches Kohlendepot
ist bemüht, möglichst viele Kohle
kaufen, hoffen Montag 2000 Tonnen
gemischte gut Kohle zu sammeln und
Bescheid zu geben.  Welche Menge von
Kohle gebraucht und wohin zu liefern?
Herff[29]
```

Other records describe the requisition of German merchant ships and their coal, the securing of funds for transactions, and negotiations with Italian authorities. Eventually, the Goeben and Breslau were able to obtain significant quantities of coal, allowing them to escape the British and French fleets, and to reach the Dardanelles. They joined the Ottoman fleet under the Ottoman flag. Their attack on Russian facilities, carried indepen-

[28] 'Number 8. By highest cabinet decision mobilization has been ordered. Please continue warning German ships in the local district, regardless of confidentiality, and request those liable for [military] service to return. Jagow.'

[29] 'Goeben - Messina. At the request of Breslau: Coal steamer is not available. German coal depot working hard to buy as much coal as possible and expects to collect 2000 tons of mixed, good quality coal on Monday, and will report on it. How much coal is needed and where to deliver? Herff'

dently of their Turkish counterparts, later precipitated the entry of the Ottoman Empire into the war (Van der Vat, 2000). As a result, the Entente powers had to divert significant resources to the Mediterranean Sea and the Middle East, including for the catastrophic Dardanelles offensive in 1915. The critical role played by the consulate in Genoa is for the first time exposed in the decrypted messages from the Genoa collection.

5 Conclusion

This research highlights inherent weaknesses in German cryptographic methods and procedures for diplomatic and naval communications at the beginning of WW1, as follows:

- Most of the confidential diplomatic communications relied on codebooks, which were in use for long periods of time. Also, the compilers of codebooks often used regular patterns, rather than fully random patterns, to map certain elements of the codebook to their equivalent numerical codes, thus facilitating the work of adversarial codebreakers.

- Instead of issuing entirely new codebooks, the German cryptographic services created new variants of existing codebooks by only modifying the order of their pages. As a result, the capture of one codebook was often enough in order to reconstruct other related codebooks.

- The key for the superencipherment of one codebook was often transmitted using another, possibly compromised codebook. Moreover, the superencipherment methods, as well as the keys, were infrequently modified.

As a result of those weaknesses, the author was able to decipher the vast majority of the Genoa encoded traffic, using methods which are very similar to those employed by Room 40 and other WW1 codebreaking agencies. The decipherment of the cryptograms in the Genoa collection also exposes new historical material related to key developments and events in 1914-1915. Further research is underway to analyze the contents of the messages, and their historical context and significance.

References

ADM. 137. *Admiralty: Historical Section: Records used for Official History, First World War*. The National Archives.

ADM. 223. *Admiralty: Naval Intelligence Division and Operational Intelligence Centre: Intelligence Reports and Papers*. The National Archives.

Peter Freeman. 2006. The Zimmermann Telegram Revisited: A Reconciliation of the Primary Sources. *Cryptologia*, 30(2):98–150.

Paul Gannon. 2010. *Inside Room 40: The Codebreakers of World War 1*. Ian Allan Publishing Ltd.

HW. 7. *Room 40 and successors: World War I Official Histories*. The National Archives.

Saul Kelly. 2013. Room 47: The Persian Prelude to the Zimmermann Telegram. *Cryptologia*, 37(1):11–50.

George Lasry, Ingo Niebel, Nils Kopal, and Arno Wacker. 2017. Deciphering ADFGVX messages from the Eastern Front of World War I. *Cryptologia*, 41(2):101–136.

Hermann Lorey. 1928. *Der Krieg in den türkischen Gewässern: Bd. Die Mittelmeer-Division*, volume 1. ES Mittler.

Charles J. Mendelsohn. 1937. *Studies in German Diplomatic Codes Employed during the World War*. War Department, Office of the Chief Signal Officer, Government Printing Office, Washington, DC. Register 191.

PAAA. c. 1915. *RAV Genua - Records from the German General Consulate in Genoa*. Politisches Archiv des Auswärtigen Amtes.

Hermann Stützel. 1969. Geheimschrift und Entzifferung im Ersten Weltkrieg. *Truppenpraxis*, 7:541–545.

Geoff Sullivan and Frode Weierud. 2005. Breaking German Army Ciphers. *Cryptologia*, 29(3):193–232.

Dan Van der Vat. 2000. *The Ship that Changed the World. The Escape of the Goeben to the Dardanelles in 1914*. Edinburgh.