Documents of Polish-Soviet War of 1919-1920 Codebreaking

Marek Grajek
Independent researcher
mjg@interia.eu

Abstract

Codebreaking during the Polish-Soviet war of 1919-1920 not only assured Polish victory in this conflict but also provided the foundations for the future triumph of the Cipher Bureau over Enigma. Original documents from that period not only survived several storms of history, but have been digitized and are now available for the researchers. This paper is divided into three parts. The first one drafts the historical context of the documents, the second presents their structure and contents, and the final one offers some remarks regarding errors committed by Soviet cipher clerks which had facilitated Polish victory.

1 Introduction

Having been reborn in 1918, after 123 years of partitions, Poland had no tradition in the cryptology or the codebreaking. Its international situation did not place either of them in the center of attention. Immediately after its resurrection the new state had to fight five wars on its only vaguely defined borders. It was natural for its leaders to focus on the number of available bayonets and sabers rather than on arcane and mysterious discipline – the codebreaking. But in spite of this understandable tendency its was the codebreaking that provided the cornerstone for Polish victory in the most deadly conflict of that period – war with the Soviet Russia in 1919-1920.

Only few documents from that period survived the storms of history that kept rolling over Poland through the next decades. Files referring to the cryptology and the codebreaking operations are usually well guarded and protected from falling into foreign hands. Historians knew quite a bit about the scale of Polish success with the Soviet ciphers from the indiscretions of the participants of the events (Wyżeł-Ścieżyński, 1928). However, it seemed unlikely that the original documents of this operation might have survived and reemerge in rather surprising circumstances.

After the collapse of communism in Poland most archives of the former secret police were transferred to the civilian institutions. Historians were surprised to find among them the presumably complete archive of the Polish Army codebreaking operation from the period of the Polish-Soviet war. The stamps and inventory numbers on the files witnessed its long and complicated journey to its final destination – country's Central Military Archive. Over a period of more than ten years the files have been catalogued, digitized and made available for the researchers. Finally, in 2017, the entire archive was included into the UNESCO Memory of the World register.

2 Historical background

This paper is not intended to introduce the reader into the history of the Polish-Soviet war of 1919-1920. Interested reader will find its more extensive coverage in (Davies, 2003) and (Zamoyski, 2008). Minimal historical background provided below is addressed mostly to the readers interested mainly in cryptography.

Polish-Soviet war of 1919-1920 broke out undeclared. On 5 February 1919 Poland and Germany had signed an agreement concerning the evacuation of German troops stationed at the former eastern front of WWI. Their gradual transfer to Germany was leaving vacuum in the previously occupied Polish and Russian territories. That vacuum was being gradually filled in by the troops of the neighboring states: Soviet Russia, Poland, Ukraine and the Baltic countries. Considering the collapse of the Tsarist Russia, replaced by the aggressive Soviet regime,

emergence of the successor states and lack of the defined and recognized borders between them, peaceful solution seemed unlikely.

Polish soldiers first clashed with the advancing Soviet troops on 14 February 1919 near Mosty, stopping the Soviet advance and then gradually pushing Bolsheviks back to the east, reaching in August of the same year Minsk, Bobruisk and Borisov. During the following period of lull, in July and August 1919, a lucky coincidence facilitated Polish breakthrough with the Soviet ciphers. One of the officers of the emerging cipher service of the Polish Army wished to dance at his sister's wedding and asked a colleague for replacement at the night duty. Lieutenant Jan Kowalewski had no previous experience with the ciphers or the codebreaking, but his perfect knowledge of Russian language plus common sense permitted him to break the cipher before the morning. Kowalewski was immediately transferred to the cipher section of the General Staff, where during the following months he managed to organize an effective and efficient codebreaking service.

Polish codebreakers permitted the Polish Army HQ an almost complete penetration of enemy's communications and played a crucial role in pivotal episodes of the war. More or less at the same time when Kowalewski was breaking the first Soviet message, Polish-Soviet peace talks started in Mikaszewicze. Bolsheviks, fighting at the same time desperately against Denikin's white Russians, were offering considerable territorial concessions for the peace at the Polish front. Some historians describe Polish operation in Ukraine in April 1920 as an unprovoked aggression. Two facts contradict this opinion. Polish Army was entering Ukraine in alliance with the Directorate of People's Republic of Ukraine. Kowalewski and his service provided the second critical element of decision. Immediately after decisive Soviet victory over Denikin, Polish codebreakers were able to detect a fast buildup of the Soviet forces at the Polish front, indicating clearly Soviet aggressive intentions; escalation of the conflict was unavoidable.

During the following operations the codebreakers managed to play the decisive role. Their precise information about Soviet forces in Ukraine assured a complete Polish victory in this theater of operations. The codebreakers were also able to provide a timely warning about the Budionny's First Cavalry Army being transferred from Caucasus to the Polish front, changing thus the strategic situation in Ukraine. During the operations following Soviet attack in the northern front sector on 4 July, information provided by the codebreakers was of utmost importance for the Polish Army HQ. Warfare took highly mobile character. Polish troops were forced to execute the strategic retreat of over 600 kilometers, ending in mid-August at the gates of Warsaw. During that period Polish forces at the front line and beyond it were instructed to damage existing wire networks, forcing the advancing Soviets to go wireless.

When the Soviet divisions were approaching the central Poland, hundreds of thousands of Poles volunteered for military service. Among them were three mathematics professors of the Warsaw University, Stanisław Leśniewski, Stefan Mazurkiewicz and Wacław Sierpiński. Attached to Kowalewski's service they played a critical role during the events of the next few weeks. It was Sierpiński, who in early August had broken the new Soviet cipher key basing on just the single intercepted message. This message, however, presented the complete Marshal Tuchachevski's plan of the decisive Warsaw operation. Precise knowledge of enemy's intentions delivered the foundations for the Polish victory in the ensuing Battle of Warsaw and the entire war. Role played by the mathematicians in this victory was well remembered and provided a cornerstone of the future Cipher Bureau's triumph over Enigma.

3 Fates of Kowalewski's archive

Soon after the victory Jan Kowalewski was transferred to other duties in Polish intelligence service. For some time in 1921/1922 he was teaching cryptology at the Japanese Military Academy. The archive of his service was deposited at the Central Military Archive, where is rested undisturbed until September 1939.

During the Polish campaign in 1939 the Cipher Bureau, successor of Kowalewski's service, managed to evacuate or destroy all the traces of its operation, including in particular its success over Enigma. However, part of the its historical records stored at Central Military Archive fell into the German hands after Warsaw surrender. From the German sources (Reile, 1963) we know that it took six trucks to transfer

captured documents to the military archive in Danzig-Oliva, were they were thoroughly examined by the Abwehr staff. This blunder brought tragic consequences for Polish intelligence service; over 100 of its agents in Germany have been identified, captured and mostly executed. But it was probably the same blunder that we owe the preservation of the codebreakers' archive.

Sometime in 1945 Soviet Army captured Danzig, where the entire archive was stored. The documents were transferred in bulk again, this time to the Soviet State Archive. We do know nothing about their fates there, judging however by the results they were considered redundant by their Russian holders and, at time and circumstances unknown, returned to Poland.

There they landed in the archive of the communist secret service, inaccessible to outsiders. Paranoia of secrecy common for the communist regimes, plus the character of the files, witnessing one of the major Polish triumphs over current forced ally, determined their fate for as long as communists ruled the country. It was only after the collapse of communism in Poland, that during the review of the archives files have been discovered, and transferred back to the place of their origin, i.e. Central Military Archive.

Their reappearance sparked considerable sensation among the military historians, catalyzing some reinterpretations of the conflict of 1920 (Nowik, 2004, 2010). This interest led to the digitization of the complete archive, comprising over 20 thousand pages, which is now accessible at:

https://wbh.wp.mil.pl/pl/pages/zdigitalizowane-teczki-polskiego-radiowywiadu-wojskowego-z-1920-roku-wpisanego-na-swiatowa-liste-unesco-pamiec-swiata-2020-06-17-kaf5/

In 2018 entire archive of Polish signals intelligence in 1920 has been added to the UNESCO Memory of the World register. This decision finalized recognition of the Battle of Warsaw as one of the decisive battles in the world history and the decisive role of the codebreakers and codebreaking therein.

4 Structure of the archive

Structure of the digitized archive is slightly chaotic and seems to reflect grouping of the documents adopted originally by the codebreakers in 1919/1920. Although the documents have been fully digitized, PDF files comprising the contents of the original folders have been placed in the directories titled after the their names in Polish language, which does not facilitate the research. This section provides brief notes concerning the contents of every directory in the collection. Names of folders in Polish language appear as the subsection titles.

4.1 Depesze nadesłane z Dowództwa Frontu Południowo-Wschodniego, Dowództwa 1 Armii oraz Dowództwa Poleskiej Grupy do Sekcji RTGt

Original Soviet cipher messages (partially deciphered inline) of messages intercepted by the listening stations of Polish South-Eastern Front Command, 1st Army, and Polesie Group (243 pages).

4.2 Depesze szyfrowane z dowództwa armii i frontów przesłane do NDWP

Continuation of the previous directory: Soviet cipher messages (mostly deciphered inline) of messages intercepted by the listening stations of Front and Army commands (329 pages).

4.3 Depesze szyfrowe z Dowództwa 2, 4 i 6 Armii, Grupy Bieniakonie i D.O.K. Lwów

Original Soviet cipher messages (mostly undeciphered) intercepted by the listening stations of 2nd, 4th and 6th Armies, Bieniakonie Group and Lwów Military District (493 pages).

4.4 Depesze szyfrowe ze Stacji RTG. Telegramy nadesłane z dowództwa armii i frontów

Cipher messages intercepted by the listening stations of Army and Front commands; mostly traffic of foreign diplomatic representations in Soviet Russia (Turkey, possibly other countries), Soviet diplomatic traffic (456 pages).

4.5 Dziennik stacji telegraficznej przy Polskiej Misji Wojskowej w Rydze. Szyfrogramy do Stacji RTG nadesłane z Dowództwa 4 Armii

Station log of Polish Military Mission in Riga. Covers the period of the peace talks between Poland and Soviet Russia (227 pages).

4.6 Komplet tłumaczeń szyfrogramów dotyczących oddziałów Armii Czerwonej

Translations into Polish of the deciphered Soviet messages (260 pages).

4.7 Kopie radiotelegramów Naczelnego Dowództwa WP i podległych oddziałów

Directory name suggests the copies of Polish Army HQ messages, however most of its content represents original Soviet cipher messages, partially deciphered (461 pages).

4.8 Korespondencja dla Delegata Łącznikowego 6 Armii, zestawienie dyslokacji nieprzyjacielskiej, zaszyfrowane depesze Oddziału II

Directory name suggests the copies messages by the liaison officer at the 6th Army, enemy's OdB, and cipher messages of Polish 2nd Dept. (Military Intelligence). Most of the content represents the translations into Polish of the broken Soviet messages (XII and XVI Armies) (574 pages).

4.9 Księgi rozwiązanych szyfrów Armii Czerwonej, oddziałów armii gen. Wrangla i gen. Denikina

One of the most interesting parts of the collection; keys to the Soviet, Wrangel's and Denikin's ciphers (485 pages).

4.10 Materiały Biura Szyfrowego-radiogramy szyfrowe i depesze radiowe nadesłane ze Stacji RTG Grudziądz i Toruń

Cipher and coded messages intercepted by the listening stations in Toruń and Grudziądz. Assortment of various ciphers and codes, mostly of diplomatic nature, some open text messages. Message headers suggest diplomatic traffic between Berlin and Moscow (1095 pages).

4.11 Materiały szyfrowe Sekcji Szyfrowej nadesłane ze Stacji RDT Lwów i Toruń

Cipher and coded messages intercepted by the listening stations in Lwów and Toruń. Assortment of various ciphers and codes, mostly of diplomatic nature. Message headers suggest diplomatic traffic between Turkey and Soviet Russia (781 pages).

4.12 Meldunki bolszewickie w tym zestawienie dyslokacji wojsk i wykaz sygnałów radiostacji sowieckich, a także rad

Deciphered and translated Soviet cipher messages, reports regarding dislocation of the Soviet troops based thereupon. Original texts of messages to and from the Soviet diplomatic representation in Warsaw (1159 pages).

4.13 Radiotelegramy dotyczące sytuacji w Rosji bolszewickiej i Anglii, projektowanej pożyczki dla Polski, sytuacji

Open text messages, mostly by news agencies of several European countries (610 pages).

4.14 Radiotelegramy przejęte przez Stację RTG

Open text messages in several languages, mostly diplomatic and news agency (395 pages).

4.15 Radiotelegramy przejęte przez Stację RTG Toruń i Poznań

Open text messages in several languages, mostly of diplomatic and agency nature (606 pages).

4.16 Radiotelegramy Stacji RTG Wilno i Lwów

Open text messages, official releases of the Red Army HQ and Soviet diplomatic sources, relating mostly to operations against Wrangel's and Denikin's forces (689 pages).

4.17 Radiotelegramy szyfrowe oraz depesze szyfrowe do NDWP wysłane z podległych oddziałów

Original Soviet cipher messages (mostly undeciphered) intercepted by various listening stations (820 pages).

4.18 Radiotelegramy zaszyfrowane nadesłane ze Stacji RTG

Soviet cipher messages, most probably in diplomatic code or cipher, addressed to the head of Soviet delegation for the peace talks in Riga (306 pages).

4.19 Radiotelegramy zawierające komunikaty dotyczące sytuacji politycznej i gospodarczej w krajach europejskich

Open text messages in several languages, mostly of diplomatic nature and news agencies (580 pages).

4.20 Radiotelegramy zawierające komunikaty ze Stacji RTG

Open text messages in several languages, mostly diplomatic and news agencies (450 pages).

4.21 Radiotelegramy ze Stacji Radiotelegraficznej RTG Warszawa, Przemyśl i Lwów

Open text messages in several languages, mostly official Soviet diplomatic messages and news agency releases (341 pages).

4.22 Sprawozdania z toczących się spraw w Referacie Śledczym oraz depesze szyfrowe z podległych oddziałów

Original Soviet military cipher messages (some deciphered inline) intercepted by various Polish listening stations (286 pages).

4.23 Sprawy szyfrów i kodów w Naczelnym Dowództwie. Szyfry nieprzyjacielskie

Polish Cipher Bureau's administrative documents (306 pages).

4.24 Sprawy szyfrów i kodów wraz z tłumaczeniem szyfrów

Polish Cipher Bureau's administrative documents, some news agency releases (252 pages).

4.25 Sprawy szyfrów i kodów. Opinia Sekcji Szyfrowej

Polish Cipher Bureau's administrative documents (12 pages).

4.26 Szyfrogramy nadesłane do Oddziału II NDWP z Dowództwa Grupy Południowej i Dowództwa 2 i 3 Armii

Translations of the decrypted Soviet military messages (490 pages).

4.27 Szyfry nadane przez attaché wojskowych

Cipher messages from Polish military attachés in several European countries (907 pages).

4.28 Szyfry nadesłane do NDWP z Grupy Bieniakonie, Ekspozytury MSWojsk, i Dowództwa 2 i 3 Armii

Soviet military cipher messages, mostly deciphered inline and transcribed (669 pages).

4.29 Telegramy dotyczące sytuacji na froncie nadesłane z Dowództwa 3, 6 i 7 Armii, Dowództwa Grupy Poleskiej

Folder name does not reflect its content: open text messages and orders directed from the HQ of Polish intelligence service to various units of Polish Army (446 pages).

4.30 Tłumaczenia nadesłanych szyfrogramów

Translations of Soviet military cipher messages, mostly relating to the critical phase of 1920 campaign directly preceding the Battle of Warsaw (190 pages).

4.31 Tłumaczenia szyfrogramów sowieckich

Translations of Soviet military cipher messages, mostly relating to the critical phase of 1920 campaign, directly preceding the Battle of Warsaw (2.269 pages).

4.32 Tłumaczenia szyfrów przejętych przez Stację RTG Kraków

Open text releases by Rosta (Russian telegraphic news agency) (581 pages).

4.33 Wyciągi z przechowywanych depesz bolszewickich, wykazy ewidencji personelu armii sowieckiej i tłumaczenia szyfrogramów

Translations of broken Soviet messages, mostly from or to the 1st Cavalry Army. Extracts from

various deciphered messages, mostly unrelated to the Polish campaign (Black Sea, Caucasus) (1.217 pages).

4.34 Wykazy depesz szyfrowych nadesłane z Poselstwa Polskiego w Wiedniu i z Dowództwa Frontu gen. Szeptyckiego

Inventory of messages from Polish Military Attaché in Vienna. Soviet messages in various codes and ciphers (384 pages).

4.35 Zaszyfrowane depesze Oddziału II nadesłane przez attaché wojskowych

Messages in cipher from and to Polish military attachés in several European countries and White Russian commands in the South of Russia (294 pages).

4.36 Zaszyfrowane dokumenty i radiotelegramy nadesłane z Dowództwa 7 Armii, Dywizji Legionów i Frontu gen. Szeptyckiego

Soviet coded messages, mostly in 6-letter code and 5-digit codes (329 pages).

4.37 Zaszyfrowane meldunki z podległych oddziałów do NDWP Oddział II

Soviet coded messages, mostly in 6-letter and 5-digit codes (440 pages).

4.38 Zestawienia telegramów wysłanych przez attaché wojskowego w Brukseli do NDWP

Soviet military cipher messages, some deciphered inline (folder name misleading) (175 pages).

5 Basic features of Soviet military ciphers of 1920 campaign

Discussed archive contains examples of many codes and ciphers used in the period of 1919-1920 by several European and non-European countries. It was natural that Polish signals intelligence was heavily focused on the Soviet Russia, representing the most serious threat to Poland's freshly regained independence.

The archive contains many examples of Soviet codes and ciphers, both military and diplomatic. It seems that Polish codebreakers have not undertaken a serious attack at the Soviet diplomatic codes. After all, the codes became important only after the victory, but considering the scale of the Soviet defeat in war against Poland and Bolsheviks' problems in other parts of their nascent empire stimulated the peace talks in Riga, reducing the need for the codebreaking. Therefore Soviet military ciphers, and their solutions, represent much more interesting part of the archive.

Most Soviet military messages of the period were transmitted in numeric groups, each consisting of 5 digits. In their basic form virtually all ciphers were representing a monoalphabetic substitution based on Polybius square extended to 10x10 fields (Fig. 1).

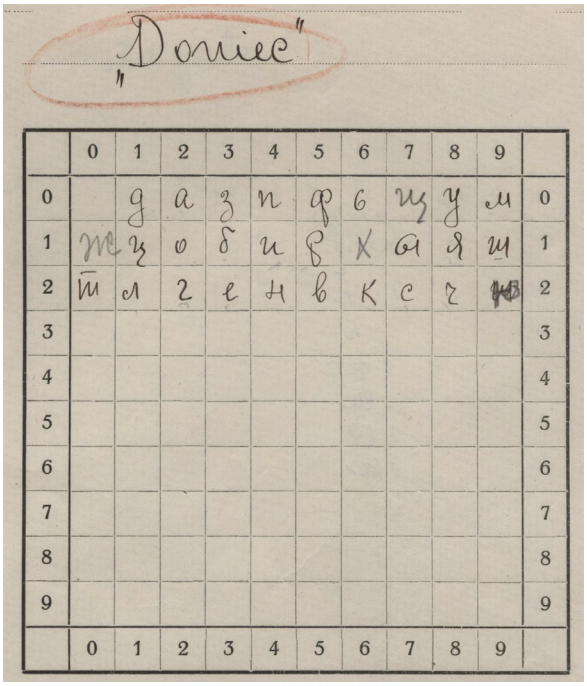

Figure 1. Key "*Donets*"

In spite of their construction permitting many homophones, only some cipher keys were using them, "Boievoi" (Fig. 2) being one of their examples.

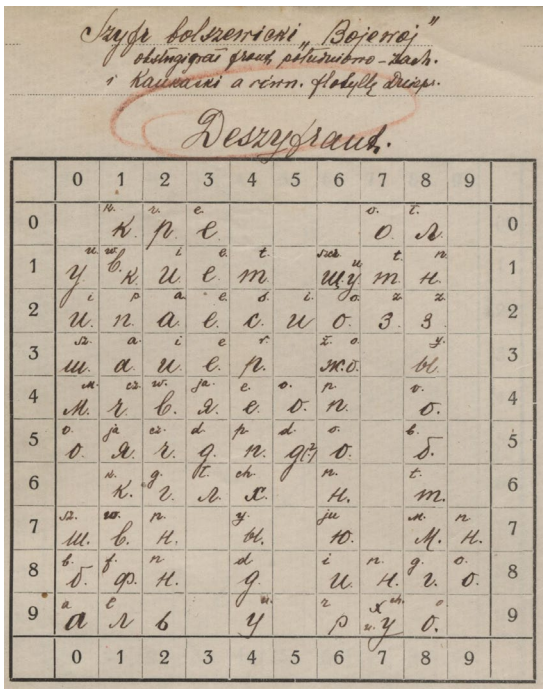

Figure 2. Key *"Boievoi"*

Some cipher keys took syllabic nature, where pair of digits represented single letters and/or their pairs, key "Vintovka/Molot" being a good example of this group (Fig.3).

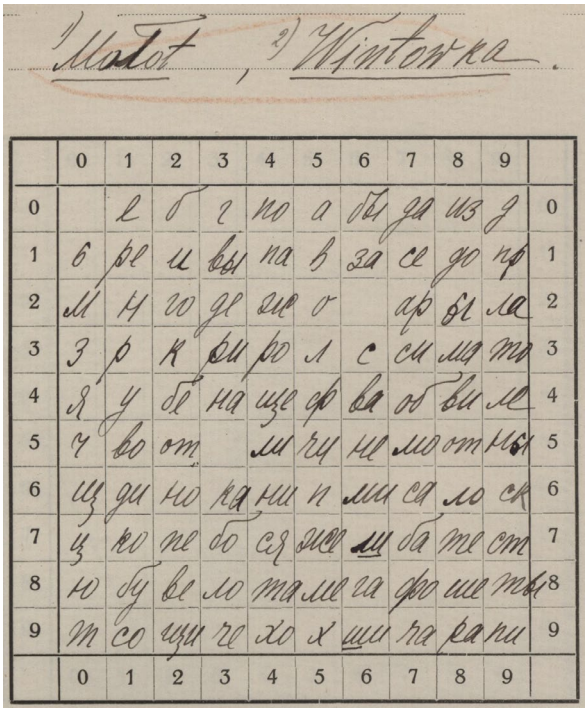

Figure 3. Key *"Vintovka/Molot"*

In the simplest scenario, when no superencipherment was used, result of the character substitution was simply combined into 5-digit groups and transmitted in this form. However, many keys were using additional layer of protection, inserting dummy digits into every group. In the simplest case a dummy digit was inserted into the constant (usually middle) position of the group. In more elaborate examples dummy digits were not only changing their positions, but were used to transform the pairs of digits representing letters within the same group. For example, in the cipher key "Сюртук" (frock coat) dummy digit was inserted in the first position of the first group, second position of the second, and so on until the fifth group. Moreover, the value of the dummy digit was subtracted (arithmetically) from both pairs representing the letters in a given group.

Most keys were utilizing superencipherment in a rather basic form. After the open text has been transformed into the numerical groups using the Polybius square, a superencipherment key was added or subtracted (without carry or borrow). Superencipherment key usually represented a number from three to six digits long used twice; in its normal and then reverse order. For instance the basic superencipherment factor for "Centralnyi" key was 234571, but was used as a sequence of 234571175432.

In some keys an additional transposition layer was added in the form of switching the positions of digits within a group.

Cipher elements described above were combined in the real keys in various scope, resulting in a variety of ciphers ranging from the basic monoalphabetic substitution to more elaborate examples, combining substitution with transposition and superencipherment.

6 Some Soviet crypto blunders

Most probably the largest Soviet blunder facilitating Kowalewski's and his section's job was having lost one of their keys, using most common features, to the enemy. According to Kowalewski's notes at the margins of "Delegate" key (Fig.4) he has broken the key cryptanalytically, but its copy had been also seized by Polish intelligence service.

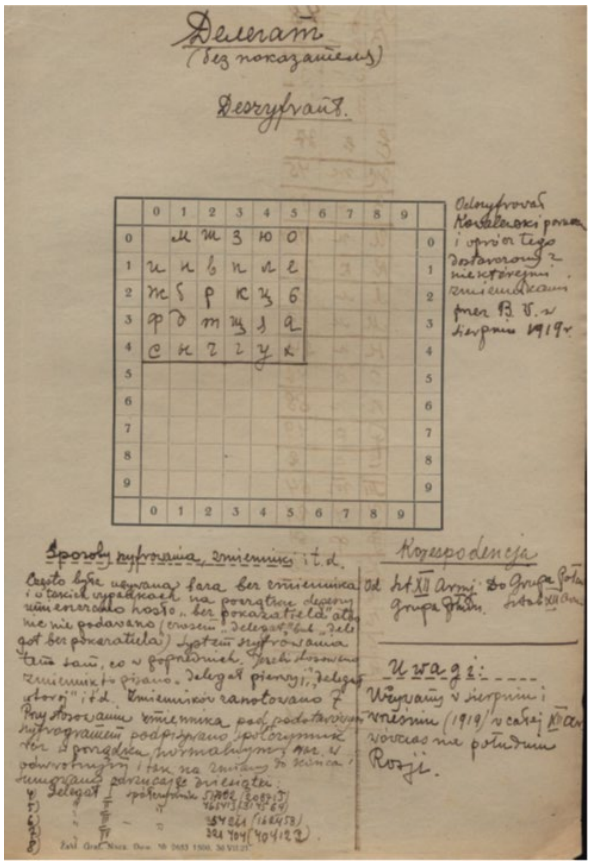

Figure 4. Key *"Delegate"*

This key represented a good example of the principles of cipher construction and Soviet cipher procedures.

Some other blunders, of a more conceptual nature, included:

- frequent use of a monoalphabetic substitution without any other form of complexity,
- generating new key tables using the circular shifts of the old ones,
- making only a half of the superencipherment key independent and reusing it in the reverse order,
- frequent reuse of the same superencipherment key by various keys,
- transmitting the reference to the superencipherment key in open text,
- even number of digits in both letter representation and superencipherment resulting in auto resynchronization of both streams,
- inserting punctuation in open text into the cipher messages and restarting the superencipherment from every punctuation mark, facilitating setting the message parts in depth,
- extensive use of the Soviet military jargon ("komdiv" - officer commanding the division, "kavkor" – cavalry corps, etc.) providing reliable cribs.

All of these blunders, and some more, were used by Polish codebreakers with good effect. Desperate state of the army and the country in the summer of 1920, and the sudden reversal of fortunes during the Battle at the Vistula river caused Polish victory to be traditionally described as the "Miracle at the Vistula". Now, that we are all able to access and study the digitized archives of Polish codebreaking service, we have to admit there was nothing supernatural in Polish victory. The newly established codebreaking service of Polish Army provided a solid foundation for the victory. Polish soldiers and their commanders managed to make good use of this advantage. And the role of the mathematicians in this cryptologic adventure provided foundations for the future triumph of Polish Cipher Bureau over Enigma.

References

Davies Norman. 2003 (1972). *White Eagle, Red Star: the Polish-Soviet War, 1919–20* (New ed.). New York.

Nowik Grzegorz. 2004. *Zanim złamano Enigmę*, Warszawa.

Nowik Grzegorz. 2010. *Zanim złamano „Enigmę" rozszyfrowano Rewolucję. Polski radiowywiad podczas wojny z bolszewicką Rosją 1918–1920,* Warszawa.

Reile Oskar. 1963. *Geheime Ostfront. Die deutsche Abwehr 1921–1945, München/Wels.*

Wyżeł-Ścieżyński Mieczysław. 1928. *Radiotelegrafia jako źródło informacji o nieprzyjacielu,* Przemyśl.

Zamoyski Adam. 2008. *Warsaw 1920: Lenin's Failed Conquest of Europe*, UK.