Cryptology in the Slovak State During WWII

Eugen Antal
Slovak University of Technology in Bratislava
Slovakia
eugen.antal@stuba.sk

Pavol Zajac
Slovak University of Technology in Bratislava
Slovakia
pavol.zajac@stuba.sk

Otokar Grošek
Slovak University of Technology in Bratislava
Slovakia
otokar.grosek@stuba.sk

Abstract

We explore the up-to now unknown details of the history of cryptology in Slovakia found in Slovak archives. This contribution focuses on cryptology of the Slovak State, which was a German puppet state during WW2. We identify three main types of ciphers in use. Firstly, ciphers from the former Czechoslovakia were adopted. During main military campaigns, the ciphers were mostly dictated by Germany. Finally, we describe a series of hand ciphers A-x specifically designed in Slovakia, mostly for internal use.

1 Introduction

The territory of modern Slovakia was for a long time a part of the Kingdom of Hungary. After the proclamation of the first Czechoslovak Republic on October 28, 1918, it has become a part of the new republic. A good overview of the situation of cryptology in the former Czechoslovakia is given by Š. Porubský in (Porubský, 2017).

On March 14, 1939, a separate Slovak State was created as a puppet state of the Nazi Germany. Czech territory was directly absorbed by Germany as a Protectorate. Former representatives of Czechoslovakia escaped to France, and later to the UK, to form the foreign resistance. Top intelligence officers of Czechoslovakia managed to escape to London along with intelligence files. However, the cryptology in Czechoslovakia, and later in London resistance movement was very weak, as it is demonstrated in books written by J. Janeček (Janeček, 1998; Janeček, 2001; Janeček, 2008), as well as in Cigáň's manuscript analysed by Š. Porubský (Porubský, 2017). Communications with the exile movement played an important role during the anti-nazi Slovak National Uprising that started in August 1944. The situation with exile movement was complicated by cooperation with communist exile, which was connected to the Soviet Union, and partisan movement.

While the state of cryptology and secret communications of the exile government of Czechoslovakia are relatively well-known, as far as we know, the situation of the cryptography during the Slovak State was not studied in details yet. As mentioned, the Slovak State was a puppet state, and ally of Nazi Germany. The Slovak State declared war against German enemies, including the USA (curiously, there was never a peace treaty signed, because the Slovak State was not recognized in the aftermath of war). Slovak Army participated in military campaigns against Poland in 1939, and against the Soviet Union. In June 1944 remnants of the two Slovak divisions were disarmed due to low morale, and possibly due to mistrust by German command.

In our contribution we present some of cryptologic facts uncovered in the Military History Archive (part of the Institute of Military History established by the Ministry of Defence of the Slovak Republic). We want to clear a common misconception that the Slovak State cryptology was only directly dictated by Germany. We show some of the means of the cryptologic cooperation between German and Slovak armies, as well as some specific ciphers developed in Slovakia during WWII.

2 At the beginning of the war

In June 1939, the MNO - "Ministerstvo národnej obrany" (Ministry of National Defence) ordered the subordinate headquarters to report the list of officers with a cryptologic training. One month later it was ordered to report all the available ciphers and cryptographic directives. The goal of the ministry was to review the current state of secrecy in the newly established Slovak State.

From these reports we can conclude that the

Proceedings of the 2nd International Conference on Historical Cryptology, pages 23-30
Mons, Belgium, 23-26 June, 2019

available ciphers (and codes) belong to the pre-war era, namely:

- code "ZSD",
- hand-cipher "Q" (also called as key "Q"),
- cipher-machine (without any name in the archival documents).

All these ciphers (and codes) have been used before the war by the Czechoslovakian army[1]. We were unable to find any document mentioning the cipher-machine's name, but based on (Šklíba, 2007- 5; Šklíba, 2007- 7/8), only the ŠTOLBA cipher-machine was in use before 1938[2].

The encryption service was reopened on 15th of July, 1939 - reusing the available ciphers. The hand-cipher "Q" was selected as the main cipher system. The document "Spojovací rozkaz č. 1" (Communication directive no. 1) from August 1939[3] was an order to encrypt all internal radio-telegraphic messages using this cipher. In the same month, on the 15th of August, 1939, the use of available cipher-machines was also (re)started. Document called *G-VII-8* named "šifrování" (encryption) was the main cryptographic directive in use with attachments describing the cipher systems such as the key "Q".

The available materials and directives show only internal use of these ciphers. Unfortunately it's not known, whether these ciphers were also used in a communication with the allies. This hand-cipher "Q" with the cipher-machine was still in use in December 1942, and the keys and passwords were distributed at least up to April 1943[4]. The daily keys for the cipher-machine were distributed for the whole year of 1943.

The *G-VII-8* was extended in 1943 with directives from Germany (without changing the name of the document). At this time the Slovak State also adapted some German ciphers including the Enigma - as described in the next section.

[1]Document 20.800/Taj.3.odd.1939 in (Military History Archive in Bratislava, 2019), fund KVV, box n. 2.

[2]ŠTOLBA is a cipher-machine with 6 main rotors and with 3 rotors controlling the rotor stepping. The daily keys distributed in 1939 for the "cipher-machine" also contains a 3 letter word and a 6 letter word.

[3]Document k. č. 77/39/Taj.3.odd.1939 in (Military History Archive in Bratislava, 2019), fund MNO tajné, box n. 2.

[4]Document 404621/Taj.obr.1942 in (Military History Archive in Bratislava, 2019), fund 53 (53-88/1-19).

3 Ciphers from Germany

> "...The encryption is performed by the commander of the division using a cipher-machine. ... The cipher-machine is a box of dimension appr. 40x50 cm. The machine has keys like the typewriter and letters that lights during the encryption. The encryption is enabled by a 3-wheel system...
> Created in Germany (Berlin)."[5]

In September 1942 Ján Morvic completed a signal corps training in Germany (Nachrichtenschule, Halle). One part of the course was about secrecy, describing the German Enigma (without mentioning the name of equipment in the report).

In March 1943, an encryption training was designed[6] to learn the German hand-ciphers and the cipher-machine.

In April 1943, a new document called "návod k šifrovaniu" (manual of encryption) was created[7]. This document contained a description and instructions for two German hand-ciphers NS42[8] and TS42a[9] - introducing the German ciphers to the Slovak State departments.

Germany also gave an order[10] to unify the encryption among the allies. The Slovak State received directives for translation, extending the existing crypto-directive *G-VII-8*. The new directive consisted of four parts:

- general encryption rules (H.Dv.g.7) as G-VII-8-a,
- instructions to the "Enigma" (H.Dv.g.13, H.Dv.g.14) as G-VII-8-b,
- instructions to NS42 as G-VII-8-d,
- instructions to TS42a as G-VII-8-c.

When the German ciphers were in use, the daily keys were distributed monthly. There were 2 types of Enigma keys:

[5]Document 83375/spoj.2.1942 in (Military History Archive in Bratislava, 2019), fund MNO tajné, box n. 18.

[6]Telegram from 24. III. 1944 as an attachment to 2879/Dov.3./6.1944 in (Military History Archive in Bratislava, 2019), fund MNO dôverné, box n. 475.

[7]Document 7.632/Taj.3.odd.1943 in (Military History Archive in Bratislava, 2019), fund RD, box n. 45.

[8]Gen.StdH/Chef HNW IV.89 b 30 Nr.7.370/42.

[9]Gen.StdH/Chef HNW IV.89 b 30 Nr.7.360/42.

[10]Höherer Wehrmacht - Nachrichtenführer Mittelost Nr. 2241/geh.1942 referring to Gen.StdH/Chef HNW IV Nr. 8537/42.g.v.10.1942.

- marked as "Slovensko" (Slovakia) - to be used in the country,
- to be used with the allies.

The NS42 keys were distributed alongside with the TS42a, where the TS42a was designed to replace the NS42 in case of offensive army movement.

The knowledge of German ciphers among the Slovak signal corps officers wasn't on the required level, so there was an effort to train the staff to use these ciphers[11].

4 Design of a Slovak cipher

The Slovak State started the war with the available Czechoslovakian ciphers. Before adapting German ciphers and directives, the Slovak State developed own ciphers (called "A-2") for internal use. Note, that the cipher development was still overseen by Germany.

A new cipher called **"A-2"** was firstly introduced in May 1940. The cipher was described as a complicated transposition designed to encrypt $50 - 600$ letters in a case of less-important radiograms. After the first distribution, all headquarters were asked to encrypt some radiograms with this cipher, and to send them to a corresponding place for the analysis[12]. The received reports describe the cipher as a practical, fast and secure enough[13]. It was also tested by the OKW Berlin. OKW Berlin allowed to use (see Figure 1, the stamp "Tajné" means "Secret") this cipher.

But the use of this cipher wasn't always without problems. Due to a large amount of errors made by encryption officers, it was ordered to re-train the use of the "A-2" cipher.

In 1941 a new directive for the encrypted communication was implemented replacing the previous one. Based on the directive, it was allowed to use only "A-2", the cipher-machine and the "ZSD" code. Most of the departments and battalions were allowed to use the "A-2" cipher only[14].

Later on, in 1943, after the German ciphers were adapted, the Slovak one was still in use and trained alongside with the German hand-ciphers and the cipher-machine[15].

During the WW2 years, several upgrades/versions were created, the known versions are from "A-2" up to "A-5". The main contributor on the development was Michal Kmeťo-Dovina[16].

4.1 M. Kmeťo-Dovina

Michal Kmeťo-Dovina was the commander of the "hlavná voj. radiostanica MNO" (the main military radio-station of the Ministry of National Defence) and later on from 1943 worked as an encryption officer of second department of the Ministry of National Defence (VHU, 2013). He completed a cryptographic course "Písemné kursy kryptografie"[17] before WWII in 1938 - with a good score.

Due to a lack of officers experienced with encryption, in 1940, a creation of an encryption course was ordered. One of the instructors from this course was Michal Kmeťo-Dovina[18].

During the Slovak National Uprising (SNP), Kmeťo-Dovina was helping the anti-nazi movement, keeping communication channels and developing new encryption system for the Uprising and later guerrilla fighters (VHU, 2013). From the available documents, it is not clear whether the development of the specific Slovak cryptographic systems was a part of the Uprising preparations. However, the cryptography during SNP is a very large and specific topic that is out of the scope of this article.

5 The "A-x" hand-cipher

The "A-2" hand-cipher was developed as a first cipher from the "A-x" series. The cipher was updated several times during the years. Versions "A-2" and "A-3" consisting of 4 tables, and "A-4" consisting of 2 tables. We don't have detailed information about the other versions.

The "A-2" is a transposition cipher, designed to encrypt less important messages of length up to 600 letters. Main transposition was defined by a

[11] Document 2823/dov.spoj.1944 in (Military History Archive in Bratislava, 2019), fund MNO dôverné, box n. 475.

[12] Document 156.458/9.1940 in (Military History Archive in Bratislava, 2019), fund MNO dôverné, box n. 34.

[13] Document 135.992-II/9.Taj.1940 in (Military History Archive in Bratislava, 2019), fund MNO dôverné, box n. 34.

[14] Document 30.196/Taj.spoj.1941 in (Military History Archive in Bratislava, 2019), fund 55 (55-27-5).

[15] Telegram from 24. III. 1944 as an attachment to 2879/Dov.3./6.1944 in (Military History Archive in Bratislava, 2019), fund MNO dôverné, box n. 475.

[16] Documents 173.074/Taj.spoj.1941, 592/Taj.spoj.1941 and 22/Taj.1941 in (Military History Archive in Bratislava, 2019), fund MNO tajné, box n. 10.

[17] Document 151332/-II/9.1940 in (Military History Archive in Bratislava, 2019), fund MNO dôverné, box n. 57.

[18] Document 151332/-II/9.1940 in (Military History Archive in Bratislava, 2019), fund MNO dôverné, box n. 57.

series of secret tables, and each message had also a specific message key. It was forbidden to encrypt text of length under 50 letters. Each table has four logical sides — two are printed on the front page (the second one is upside-down version of the same page), and two on the back page. The logical side and the table's identification is marked with a red and black color on each side as *side/table*, later on in "A-4" this was flipped to *table/side*.

On each side, in the first row (header) of the table are two strings:

1. table identificator: 13 letters (unique for each table),
2. side identificator: 6 or 7 letters (different for each side).

The rows of the table are also labelled with one or two letters from the alphabet. Before encrypting a message, the message key is constructed from the letters identifying the order of tables, pages and starting positions within pages.

Before encrypting a message, several rules[19] were defined how to pre-process the input text:

1. Replace:
   - . with *X*,
   - *:* with *XX*,
   - *,* with *QW*,
   - . (full stop) with *XW*.
2. Write special characters with a full name, such as:
   - *"* as *UVODZOVKY* (*quotation mark*),
   - *(* as *ZÁTVORKA* (*parenthesis*).
3. Write numbers with a full name, divided to digits:
   - *14* as *JEDNA ŠTYRI* (*one four*).
4. Replace accent, like:
   - *á* with *AA*,
   - *č* with *CV*.
5. When an accent is removed from a name, a letter *Q* should be put after this name.
6. When the text does not divide the number *5* a padding should be used (no longer as 4 letters) using some of the *QXW* letters or using the "*STOP*" word.

[19]Document 164/Taj.spoj.1941 in (Military History Archive in Bratislava, 2019), fund MNO tajné, box n. 10.

The cipher "A-2" had 4 tables. Later on, in version "A-4", this was reduced to only 2 tables. As "A-4" encryption mechanism is otherwise the same as "A-2", for the sake of simplicity, we will continue the description with "A-4" procedure. In Figure 2 we show one of the pages showing two sides of one table.

To start an encryption, sender of the group created a message key called "skupina oznamovateľa" (*sender group*), consisting of 5+5 letters. He selected

1. the order of the tables,
2. the order of the four available sides for each table,
3. the offset (row identificator), defining where to start writing the text,

and encoded his selection as a group of first 5 letters. The first letter of this group contains a randomly chosen letter from the identificator label of the first selected table, and the remaining four letters are randomly chosen letters from the labels of the sides (in the corresponding order). During the encryption, after the four sides of the first selected table were used, the encryption would automatically continue with the remaining table. The second 5 letters were used to encode the row-offset identificator, and then the order of the sides of the second table.

As an example (using the Figure 2), we can choose to start with the table marked 2. We select randomly one letter from the selected table identificator string "RKGJXDOQHFVB". If we want to start the encryption from side 2 (marked 2/2), we select randomly one letter from the side identificator "JLIXZA". Next we choose the side 1 (marked 2/1) as the second side, selecting a letter from "CURKTG", and so on.

The encryption table itself consists of small rectangles forming a matrix, where some of the cells are cut off. This is essentially a variant of the Fleissner grille. Each table realizes multiple 5×5 grilles in parallel, randomized by a message key.

The plain-text letters are filled into these cells based on the message key. The text is written in an order defined by the red arrow painted on the corresponding side. On every side, we start to fill the first available (cut off) cell on the row labelled with the chosen row identificator. It is necessary to note, that in case of a shorter text, only a part

of the matrix is used (not ending on the last free cell). The encryption grille was designed to automatically form five letter groups of the encrypted text. On each side, there are columns labelled with numbers. Since the first row is known, we can save the last number from the previous row. If we add the plain text length (after the pre-processing) to this number, we obtain the position of the final cell.

To continue in our example, we choose the row offset "Q" (starting in the seventh row). The last number from the previous row is 180 (red color). Suppose the text length to be 50 letters long. Our ending position will be $180+50=230$, so we cannot use cells after this position.

The decryption is straightforward, using the same order of tables, sides and using the same cell range.

For the interested reader, we include an example of the encrypted telegram (Figure 3), with the following transcript:

```
VVXKW QUKQW
PZJXY AVTQA ZVRPO DAOSV PLLQA XIMVS
UOLNT IURTC DVEAL ATSNE WPDSE EUOPU
LSOTR OYKOJ UAOXV ECDTQ AKXLS JSSPD
SCAXR VPEAI RVIOT UOXAO SXNRK ESAPU
```

Acknowledgments

This work was partially supported by grant VEGA 1/0159/17.

References

Military History Archive in Bratislava (Vojenský historický archív v Bratislave).

Jiří Janeček. *Gentlemani (ne)čtou cizí dopisy* (in Czech). 1998. Books - bonus A. ISBN:8072420232.

Jiří Janeček. *Válka šifer* (in Czech). 2001. Votobia. ISBN:8071985058.

Jiří Janeček. Rozluštěná tajemství (in Czech). 2008. XYZ. ISBN:8086864545.

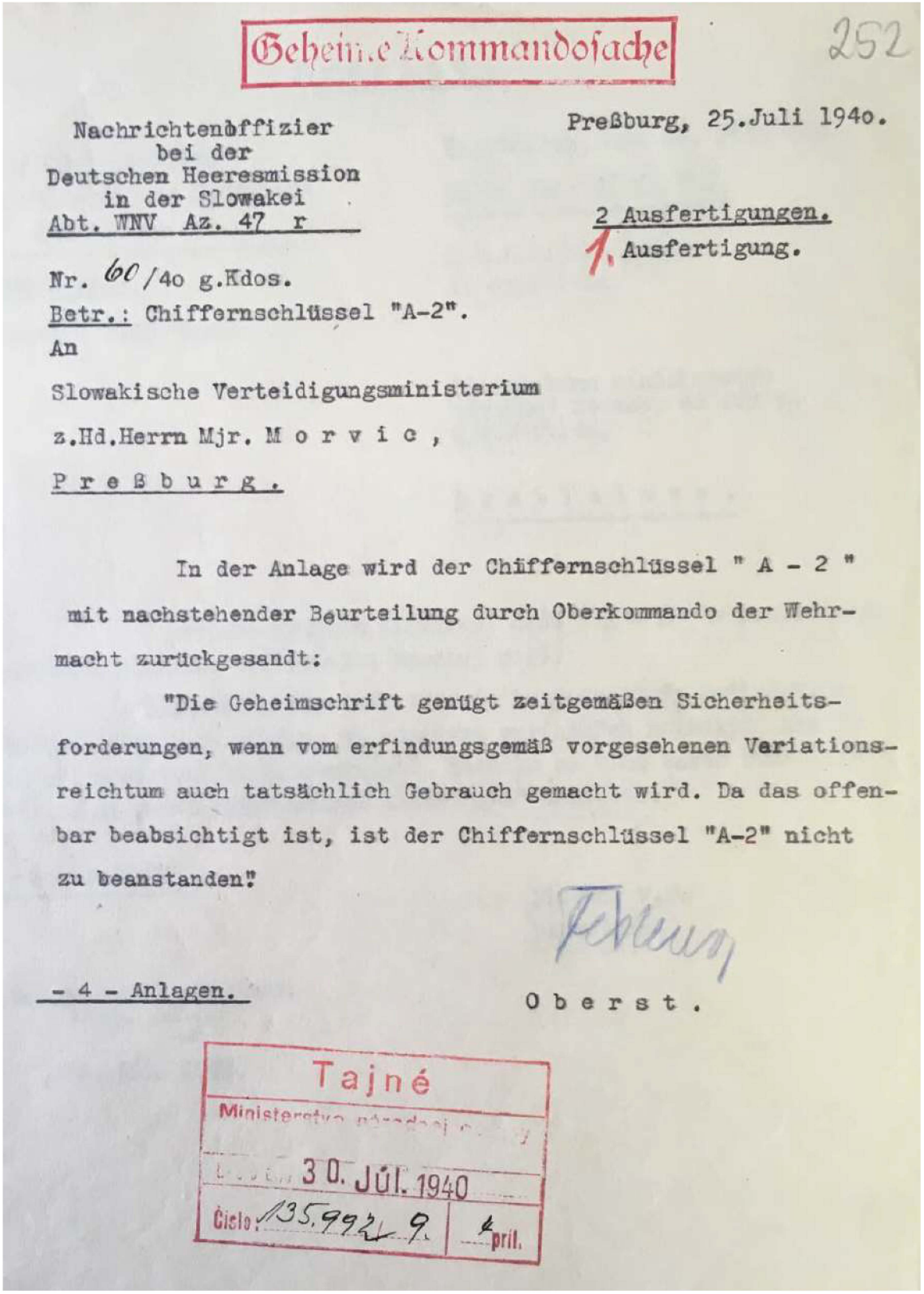
Štefan Porubský. Application and Misapplication of the Czechoslovak STP Cipher During WWII. 2017. *Tatra Mountains Mathematical Publications*, 70(1):41–91.

Karel Šklíba. Z dějin československé kryptografie, část I.,. Československý šifrátor MAGDA (in Czech). 2007. *Crypto-World*, (5).

Karel Šklíba. Z dějin československé kryptografie, část II.,. Československý šifrovacie stroje z období 1930-1939 a 1945-1955 (in Czech). 2007. *Crypto-World*, (7/8).

František Cséfalvay et al. 2013. *Vojenské osobnosti dejín Slovenska 1939-1945* (in Slovak). Vojenský historický ústav Bratislava. ISBN:9758089523207.

Appendices



Geheime Kommandosache

252

Nachrichtenoffizier
bei der
Deutschen Heeresmission
in der Slowakei
Abt. WNV Az. 47 r

Preßburg, 25.Juli 1940.

2 Ausfertigungen.
1. Ausfertigung.

Nr. 60/40 g.Kdos.
Betr.: Chiffernschlüssel "A-2".
An
Slowakische Verteidigungsministerium
z.Hd.Herrn Mjr. M o r v i c ,
P r e ß b u r g .

In der Anlage wird der Chiffernschlüssel " A - 2 " mit nachstehender Beurteilung durch Oberkommando der Wehrmacht zurückgesandt:

"Die Geheimschrift genügt zeitgemäßen Sicherheitsforderungen, wenn vom erfindungsgemäß vorgesehenen Variationsreichtum auch tatsächlich Gebrauch gemacht wird. Da das offenbar beabsichtigt ist, ist der Chiffernschlüssel "A-2" nicht zu beanstanden."

- 4 - Anlagen.

O b e r s t .

Tajné
Ministerstvo národnej [illegible]
30. JÚL. 1940
Číslo: 135.992/9. 4 príl.

Figure 1: Report of the ”A-2” from the OKW Berlin - in (Military History Archive in Bratislava, 2019), fund MNO dôverné, box n. 34.

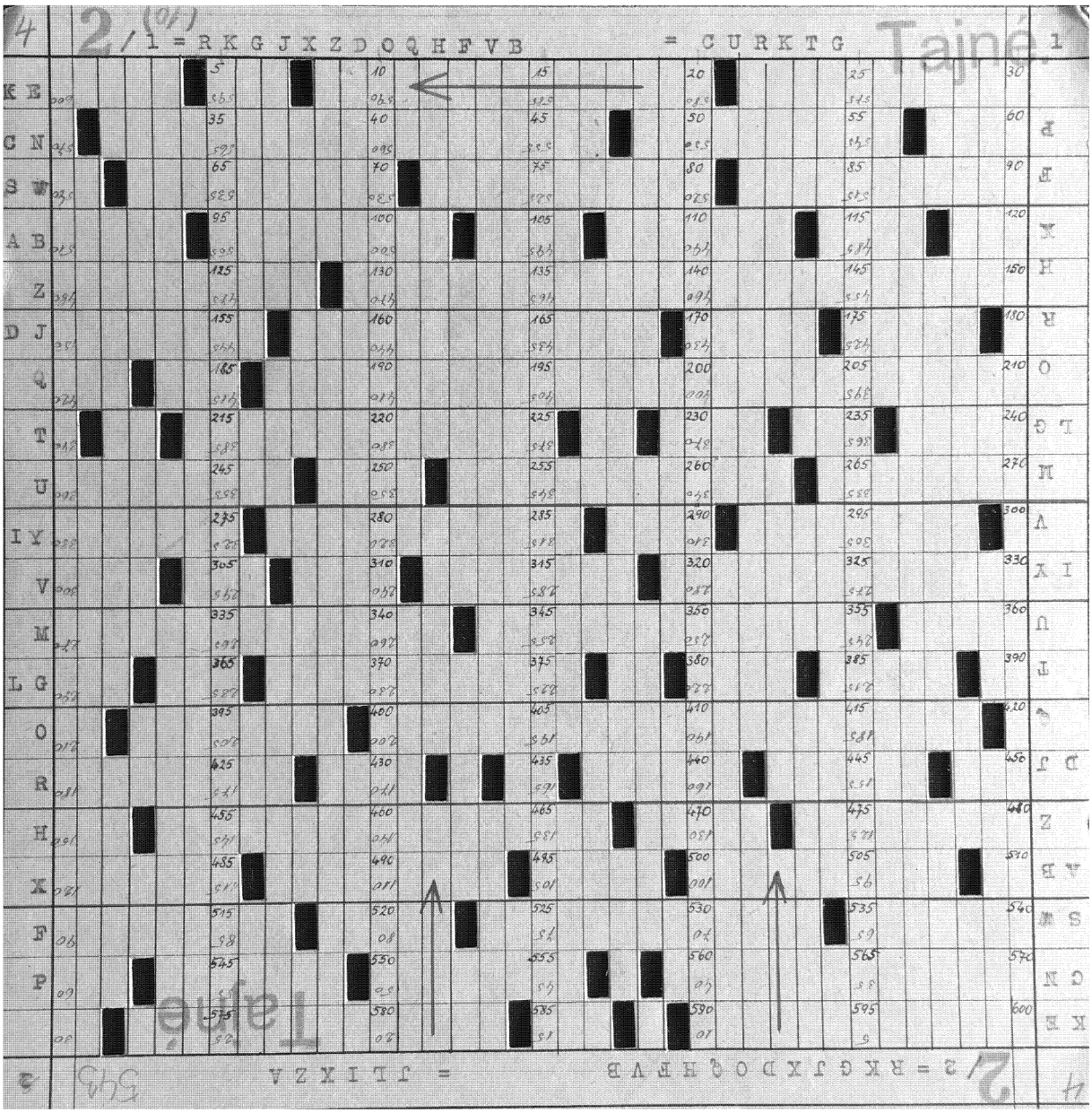


Figure 2: The ”A-4” hand cipher (Table 2, sides 1 and 2) - in (Military History Archive in Bratislava, 2019), fund MNO tajné, box n. 10.

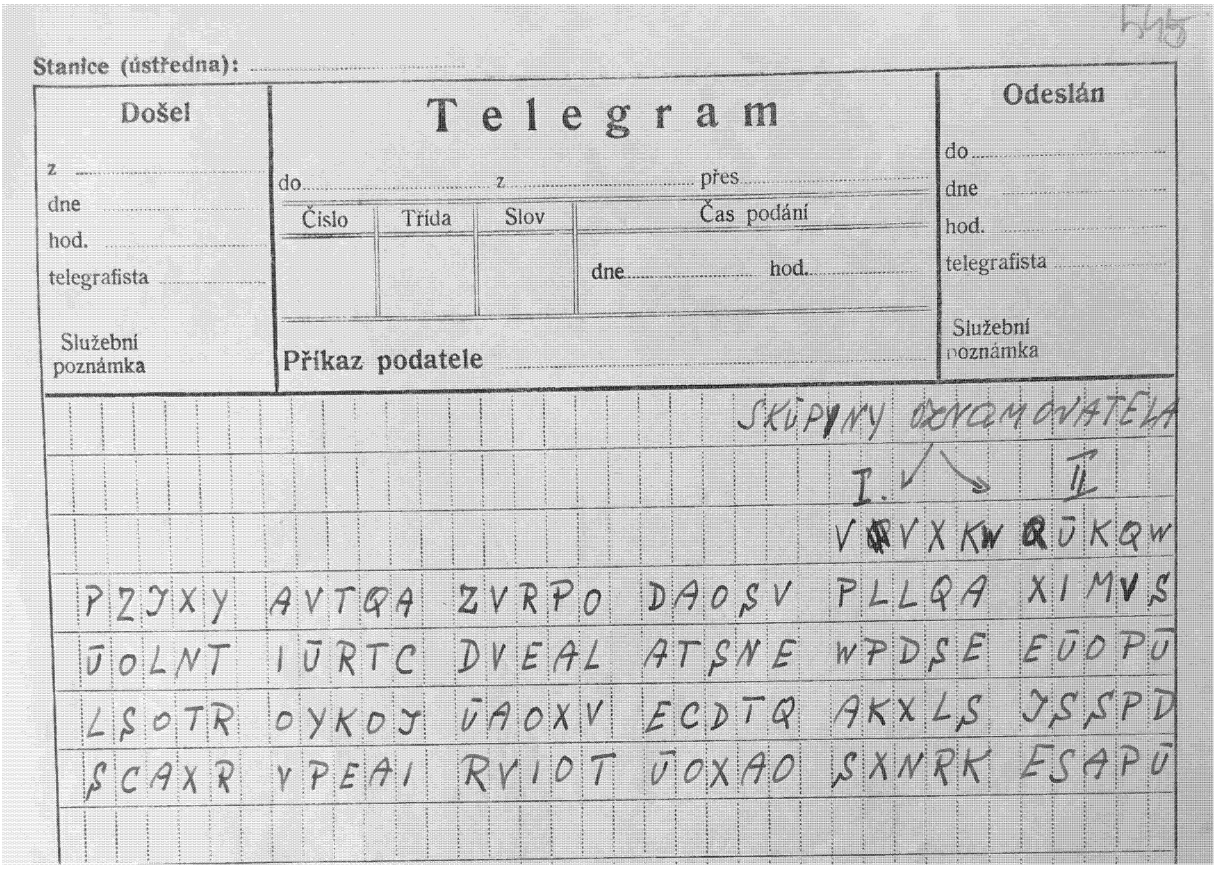


Figure 3: Text encrypted with the ”A-4” hand cipher - in (Military History Archive in Bratislava, 2019), fund MNO tajné, box n. 10.