Diplomatic Ciphers Used by Slovak Attaché During the WW2

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

Slovakia was an allied (puppet) state of Germany during WW2. In various Slovak and Czech archives, we found previously unknown details about diplomatic ciphers used by the Ministry of Foreign Affairs during WW2 in Slovakia. Here we present cipher systems used by Slovak Attaché and give insight into the encryption problems of the Ministry and embassies.

1 Introduction

After the Munich agreement (September 30, 1938), Czechoslovakia was betrayed by her allies and Germany invaded first the Sudeten region, and then Bohemia and Moravia. Former representatives of Czechoslovakia escaped to the UK and organized foreign resistance. In March 1939 a separate Slovak State (Slovakia)[1] was created as a puppet state of the Nazi Germany. The Czech territory was directly absorbed by Germany as a Protectorate.

Cryptology was changing separately in Slovakia and in the Czechoslovakian Government in Exile. We can separate the ciphers used in Slovakia, to *military ciphers*, used by the army[2] and to *diplomatic ciphers* used by the Ministry of Foreign Affairs. In this paper, we focus on the diplomatic ciphers used during the war and their connection to military ciphers. Ciphers, used by the Czechoslovakian Government in Exile, are not covered by this article[3].

We also introduce a special type of transposition cipher - a *triple columnar transposition*. As far as we know, there is no information about usage of that kind of transposition in any other country during the WW2.

Presented facts are based on archival documents uncovered in the Military History Archive in Bratislava, Slovak National Archive in Bratislava, Central Military Archives in Prague and in the Security Services Archive in Prague.

2 Ciphers Used by the Ministry of Foreign Affairs

The Ministry of Foreign Affairs (Ministerstvo zahraničných vecí - MZV) was completed in 1941 and consisted of four departments. Slovakia had embassies in Berlin, Bern, Budapest, Bucharest, Madrid, Moscow, Rome, Sofia, Warsaw, Vatican, Zagreb and later in Helsinki. Slovak consulates were in Belgrade, Milan, Prague, Stockholm and Vienna.

In diplomatic correspondence, different[4] ciphers were used than those used by the army. The cryptology was a part of the first department and second division of the Ministry (Bielik et al., 1965). The importance of using encrypted telegrams was stressed in a circular letter[5] sent to all foreign representative offices already in 1939.

In the documents we found, the following cipher names were mentioned:

- Hand ciphers: *C*, *XQ*, *R*;
- Cipher machines: Cipher machine[6], *K*, *Kryha*, *SVERK*.

In the following subsections we briefly introduce the used ciphers (see Figures 6 and 7 for encrypted telegram examples).

[1] The Slovak State name was officially used between March 14 and July 21, 1939. In July 21, 1939 the Slovak State was declared as a republic and renamed to Slovak Republic. The Slovakia acronym was also in use.

[2] Overview of the Slovak military ciphers used during the WW2 can be found in (Antal et al., 2019).

[3] See (Janeček, 1998; Janeček, 2001; Janeček, 2008; Porubský, 2017) for more details.

[4] Except of 10 cipher machines borrowed from the Ministry of National Defence.

[5] Document n. 1882/39 in (Slovak National Archive in Bratislava, 2020), f. MZV, box n. 42.

[6] Without mentioning a name, borrowed from the Ministry of National Defence.

2.1 Cipher *C*

The most simple cipher in use by the Ministry of Foreign Affairs was a monoalphabetic substitution called *C*. It was used[7] usually alongside with ciphers K and R. The plain text letters were encrypted in a reversed order (starting from the last letter) and arranged into five letter groups.

A special header was inserted before the encrypted telegram. Firstly a capital letter "C" in a combination with a randomly chosen second letter, then the date, and finally the number of letters of the telegram. Additionally the number of the document was inserted after the telegram.

The weakness of such a primitive cipher was recognized and therefore in the official directive it was only allowed to encrypt less important messages. However, some embassies used only *C* during the first years of the war[8]. In Madrid, the *C* was replaced with a stronger cipher[9] *R* only in 1941. Later on, in April 1942, the Ministry of Foreign Affairs decided to stop distribution of new passwords for *C* due to it's weakness[10].

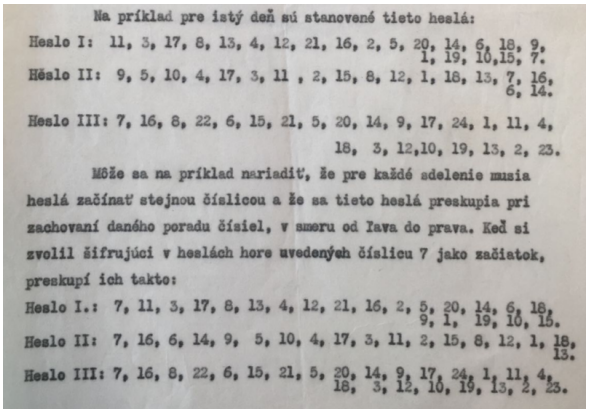
2.2 Ciphers *XQ* and *R*

More powerful hand ciphers were used by the Ministry of Foreign Affairs - a triple columnar transposition called *XQ* and *R*. Based on the available manuals, both names stands for the same cipher[11]. Our opinion is that notation *XQ* means "extended/extra Q", as the Ministry of National Defence used a double transposition cipher called *Q* as a main hand cipher (Antal et al., 2019). The notation *XQ* was later on changed[12] to *R*.

This kind of transposition was used by all embassies and consulates where an encryption service was available[13].

The triple columnar transposition is an encryption system where three columnar transpositions are applied in a cascade. These ciphers were designed to encrypt messages of length from 50 letters up to 200 for *XQ*, and up to 250 for *R*, respectively. All three transpositions were defined by a specific password (permutation). For *XQ* the password length was limited between 16 and 28, in case of *R* between 16 and 22 [14].

Each password was valid for 24 hours. To avoid encryption with the same password during the day a special alignment technique was used ("usmerniť" and "preskupiť" in original). A simple arrangement could be a rotation of all three permutations until they start with the same number (see Figure 1 - permutations arranged to start with number 7). Another option was to arrange the first permutation to a number n, the second shifted by one to $n+1$, etc.


Na príklad pre istý deň sú stanovené tieto heslá:

Heslo I: 11, 3, 17, 8, 13, 4, 12, 21, 16, 2, 5, 20, 14, 6, 18, 9, 1, 19, 10, 15, 7.

Heslo II: 9, 5, 10, 4, 17, 3, 11, 2, 15, 8, 12, 1, 16, 13, 7, 16, 6, 14.

Heslo III: 7, 16, 8, 22, 6, 15, 21, 5, 20, 14, 9, 17, 24, 1, 11, 4, 18, 3, 12, 10, 19, 13, 2, 23.

Môže sa na príklad nariadiť, že pre každé sdelenie musia heslá začínať stejnou číslicou a že sa tieto heslá preskupia pri zachovaní daného poradu čísiel, v smeru od ľava do prava. Keď si zvolil šifrujúci v heslách hore uvedených číslicu 7 jako začiatok, preskupí ich takto:

Heslo I.: 7, 11, 3, 17, 8, 13, 4, 12, 21, 16, 2, 5, 20, 14, 6, 18, 9, 1, 19, 10, 15.

Heslo II: 7, 16, 6, 14, 9, 5, 10, 4, 17, 3, 11, 2, 15, 8, 12, 1, 18, 13.

Heslo III: 7, 16, 8, 22, 6, 15, 21, 5, 20, 14, 9, 17, 24, 1, 11, 4, 18, 3, 12, 10, 19, 13, 2, 23.

Figure 1: Triple columnar transposition password alignment (from the manual of *XQ*) - in (Slovak National Archive in Bratislava, 2020), f. MZV, box n. 580.

This permutation alignment was a part of the message key, and was specially transformed to a five letter group and inserted to the cipher text. Both sides of the communication had to know the position of this group. The arrangement (number) is transformed to a five letter group in two steps.

1. The selected one or two digit number is converted to a five digit number based on the following rules:
   - If the number n contains one digit only ($n < 10$), create a group consisting of numbers $\{n, n+1, \ldots, n+4\}$, all modulo 10. E.g. 3 is converted to 34567 and 7 is converted to 78901.
   - If the number n contains two digits ($n \geq 10$), create a group consisting of num-

[7] Document n. 7865 in (Slovak National Archive in Bratislava, 2020), f. MZV, box n. 42.

[8] Document n. 28.114, 28.174 and 28.241 in (Slovak National Archive in Bratislava, 2020), f. MZV, box n. 40.

[9] Document n. 28.241 and 28.245 in (Slovak National Archive in Bratislava, 2020), f. MZV, box n. 40.

[10] Document n. 38.009 in (Slovak National Archive in Bratislava, 2020), f. MZV, box n. 41.

[11] Cipher *R* differs only slightly from *XQ*.

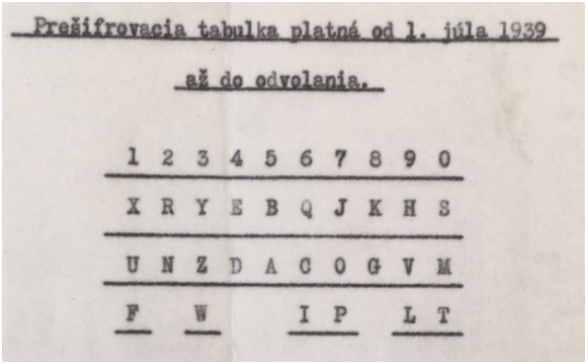
[12] The keys were distributed as *XQ* during years 1939 -1941 and as *R* from 1940/1941. Some documents also contains a dual notation *XQ* with *RR*.

[13] Document n. 28.114 and 28.174 in (Slovak National Archive in Bratislava, 2020), f. MZV, box n. 40.

[14] There is no information why the key space was reduced to the maximal password length 22 for *R*.

bers $\{n, 0, n+1\}$. E.g. 11 is converted to 11012.

2. The five digit group is converted to a five letter group using a special "re-encryption" table ("prešifrovacia tabulka" in original). The re-encryption tables were delivered with the daily key. The table consists of 10 columns marked with digits[15] from $1, 2, \ldots, 9, 0$ and contains 26 letters of the English alphabet distributed in three rows in a random order (see Figure 2). For each digit a random letter is selected from the column defined by the digit, so there are two or three options (rows) how to substitute a specific digit with a single letter.


Prešifrovacia tabulka platná od 1. júla 1939
až do odvolania.

1	2	3	4	5	6	7	8	9	0
X	R	Y	E	B	Q	J	K	H	S
U	N	Z	D	A	C	O	G	V	M
F	W			I	P		L	T	

Figure 2: Triple columnar transposition password alignment re-encryption table (from the manual of *XQ*) - in (Slovak National Archive in Bratislava, 2020), f. MZV, box n. 580.

Before encrypting a message, few rules were defined how to pre-process the input text:

1. Remove accents (e.g. á → A, č → C, etc.).
2. The end of a sentence can be marked with letter "X".
3. Write numbers with a full name, divided to digits:
   - *1907* as *JEDNA DEVAT NULA SEDEM* (*one nine zero seven*).
4. Write Roman numbers with a full name after the word "rim":
   - *IV* as *RIM STYRI*.
5. Proper nouns, shortcuts, time, etc. are divided with letter Q.
6. When the text is shorter than *50* letters, insert the "KONIEC" ("STOP") word and a random padding if necessary.

To encrypt[16] a message P with permutations from the daily key marked I, II, III, arrangement number n and position indicator ip, do the following:

1. Pre-process the input as described above $P \rightarrow P_1$.
2. Arrange $I, II, III \rightarrow I', II', III'$ (based on n), and convert n to a five letter group N.
3. Apply the first columnar transposition (permutation I') to the input $P_1 \rightarrow P_2$.
4. Apply the second columnar transposition (permutation II') to the input $P_2 \rightarrow P_3$.
5. Apply the third columnar transposition (permutation III') to the input $P_3 \rightarrow C'$.
6. Separate cipher text C' to five letter groups and insert N to position ip, the final cipher text is C.

It was recommended to use a grid paper for encryption/decryption. See Figure 5 for a step-by-step example of the encryption process ($n = 7$ and $ip = 5$).

In the investigated cryptologic literature we were unable to find information about any real use of the triple columnar transposition. On the other hand a simpler version - the double columnar transposition - was commonly used as a hand cipher during (and before) WW2. Despite the fact that some special cases (constructions) of this cipher were weak and solvable - it was considered as a secure cipher in general. There are well known materials on how to solve these special constructions. Except of (Kullback, 1934), (Friedman, 1941) and (Barker, 1995) we found also literature about double transposition cryptanalysis in Czech and Slovak language[17]. The most important are:

[15] We also found variations where the digits starts with 0 and ends with 9.

[16] The decryption is in a reverse order.

[17] Various documents in (Security Services Archive in Prague, 2020), f. Zpravodajská správa Generálního štábu; and (Central Military Archives in Prague, 2020), Security Services Archive, f. MNO HŠ.

- J. Růžek: Encryption systems and manual to solve cryptograms (Šifrovací systémy a návod k luštění kryptogramů), 1926;

- K. Cigáň and F. Křepelka: Solving double transpositions (Luštění dvojitých transpozic")[18], 1953.

A modern approach to solve the double transposition in general was presented in (Lasry et al., 2014). It is not clear, whether it can be used to solve triple transpositions as well.

2.3 Cipher Machines

The Ministry of Foreign Affairs borrowed 10 machines[19] from the Ministry of National Defence on Sep 27, 1939. The machine description is given to consist of

> 1 box with registration number, 1 crank with screw, 1 auxiliary hook, 1 stand for text, 1 flannel blanket - with each machine, and 1 cipher manual /cipher manual was revised and old one destroyed/.

From comparing the registration numbers[20] it is clear that the borrowed machines used by the diplomacy were the same as used by the army itself. Therefore the machines were available in Czechoslovakia before WW2 (at least from 1938)[21]. In the documents from the Ministry of National Defence, the machine is simply called as "cipher machine" without additional name (Antal et al., 2019). Despite of the missing information, at least the price of the machine is available[22] in Slovak crowns ("120 000 Ks").

Four cipher machines were made available to embassies:

- 1940 - Berlin, Budapest, Moscow;

- 1941 - Rome.

In April 1944, only six machines were returned back to the Ministry of National Defence[23]. One machine was burnt in air strike in Berlin (November 1943). The machine from Rome was moved to Venice. It is not clear, whether it reached Slovakia, was destroyed, or captured later in the war. One machine, that was located in Budapest, was presumably faulty, but its final fate is also unknown. Machine from Moscow was left[24] in Sweden embassy basement (without official knowledge of the Swedes) when evacuating Moscow embassy in June 1941. However, the cipher manuals were all destroyed. Further fate of the Moscow cipher machine is also unknown, might it be still in some storage?

In multiple telegrams, the unnamed cipher machines are mentioned along with cipher *K*. According to preserved documents, system *K* was directly connected to the cipher machine borrowed from the Ministry of National Defence. System *K* was used and distributed only in embassies where the cipher machine was sent[25].

Our early hypothesis was that "K" cipher machine was the same as Kryha (see later). There is a circumstantial evidence, that cipher system *K* was a more complex system than *Kryha*. E.g., in July 1940, The Ministry of Foreign Affairs sends[26] a cipher machine to Budapest embassy by courier, along with cipher keys for cipher *K* for the rest of the year. In this telegram, the Ministry urges the embassy not to encrypt messages longer than 200 letters. They also give operation instructions for the machine:

> When encrypting with a machine, check each line, by operator marking **the status of the cylinders**, and send the message when you have checked it all out only.
>
> Treat the machine, clean it at least every month and lightly grease. In case of the smallest error that you will not be able to eliminate, do not try to disassemble the machine, but immediately report to

[18] It may be of interest to note that they have broken a double columnar transposition variant used by Yugoslavia.

[19] Document n. 28.050 and 7317 in (Slovak National Archive in Bratislava, 2020), f. MZV, box n. 40.

[20] Document n. 28.114, 1772 and 13.507 in (Slovak National Archive in Bratislava, 2020), f. MZV, box n. 40 and various documents in (Military History Archive in Bratislava, 2020), f. 55.

[21] Document n. 11.654 and 11.331 in (Central Military Archives in Prague, 2020), f. MNO HŠ, boxes n. 283 and 377.

[22] Document n. 75.031 in (Slovak National Archive in Bratislava, 2020), f. MZV, box n. 41.

[23] Document n. 28.050 in (Slovak National Archive in Bratislava, 2020), f. MZV, box n. 40.

[24] Document n. 28.304 in (Slovak National Archive in Bratislava, 2020), f. MZV, box n. 40.

[25] Document n. 28.114 and 28.174 in (Slovak National Archive in Bratislava, 2020), f. MZV, box n. 40.

[26] Document n. 6987 in (Slovak National Archive in Bratislava, 2020), f. MZV, box n. 40.

> the headquarters that the machine is not working, of course also encrypted /*R*/.

From the description, it is not clear, whether mentioned cylinders (*"valce"* in original) could denote two cipher rings of *Kryha*. Machine "K" could also be a completely different cipher machine of rotor type (*"valce"* can also denote drums, gear wheels, or *Enigma* rotors). One potential candidate is the commercial Enigma K machine (Hamer et al., 1998) (used also by Switzerland).

In telegram from March 1941, Dr. Šulík[27] sent a wire to Berlin, Budapest, Rome and Moscow embassies[28] that system *K* is recommended for longer messages. However there is a concern with decryption errors caused by transmission errors (by post office). The telegram indicates, that when a single mistake is made in a five letter group, the message group can still be decrypted. However, if two letters are changed (or) swapped, the whole telegram is unreadable and must be resent. The cause of this behaviour is attributed to the "state of the cylinders".

However, situation is more complicated as wrote Dr. Bukovinský[27] in December 1941 (a handwritten note in the original document) :

> Because instruction is incorrect, I have burned all originals of the expedition.

From pencilmarks on the telegram, the incorrect part is essentially the description of the behaviour of transmission errors. Thus we cannot properly conclude anything about the cipher system based on this telegram.

Further details reveal that longer messages should be split into groups of at most 300 letters. The telegram starts with *K*, a date (day only), and length of each paragraph. The first starting group of the first paragraph contains six letters of the "individual password" (see Figure 3).

It is not clear how an individual password was used. If the unknown machine was Kryha, it could denote setting of clocking pins, or the setting of the alphabet on cipher rings. It could also be a password to a superencryption system. Alternatively, it could be similar to a standard Enigma

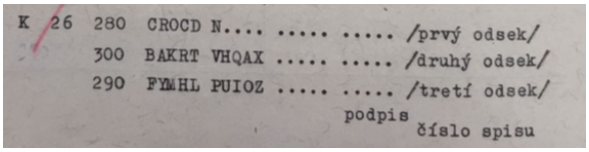


Figure 3: *K* message divided to three paragraphs - Document n. 28.090 in (Slovak National Archive in Bratislava, 2020), f. MZV, box n. 40.

six-letter indicator, which could support Enigma K hypothesis.

Dr. Šulík further mentioned that previous telegrams contained (the same) individual password at the beginning of each group of 300 letters, which practice was forbidden in the telegram. This property can help identify diplomatic telegrams encrypted by the system *K* between July 1940 and March 1941.

There were continuous problems with this cipher machine in Berlin[29], Budapest[30], Moscow[31] and Rome[32]. Some embassies also requested a new cipher machine. Probably for this reason the available cipher machines were replaced by a (different/new?) cipher machine openly called *Kryha* in 1943.

In a document[33], there is an explicit reference to "six complete cipher machines KRYHA-S TANDaRD". Kryha Standard was a commercial cipher machine released by Alexander (von) Kryha in 1924 (Schmeh, 2010). Machine was based on a cipher disk, with 2 rings: outer ring was fixed, and inner ring was rotated by a clockwork machine with irregular stepping. Ring alphabets could be changed by the operator. To encrypt a message, operator pushed the button to rotate the machine, and then replaced plain text letter found on the inner ring by cipher text letter on the outer ring. From cryptological point of view, the cipher is a polyalphabetic substitution with individual alphabets rotated by the amount given by clocking se-

[27] Secretary of the Ministry of Foreign Affairs working in cipher department. We have no further details available.

[28] Document n. 28.090 in (Slovak National Archive in Bratislava, 2020), f. MZV, box n. 40.

[29] Document n. 75.242 in (Slovak National Archive in Bratislava, 2020), f. MZV, box n. 41.

[30] Document n. 38.019, 38.024, 38.026 and 38.124 in (Slovak National Archive in Bratislava, 2020), f. MZV, box n. 40.

[31] Document n. 610 in (Slovak National Archive in Bratislava, 2020), f. MZV, box n. 40.

[32] Document n. 28.272 and 52/dov/Dr.M.-taj in (Slovak National Archive in Bratislava, 2020), f. MZV, box n. 40 and 41.

[33] Document n. 75.020 in (Slovak National Archive in Bratislava, 2020), f. MZV, box n. 41.

quence of the machine. Such a system was known to be broken even before WW2 (Marks, 2011).

There were at least eight *Kryha* machines available to the Ministry of Foreign Affairs, some were distributed to embassies in the following years:

- 1943 - Helsinki;
- 1944 - Bucharest, Madrid, Budapest;
- 1945 - Berlin.

Another cipher machine, called *SVERK* (see Figure 4), was sent to Helsinki in 1943. The document[34] also describes some parts of the machine - it contains one encryption wheel and plugs to the wheel. In a different document the machine sent to Helsinki (referring to the same registration number and document number) is called *Kryha*. Therefore we think that *SVERK* is only a covername for *Kryha*.

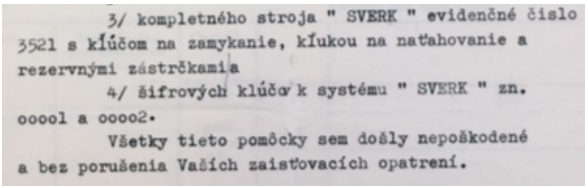

3/ kompletného stroja " SVERK " evidenčné číslo 3521 s kľúčom na zamykanie, kľukou na naťahovanie a rezervnými zástrčkami
4/ šifrových kľúčov k systému " SVERK " zn. ooool a oooo2.
Všetky tieto pomôcky sem došly nepoškodené a bez porušenia Vašich zaisťovacích opatrení.

Figure 4: *SVERK* cipher machine - Document n. 12/dov. 1943 in (Slovak National Archive in Bratislava, 2020), f. MZV, box n. 41.

3 Encryption Problems on Embassies and on the Cipher Department

The encryption service on embassies did not work without problems. There were three major types of problems:

1. Telegram corruption - From the documents we found so far, the most frequent problem was that the telegrams could not be decrypted due to corruption. In some cases the post office was responsible[35] for modifying (or dropping) the part of the encrypted text, in other cases, it was a fault in the encryption officers work[36].
2. Not respecting the manuals and encryption directives - E.g. partially encrypted messages[37]; resending previously encrypted messages in plain text[38]; writing about encryption[39] etc.
3. Problems with cipher machines (see section 2.3).

Because of the frequency of operation problems the Ministry of Foreign Affairs informed the embassies several times about cryptographic principles[40], such as:

- Never use the word ”cipher” in documents.
- The content of the message should be reworded.
- All used papers must be burned after encryption/decryption.
- To any encrypted message reply by using encryption only.

In 1941, Dr. Bukovinský created a report[41] about experiences and problems in the cipher department of the Ministry of Foreign Affairs. We briefly summarize his report:

- The department is located in a room, where other personnel (not from the cipher department) is also located, and there are even visits from outside the Ministry.
- There is no curtain on the window, so the cipher machine is visible from the opposite building through the window.
- There are no special blankets used for encryption (only a standard paper).
- The used cipher is marked on telegrams, so the foreign countries can simply sort the encrypted telegrams by the used cipher system.

[34] Document n. 75.010 in (Slovak National Archive in Bratislava, 2020), f. MZV, box n. 41.

[35] Document n. 28.090, 28.272 and 90.000 in (Slovak National Archive in Bratislava, 2020), f. MZV, box n. 40 and 42.

[36] Document n. 38.021 in (Slovak National Archive in Bratislava, 2020), f. MZV, box n. 41.

[37] Document n. 75.219 in (Slovak National Archive in Bratislava, 2020), f. MZV, box n. 41.

[38] Document n. 760 and 28.061 in (Slovak National Archive in Bratislava, 2020), f. MZV, box n. 41.

[39] Document n. 38.008 in (Slovak National Archive in Bratislava, 2020), f. MZV, box n. 41 - ”chiffraantwort folgt” was used.

[40] Document n. 28.302 and 75.008 in (Slovak National Archive in Bratislava, 2020), f. MZV, box n. 40 and 41.

[41] Document n. 28.300 in (Slovak National Archive in Bratislava, 2020), f. MZV, box n. 41.

- Cipher machines are not working correctly because of incorrect usage.
- Systems *K* and *R* are used to encrypt non important messages, and the most simple system *C* is used to encrypt important messages.

Later, in 1943, Dr. Bukovinský was asked[42] to check the embassies in Budapest, Zagreb, Rome and Berlin. The goal was to check and correct the lack of encryption:

- The cipher machine in Budapest was set incorrectly.
- Only hand cipher was available in Zagreb. The secretary of the embassy was trained in encryption.
- The cipher machine in Rome was not working.
- In Vatican, there were no ciphers available, and nobody knew encryption.
- In Bern, the head of the office did not know encryption.

We do not know whether these problems and mistakes were exploited by attackers in practice. If cryptanalytic public is interested, we have found some encrypted telegrams in the archives that remain an unsolved challenge.

Acknowledgments

We are grateful to the Military Intelligence (Ministry of Defence of the Slovak Republic), for the help and resources made available.
This work was partially supported by grants VEGA 1/0159/17 and VEGA 2/0072/20.

References

Central Military Archives in Prague (Vojenský ústřední archiv v Prahe).

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

Security Services Archive in Prague (Archív bezpečnostních složek v Prahe).

Slovak National Archive in Bratislava (Slovenský národný archív v Bratislave).

[42]Document n. 75.001 in (Slovak National Archive in Bratislava, 2020), f. MZV, box n. 41.

Eugen Antal, Pavol Zajac and Otokar Grošek. Cryptology in the Slovak State During WWII. In *Proceedings of the 2nd International Conference on Historical Cryptology, HistoCrypt 2019*, pages 23 - 30.

František Bielik, Ján Gáll and Klára Kunkelová. Ministerstvo zahraničných vecí 1939 - 1945 Inventár. 1965. Štátný slovenský ústredý archív v Bratislave.

Wayne G. Barker Cryptanalysis of the Double Transposition Cipher: Includes Problems and Computer Programs. 1995. Aegean Park Press.

Wiliam F. Friedman Military Cryptanalysis. 1941. US Government Printing Office.

David H. Hamer, Geoff Sullivan and Frode Weierud. Enigma variations: An extended family of machines. 1998. *Cryptologia*, 22(3):211-229.

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.

Solomon Kullback General Solution for the Double Transposition Ciphers. 1934. Aegean Park Pr .

George Lasry, Nils Kopal and Arno Wacker. Solving the Double Transposition Challenge with a Divide-and-Conquer Approach. 2014. *Cryptologia*, 38(3):197-214.

Klaus Schmeh. Alexander von Kryha and His Encryption Machines. 2010. *Cryptologia*, 34(4):291–300.

Philip Marks. Operational Use and Cryptanalysis of the Kryha Cipher Machine. 2011. *Cryptologia*, 35(2):114–155.

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

Appendices

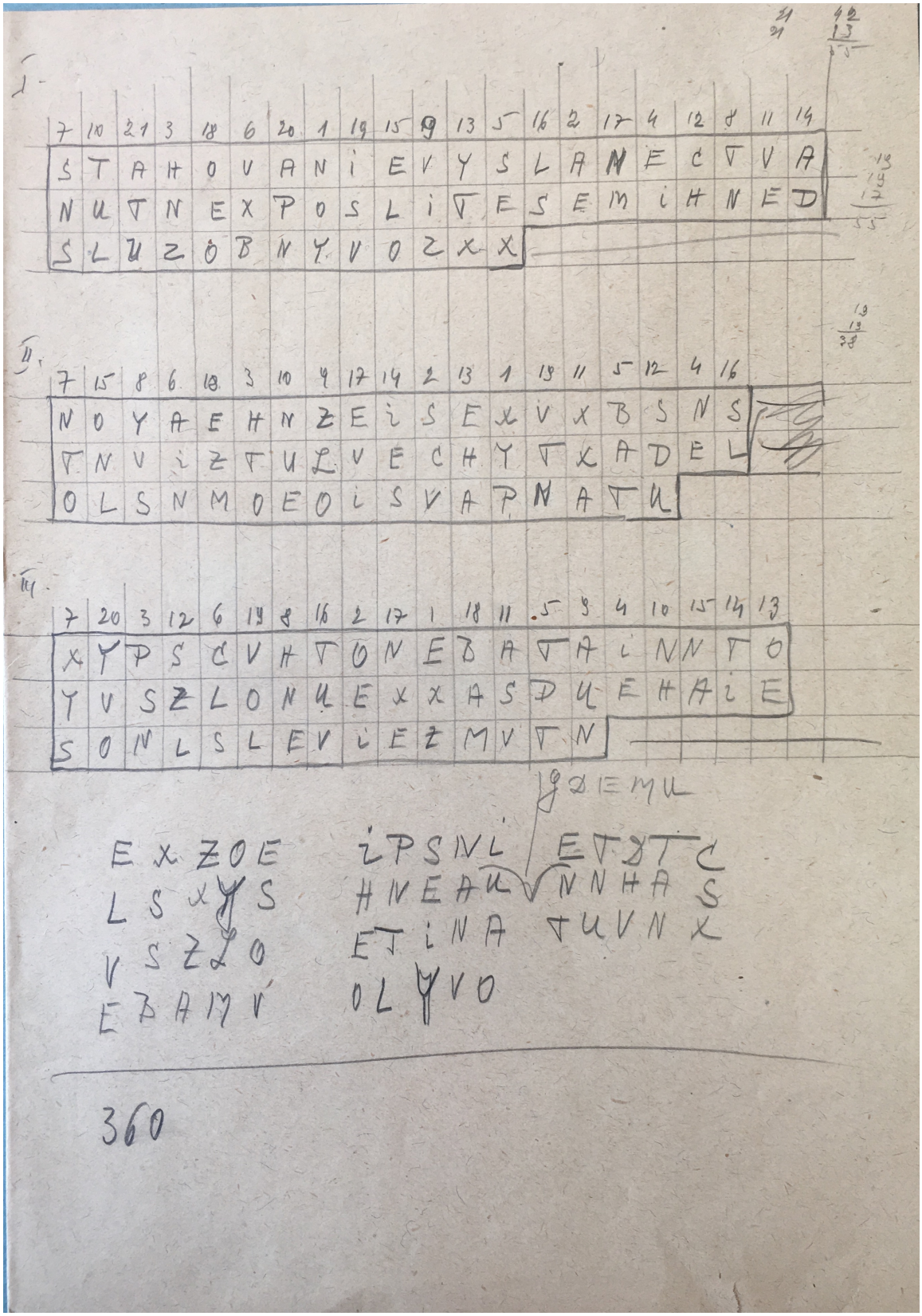
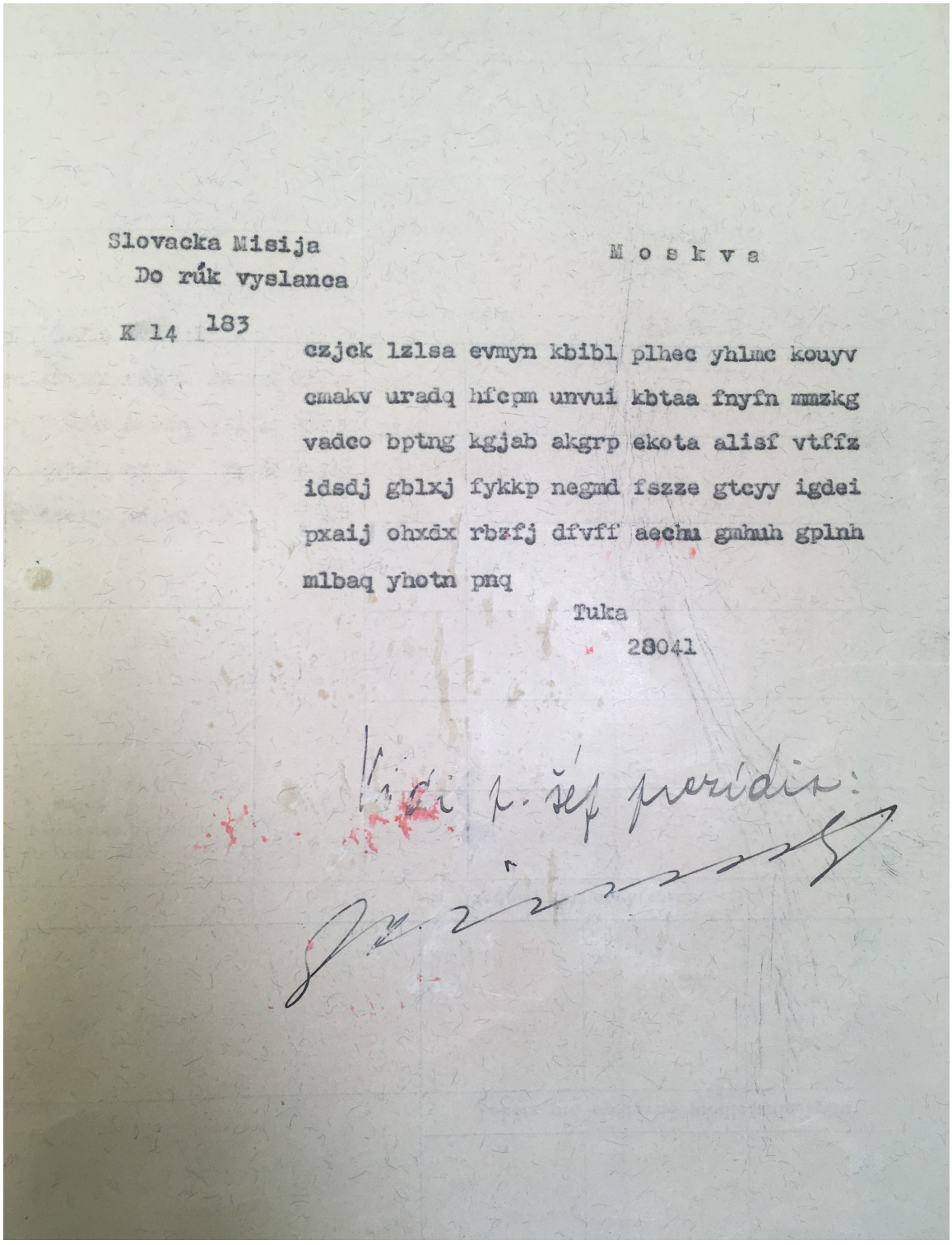


Figure 5: An example of triple columnar transposition encryption - in (Slovak National Archive in Bratislava, 2020), f. MZV, box n. 507.



Slovacka Misija
Do rúk vyslanca

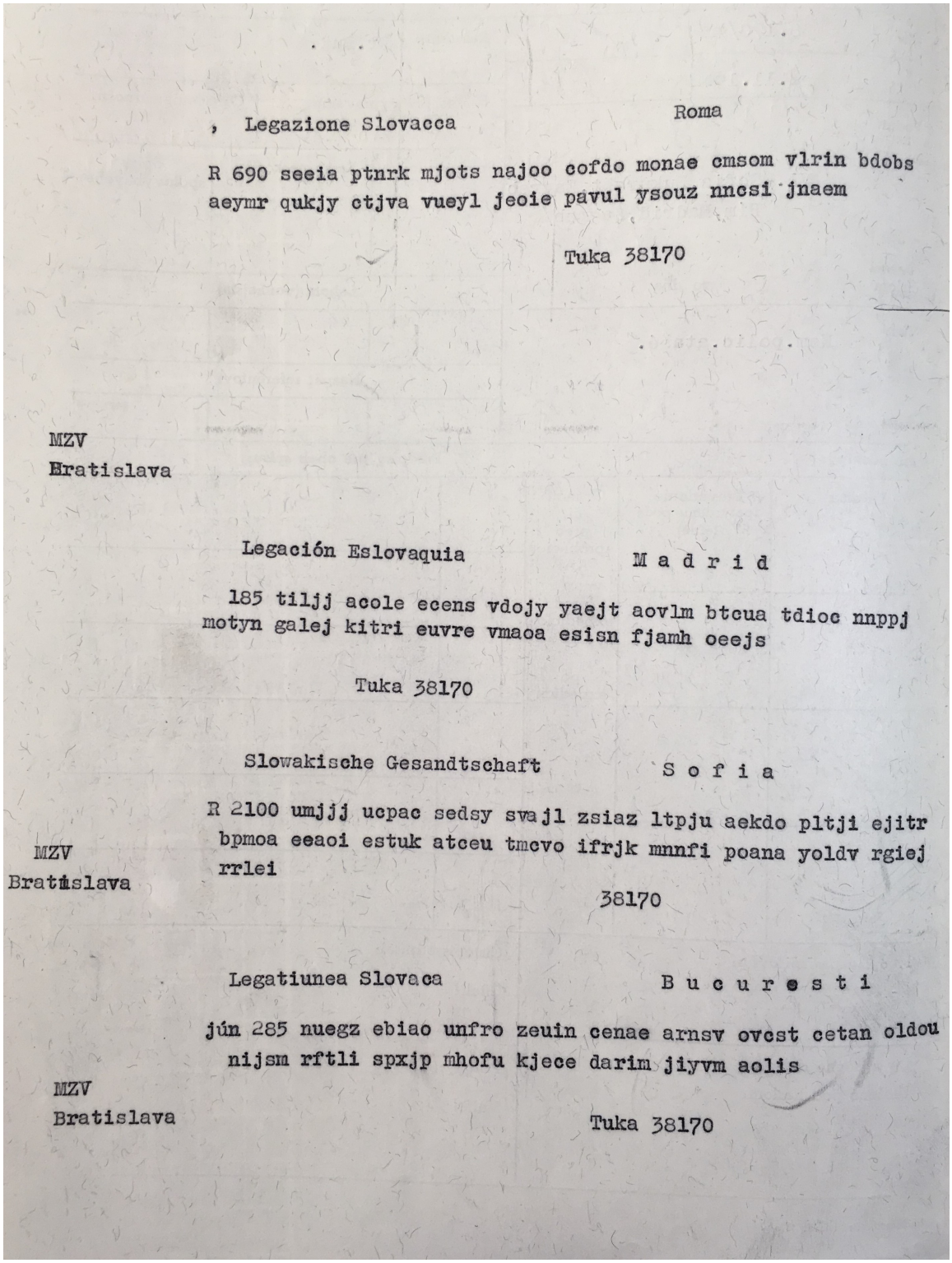
Moskva

K 14 183

czjck lzlsa evmyn kbibl plhec yhlmc kouyv
cmakv uradq hfcpm unvui kbtaa fnyfn mmzkg
vadco bptng kgjab akgrp ekota alisf vtffz
idsdj gblxj fykkp negmd fszze gtcyy igdei
pxaij ohxdx rbzfj dfvff aechu gmhuh gplnh
mlbaq yhotn pnq

Tuka
28041

Figure 6: Text encrypted with system *K* - in (Slovak National Archive in Bratislava, 2020), f. MZV, box n. 40.



, Legazione Slovacca Roma

R 690 seeia ptnrk mjots najoo cofdo monae cmsom vlrin bdobs
aeymr qukjy ctjva vueyl jeoie pavul ysouz nncsi jnaem

Tuka 38170

MZV
Bratislava

Legación Eslovaquia M a d r i d

185 tiljj acole ecens vdojy yaejt aovlm btcua tdioc nnppj
motyn galej kitri euvre vmaoa esisn fjamh oeejs

Tuka 38170

Slowakische Gesandtschaft S o f i a

R 2100 umjjj ucpac sedsy svajl zsiaz ltpju aekdo pltji ejitr
bpmoa eeaoi estuk atceu tmcvo ifrjk mnnfi poana yoldv rgiej
rrlei

MZV
Bratislava

38170

Legatiunea Slovaca B u c u r e s t i

jún 285 nuegz ebiao unfro zeuin cenae arnsv ovcst cetan oldou
nijsm rftli spxjp mhofu kjece darim jiyvm aolis

MZV
Bratislava

Tuka 38170

Figure 7: Encrypted telegrams sent to Rome, Madrid, Sofia and Bucharest - in (Slovak National Archive in Bratislava, 2020), f. MZV, box n. 41.