DE GRUYTER
OPEN

TATRA MOUNTAINS
Mathematical Publications

DOI: 10.1515/tmmp-2017-0019
Tatra Mt. Math. Publ. **70** (2017), 41–91

APPLICATION AND MISAPPLICATION OF THE CZECHOSLOVAK STP CIPHER DURING WWII

(REPORT ON AN UNPUBLISHED MANUSCRIPT)

Štefan Porubský

ABSTRACT. Lieutenant colonel Karol Cigáň (1921–2005), head of the cryptographic unit of the Czechoslovak Ministry of National Defence in the period 1949–1958 was after discharging from this position in Prague relocated to an insignificant and substandard command position at a district military administration in Slovakia. His cryptographic experience was of no use in his new position. To profit from his previous experience as a high qualified cryptographer he started to study the accessible literature and archive materials about the usage of the Czechoslovak cipher systems during the WWII. The result of this his activity were some manuscripts where he deciphered and analyzed some Czechoslovak military wireless telegrams. His critical analysis and his conclusions did not meet an understanding or a positive response of historians and were nor accepted for publication. He had no other chance as to send them to archives. Unfortunately only one (in two copies) and a collection of small notes survived. The aim of this paper is to make decisive technical parts of manuscript [K. Cigáň: *Impacts of the decryption of the cipher system of the Czechoslovak Ministry of Defence in London from the years 1940–1945 on the resistance movement*. Archive of the Slovak National Uprising, Banská Bystrica, Slovakia, Document collection (Fond) V, manuscript no. S36/90, 46 pp.] about the usage of the so-called STP cipher accessible. Thereby we complement the paper [Š. Porubský: *STP cipher of the Czechoslovak in-exile Ministry of Defence in London during WWII,* in: Proc. of EuroHCC'17, 3rd European Historical Ciphers Colloq., Smolenice Castle, Slovakia, 2017 (J. von zur Gathen et al., eds.), Slovak Univ. of Technology in Bratislava, 2017, pp. 47–66] where the part of this manuscript containing Cigáň's method for solving STP cipher which he calls "mathematical" is published. To put Cigáň's analysis and comment into their historical framework we briefly outline the history of Czechoslovak military intelligence activities with emphasis on their cryptological component.

© 2017 Mathematical Institute, Slovak Academy of Sciences.
2010 Mathematics Subject Classification: Primary: 01A60; Secondary: 01A70, 01A85.
Keywords: STP cipher, Josef Růžek, Karol Cigáň, František Moravec, Czechoslovak military cryptography, World War II.
The author was supported by the strategic development financing RVO 67985807.

There is a mystery in the soul of State
Which hath an operation more divine
Than breath or pen can give expressure to.
SHAKESPEARE, TROILUS AND CRESSIDA

1. Introduction

K a r o l C i g á ň was a Slovak career officer who started his military career in 1944 as a graduate of the newly established military academy in Bratislava. He entered his cryptologic path in the Czechoslovak army in January 1947. In the period 1949–1959 he served as the head of the cryptologic section at the Czechoslovak Ministry of National Defence (MND). On January 9, 1959 he was fired from this position on the basis of purely political accusations. The first decision of the superior military and political authorities was to discharge him completely from the military service. A month later, this decision was withdrawn and he was relocated to a substandard command position at a district military administration in a small town Vráble in south Slovakia and in October of the same year to Komárno on Danube, on the border between Slovakia and Hungary. He stayed here with a small two-month interruption between March and May 1978 for the rest of his career and here he was retired on January 1, 1979 and died on July 5, 2005. He is buried on the local Catholic cemetery. For more details on his carrier refer to [25].

Though his high cryptographic experience was of no use in the positions after his discharge from the position of a cryptographer, the personal hard cryptographic fate did not break him. He remained a passionate cryptographer for the rest of his life. He studied and read the published literature about the communication between MND in London and Czechoslovak resistance groups, solved the related encrypted radiotelegrams deposited in archives in his leisure time. Using this material he tried to fill some gaps in some conclusions of historians about the resistance and of the role of German spies in the service of the Czechoslovak military intelligence. He was disappointed by the displeasure of professional historians to accept his analysis and the conclusions of his analysis. Most of their reservations were based on the lack of the understanding of the role of cryptography in the evaluation of the military intelligence activities and of the underground resistance saboteur actions. A starling facet of these unequal position fights was the fact that Cigáň's manuscripts were never published or released to a wider professional community (his preserved manuscripts did not attract the attention of the scholar historians neither after the fall of communism in 1989). Disappointed C i g á ň decided to deposit his manuscripts for a future better evaluation in various military of even communist party archives which he trusted in. Nevertheless, as it seems, only one manuscript [8] survived out of

these manuscripts up to these days.[1] The remaining ones disappeared (or were stolen) from the archives. Surprisingly, this one manuscript [8] survived in two archives. In a recent report [24] we published a part of the manuscript which was devoted to what C i g á ň called a "mathematical method" for the solution of the so-called STP cipher. Though without a deeper mathematical education, he tried to recover the method which the captured German cryptologists loosely denoted as "mathematical" in their interrogations after the end of WWII.

In what follows we reproduce the essential parts of manuscript [8] focusing on the technical details of the usage and solution of this cipher, as they were seen by C i g á ň. Nevertheless, the manuscript contains also many interesting analytic facts and comments on the political and military evaluation of that period in the light of some telegrams sent in the broadcasting communication between intelligence department of the in-exile MND in London and the resistance groups in the territory of the former Czechoslovakia during WWII. His analysis is based on telegrams he found in military archives, which he solved and deciphered and which he used to substantiate his conclusions and arguments. Since a reproduction of these parts of the manuscript requires a deeper knowledge of the political, military and social situation and atmosphere of that period in the territory of the former Czechoslovakia, they are mostly omitted in what follows. On the other side, to enlighten some other historical circumstances and their background we add a short (and consequently incomplete) historical account about the development of the Czechoslovak military intelligence till the end of WWII. In this part our emphasis is given on the technical and historical background connected with the usage of the cipher systems in the communication between the in-exile MND, its foreign branch offices and the resistance groups in the homeland.

It must be said, that the most information about the activities of the intelligence parts of the army or police in the former communist regime were classified. The information that there are cryptological intelligence units in the army, police, etc. was not publicly spread and the cryptologists as such were not allowed to reveal their identity. Moreover, around and after the communistic coup d'état in February 1948 a "witch-hunt" began in all levels of society, especially against those who fought in the West. Consequently, no serious professional cryptanalytical analysis of the cipher systems deposited in the military archives and used during the WWII was done (unfortunately up to now). The reason for such absence was manyfold. Firstly, an objective analysis of political and military activities coming and organized form the West was politically undesirable. Secondly and surprisingly, a similar enterprise in direction East was also not possible

[1]Besides this one manuscript there are deposited several small appendices in the Archive of the Slovak National Uprising in Banská Bystrica, Slovakia. The manuscripts – called "fascikly" – numbered from 1 to 8 can be found in the document collection (Fond) V, no. S22/2002, box 4; the first 7 of them having together 78 pages. Number 9 and 10 are promised to be sent, but they were actually not sent.

with regard to inaccessibility of Soviet archives and a bareknuckle tacitness of participants of the events.[2]

Some details, destined more for general audience than for specialists, can be found in books [13]–[15] written by a former military cryptologist. Unfortunately, a cryptographer would miss here many important details (e.g., details on used passwords, more detailed descriptions of mentioned cipher system, etc.).

As mentioned, K. C i g á ň as a "retired" cryptographer devoted himself in the spare-time to the decryption and the analysis of the archived wireless correspondence between the in-exile Czechoslovak government in London and the home resistance groups. Partly because he had a legitimate feeling that the published papers do not also employ a serious cryptographical analysis of the preserved radiotelegrams. In 1967 he succeeded in deciphering some radiograms connected with the activities of agent A-54 Paul Thümmel. This agent of the WWII Czechoslovak intelligence, often declared as a top agent of the pre-war and the second world war Czechoslovak intelligence, is a controversial figure. Thümmel was a respected member of NSPDA and holder of the Golden Party Badge of NSPDA showing his early entrance in the party. C i g á ň analyzing of till that time not decrypted radiograms[3] tried to show that A-54 was not a double agent, but an agent of the operational concealment, a point of view which was not (and still is not) fully accepted by historians. The cryptographical core of the corresponding C i g á ň' s manuscript [6] was not published and as it seems it is lost in the meantime. Its published version [7] in a military mag is actually a censored and revised version of his intended contribution to this part of the military history of the Czechoslovak intelligence service during WWII. From our point of view, the important cryptological details of the manuscript were expunged. As a whole, it seems that even this his partial success in publication of his research was a consequence of the liberalized political setting and relaxation of censorship during the period of the Prague Spring 1968. Invasion of Eastern Block armies in the night of 20–21 August 1968 not only ended this brief period of liberalization but also the effort to unprejudicedly revaluate the WWII part of Czechoslovak military history.

The exception proves the rule, but in general, the evaluation of the home resistance time period during WWII by the Czechoslovak historians during the communism time was heavily indebted to the communist ideology to heroise and glorify certain aspects of the resistance and suppress or neglect some others. One such peculiarity and particularity was the unwillingness to recognize that

[2]A seldom exception. In the interrogation of SS-Oberscharführer Dr. Alois Hornischer on 12 February 1946 in Prague it is mentioned that a Russian parachutist Josef Dicka died at one airdrop in Poland. In his material a list of addresses enciphered with an unusual cipher was found. The cipher was allegedly solved by major Ergert.

[3]The radiograms were of course decrypted during the WWII but the decryptions were often lost and the direct witnesses were mostly dead in the meantime.

it was within possibilities of the intelligence units of the enemy German army to overpower the possibilities of the home resistance and of the in-exile Ministry of National Defence on the field of breaking of ciphers considered by their users to be unbreakable. It was often politically more advantageous to exploit a failure of an individual who betrayed, as to admit that beside such regrettable episodes, there was something what did not work properly in own lines. And this was the failure of the intelligence department of the Czechoslovak in-exile MND in London in the organization of the wireless communication, and especially in the organization of its cryptographic way of operation.

2. Organization and role of the Czechoslovak intelligence till the end of WWII

Czechoslovakia (Czecho-Slovakia) as a sovereign state was founded in October 1918 when it declared its independence from the former Austro-Hungarian Empire. After the independence declaration the first highest authority of military administration became the so-called National Defense Committee (Výbor národní obrany). It was established by the National Committee (Národní výbor) on 30 October 1918 and it was responsible for the governing of all the matters concerning the army and the defense of the state. The first supreme army command was The Supreme Military Command (Vrchní vojenské velitelství) which was on December 18, 1918 replaced by the newly established Ministry of National Defence (Ministerstvo národní obrany).

The ministry had 17 departments, from which only one — the 3rd one called military one — had a real military orientation. The foreign minister Edvard Beneš[4] negotiated a military assistance with the main ally of Czechoslovakia––France. The negotiations resulted in the deployment of a French Military Mission (FMM) to Czechoslovakia. It started its mission on 13 February 1919 and its officers were directly incorporated into the organization of the Czechoslovak army and on the most important command posts. The initial number of the persons was 45 officers, and the maximum was attained in October of the same year, 145 officers.[5] The head of FMM was French general Maurice Pellé.

In May 1919 section A of the IIIrd Department was unified with until then autonomous supreme command of army in Slovakia. The General Staff (GS) was formed by merging FMM and the IIIrd Department of MND.

[4]Beneš was the first and longest-serving foreign minister of Czechoslovakia, from 1918 to 1935. When President Tomáš G. Masaryk retired in 1935, Beneš was elected as his successor in this function.

[5]Some sources claim that various command posts were filled with some 200 French non-commissioned officers, with more than 100 commissioned officers and 19 Generals.

On 4 July 1919 Czechoslovak president Tomáš Garrigue Masaryk appointed the Chief of the FMM in Czechoslovakia, general Maurice Pellé, as the supreme military commander of the Czechoslovak Armed Forces. He and later from January 1, 1921, Eugéne Mittelhauser were the first chiefs of the GS of the Czechoslovak Armed Force. Its inner organization mirrored the structure of the FMM. It consisted from a Chief, his First and Second Deputy and four departments: 1st operational, 2nd intelligence, 3rd organization and mobilization and 4st transport one. The command positions followed a parity French-Czechoslovak representation model: French head — Czechoslovak deputy head. In the period from 1919 to 1925 the head of FMM was also the Chief of GS.

In 1926 FMM became an advisory body in the matter of the organization of the Czechoslovak army. The mission was inactivated on January 31, 1939.

Only a partial information preserved about the beginnings of the Czechoslovak intelligence service. At the beginning of 1919 this component of military activity was under the auspice of section A of the mentioned 3rd Department at MND. Two smaller intelligence groups — covered as propagation and press departments — were at the Foreign Ministry (head Jan Hádek since 1919) and at the Interior Ministry (head Jan Hajšman since 1922). Acting head of section A was lieutenant colonel Rudolf Kalhous.[6]

The first known head of the intelligence department was 36 years old major Čeněk Haužvic, former head of the intelligence department of the Austria-Hungarian military government in Lublin[7]. He took over this function on November 12, 1918. The General Staff of the Czechoslovak Defence Force was officially established on 15 October 1919. His deputy since November 1, 1921 (and later head of the search group) became the major of the Italian legions Mojmír Soukup. Head of counterintelligence section in February 1920 became Vladimír Vaněk.[8] The cipher section of the 2nd Department was responsible for

[6]Section A had originally four divisions: 1st operational, 2nd organization and mobilization, 3rd intelligence and 4th transport. Later the divisions were renumbered and the intelligence department obtained number 2 to emulate its French preimage the "Deuxième bureau".

[7]Today a city in Poland. After the third of the Partitions of Poland in 1795 Lublin belonged to the Austrian empire, since 1809 to the Duchy of Warsaw, and then since 1815 it was under Russian rule. Russian rule ended in 1915, when the city was occupied by German and Austro-Hungarian armies.

[8]From February 1919 to December 1920 he directed the build-up of the counterintelligence section of the Czechoslovak intelligence service. After his "deactivation" he continued his service in a diplomatic career. In 1921 he was attache at the Czechoslovak embassy in Stockholm, in 1923 Czechoslovak counselor in Linz, in 1924–1929 attache in Paris, and during 1931–1937 again at the Czechoslovak embassy in Stockholm which he also occasionally led as chargé d'affaires. After returning to Prague, he became an officer of the 2nd section of the Ministry of Foreign Affairs responsible for Sweden, Norway and Austria. After German occupation of Czechoslovakia he managed to return back to Sweden on March 17, 1939. In August 1939 Vaněk obtained from Emil Strankmüller, who operated as an intelligencer officer in Sweden

the intelligence contact and the correspondence abroad and for the encryption and decryption of the correspondence. Head of this section was Jan Ropek. Since 1928 till March 15, 1939 its head was Josef Růžek (in 1928 major). In 1938 this section had 5 members: lieutenant colonel Josef Růžek, major Jan Brandšteter, captains Ladislav Syrový, Beřich Frýbort anf Josef Andrle. Another protagonist of our following tale captain František Fryč was member of the Offensive section of the GS in this time. In the thirties he also joined Josef Růžek in solving German double transpositions (German: Doppelwürfelverfahren).[9]

At the very beginning, the members of the new 2nd Department had almost no practical experience and theoretical knowledge in the subject. Therefore Mojmír Soukup organized crash courses for them based on the experience gained during WWI. In the courses, mainly French officers lectured. In 1920 the Department issued a first written and classified booklet *Intelligence service in war time* based on a treatise of the Russian general Pavel Fedorovič Rjabikov, who was an advisor of the Czechoslovak intelligence service till the beginning of thirties. However, there was no word in it about cryptology .

from August 1939 to spring 1940, cipher keys and a radio transmitter. In Stockholm Vaněk maintained the "Swedish corridor" of the Czech resistance and sent about 500 messages to London in period August 1941–March 1942. In March 1942 he was — upon the pressure of the Germans arrested — sentenced to three and half years' hard labor for espionage against Germany. The breaking of his telegrams to London, which were used in the process was a master piece of Arne Beurling. Clearly, before the court the explanation how they were broken was a camouflage of Swedish police. [5, p. 109-118]

[9]The Czech sources mention that it was a double transposition (cf. [14, p. 240]), but as it follows from TICOM files it was rather a transposition with dummies. Namely, as it is reported by Wilhelm Fenner [10], the chief of Hauptgruppe B of the Chifrierabteilung OKW (Armed Forces High Command): "After the fall of Czechoslovakia, Fenner had visited Růžek, the head of the Czech organisation, who told him that the Czechs had read the German military transposition with dummies, after receiving information on the system from a German informer. Fenner maintained that, without outside information, single transposition with dummies is quite unbreakable . . . "

As it seems that the German Army double transposition hand cipher was also solved by Polish Biuro Szyfrów prior to 1928 [18, p. 301 and 973]. An exchange of information between the Polish and Czechoslovak cryptologists was very improbable in that time due to bad relations between both countries. The main source of discrepancies was the demand of both sides on some border territories, e.g., on the territory of Cieszyn Silesia. This controversy finally ended in the so-called Poland-Czechoslovakia war (in Czechoslovakia known as Seven-day war (Czech: Sedmidenní válka)) in 1919. Another typical projection of mutual bad relations is from the year 1934. In this year there was organized The IInd Congress of Slavic Mathematicians in Prague. Some Polish mathematicians had problems to participate on the congress, e.g., the prominent Polish mathematician Wacław Sierpiński did not obtain permission to participate on the Congress. However, there are some indications that after all he participated on the Congress when he stopped in Prague using a permission to travel to Italy, but for his real participation on the congress there is no archival confirmation.

At the beginning of 1936 the Czechoslovak intelligence service silently changed its main strategic partner.[10] Instead of the French one it was the British intelligence service[11] who took up the leading role. After this swap the key role in the Czechoslovak–British collaboration was played by the local resident of the British Military Intelligence Harold Gibson "Gibbie" (in Czech Gibby)[12] who did serve as SIS (also known popularly as MI6) Station Head in the British Embassy in Prague from February 1934[13] and covered himself as the passport control officer.

On September 30, 1934 to the 2nd Department there was assigned military intelligence officer lieutenant colonel František Moravec[14], code name Pavel, as the head of section B – the search section.[15] Later, on March 1, 1937 Moravec

[10]In 1938 the head of the Analytic section colonel František Havel characterized the collaboration with French intelligence service as a not very fruitful bilateral relationship which gradually become cool and after the Munich Agreement it even became strained.

[11]The Czechoslovak military intelligence also started a cooperation with representatives of the Soviet intelligence service in Prague in the second half of 1936, approximately a year after the Czechoslovak–Soviet Treaty of Alliance was signed on May 16, 1935. This cooperation, which was judged positively by the members of the 2nd Dept., was performed under the auspice of colonel František Hájek, last head of the 2nd Department. Based on this agreement Růžek visited Moscow in 1936 and learned the Soviets how to solve German double transposition (cf. footnote 9).

[12]After the Germans marched into Prague on March 15, 1939 the station was closed and Gibson and his staff decamped to London on March 30. He was then sent to Istanbul, where he was active previously in the rank of major in the period 1919–1921 when the town was still Constantinople. In 1945–1948 he was again the head of station in Prague. He was later found shot dead on August 24, 1960 in his apartment at 25 Via Antonio Bosio in Rome.

[13]Gibson's counterplayer on the French side was major Henri Gouyou (code name Šmidra), intelligence officer of the Service de Renseignement of the military attache colonel d'Abord at the French Embassy in Prague. Gouyou came to Prague in 1936. After closing the joint French-Czechoslovak military mission in Prague in June 1936, Gouyou was responsible for the exchange of information, particularly about the German activities, and the encrypted radio communication.

[14]Not to be confused with Emanuel Moravec, colonel of the pre-war Czechoslovak army and later a Nazi collaborator as a Minister of Education and National Enlightenment in the puppet government of Protectorate of Bohemia and Moravia.

[15]František Moravec (1895–1966) was drafted into Austro–Hungarian Army in 1915 being a student at the Charles University. He was sent to the Eastern Front (Galicia). On 13 January 1915 he was taken as prisoner by Russian troops. In 1916, he voluntarily joined the Serbian Legion and fought on the Romanian Front. He later moved from Archangelsk to Britain, and in 1917 he joined the Czechoslovak Legions at the Salonica Front. In January 1918, the legions were sent to the Western Front in France and in summer 1918 to the Italian Front. On 1 December 1929 major Moravec become the head of the intelligence department of the Land Military Command in Prague (Zemské vojenské velitelství v Praze). By the way, Moravec sat in the same office as several years ago the renowned Austrian colonel Redl who sold the mobilization plans of the Austrian army to the Russians in 1913. The room was in the building of the Land Military Command in Prague in the so-called Liechtenstein Palace in the Malá Strana district. Since 1848 troops were settled there and 1850, it was definitely repurchased

become deputy head of the 2nd Department and on January 2, 1939 its interim head.

Shortly before World War II, on March 15, 1939, Czechoslovakia ceased to exist. Its territory was divided into three parts: The Protectorate of Bohemia and Moravia, the newly declared Slovak State and the Carpathian Ukraine. The Protectorate of Bohemia and Moravia was directly joined to the Third Reich, the Carpathian Ukraine was divided between Poland and Hungary.[16]

After the Czechoslovakia was broken up by Nazi Germany on March 15, 1939, the MND was closed by Germans on December 31, 1939.[17] The period 1939––1945 is characterized by the creation of a military administration under the conditions of the foreign exile. The center of the Czechoslovak foreign resistance was at the beginning in the United States of America, and from the summer of 1939 it was Paris and later London. There were made the first attempts to build administrative authorities, including military ones, of the Czechoslovak Republic abroad. The outbreak of World War II opened a chance to create a temporary exile government. However, France and the United Kingdom have only allowed the creation of the Czechoslovak National Committee (Národní výbor československý) at the beginning, which was established on 17 November 1939 in France. It must be said that despite massive communistic propaganda during communist period which attributed the leadership of the domestic resistance to

by the army. During the Second World War there was the German military headquarters. On September 30, 1934 Moravec was promoted to colonel and in 1943 to general.

[16]As mentioned in [23, p. 215] the Czechoslovak intelligence service knew some German ciphers which were revealed by agent A-54. Based on the deciphered radiograms of German police stations near the border the prepared invasion of German troops was evident for several days before 15 March.

[17]President Edvard Beneš abdicated from his position after the Munich Agreement on October 5, 1938 as a result of a strong German pressure. On 22 October he went into exile by a scheduled flight first to London. Later he went to USA where he lectured at University of Chicago. After the German occupation in March 1939 he returned back to London in July 1939. Most of his communist opponents from the political bureau of the Central Committee of the Czechoslovak Communist Party also emigrated, in this case to Moscow following a decision of the Comintern. The leader of the Czechoslovak communist party Klement Gottwald left Prague to Moscow via Paris in November 1938. Other groups of communist exponents left Czechoslovakia to Moscow via Paris, Copenhagen, Stockholm, Finland, Leningrad in December 1938. The most known exception was Slovak communist Vladimír Clementis, who spent the war in London. After the communist coup d'état, which he helped to organize, he succeeded Jan Masaryk as the Foreign Minister. Then he played a decisive role in organizing of the Czechoslovakia's participation in Operation Balak providing help to the newly founded Israeli Air Force. In 1950 he was forced to resign from his all political positions. He was accused of being a "bourgeois nationalist" and participating in a Trotskyite-Titoite-Zionist conspiracy. After being convicted in the Slánský show trial, he was hanged, along with Rudolf Slánský, on December 3, 1952. His ashes were scattered on a road near Prague. His communist jailers returned his wife only his two pipes and tobacco.

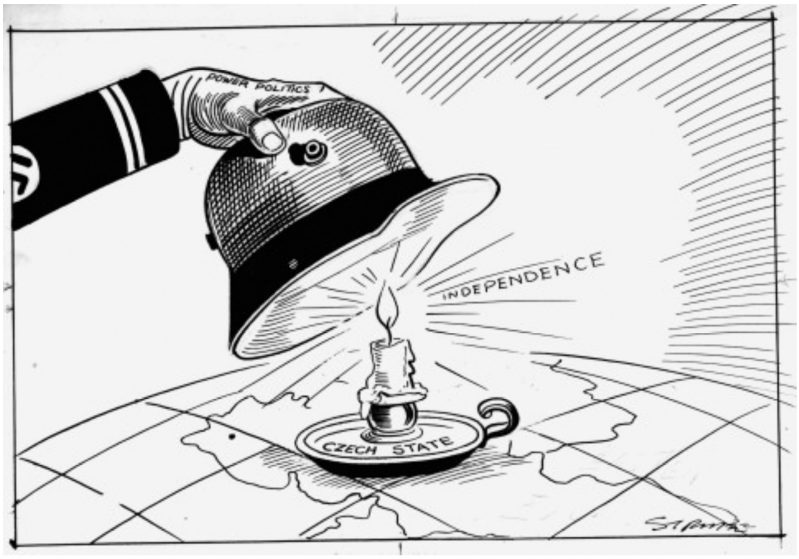


FIGURE 1. Independence of Czechoslovakia as seen by the British cartoonist Sidney "George" Strube, Daily Express March 16, 1939.

the Soviet Union via Czechoslovak communist party, the home resistance was mainly organized from the West.

One of the subdivision of the Czechoslovak National Committee called the Military Administration administered the run of the Czechoslovak army in France. The Chief of the Military Administrations had the duties and competence of the minister of MND. The Military Administration was divided into three units (1st military-political, 2nd generally military and 3rd aviation). The Czechoslovak National Committee in Paris including the Military administration was closed on June 1940 and deployed to Great Britain. Here, the in-exile MND was established in London on 22 July 1940. The organization and competence of the in-exile MND followed closely the organization of the pre-war MND. The structure of MND was later several times reorganized, for the last time in 1944. The Chief of GS in London directed the work of four departments:

1st Department was in charge of maintaining contact with home, the co-operation working with other state authorities, including military missions abroad,

2nd Department was responsible for intelligence agenda,

3rd Department dealt with the issues of training, organization and education,

4th Department was in charge of material and administrative matters. He dealt with orders and records of material intended for Czechoslovak troops.

In the evening of 14 March 1939, the night before the Germans invaded "rump" Czechoslovakia[18], Moravec and 10 of his closest fellow intelligence officers[19] secretly managed to fly away with the most valuable intelligence files and archives from Prague to London in an SIS-chartered KLM Douglas DC-3 plane. The pilot was Dutch captain Vitula, having Czech ancestors dating back to 17th century.[20] This operation, later called by Moravec the operation *Transfer* was organized and realized by Gibson.[21] The rescued archive files were handed over

[18]German occupation of Czechoslovakia started on March 15, 1939 at 6 a.m. when German troops poured into Czechoslovakia. It was the so-called Operation Southeast (Unternehmen Südost).

[19]These officers were: lieutenant colonel Oldřich Tichý, major Emil Strankmüller, major Josef Bartík, major Karel Paleček, major Alois Frank, captain František Fryč, captain Vladimír Cigna, captain Václav Sláma, captain Josef Fořt and captain Jaroslav Tauer. The group should have originally 12 members, however the twelfth member captain Bohumil Dítě due to a car crash on the way back from Bratislava missed a timely return to Prague (since it is reported that the other members of the Dítě's group returned in time, it is possible that a flabbiness in fulfilling of duties was a real reason for the holdup). Dítě was sent to Slovakia as an observer of the events that led to the independence of Slovakia on 15 March 1939 and to the break-up of Czechoslovakia. For a long time it was claimed that the decisive role in the selection of persons taken to London played the requirement that nobody of intelligence officers who came in contact with Agent A-54 should fall in German hands and so to prevent his revelation. Today, this view is taken as outdated. It were more probably requests for expertise in the offensive and defensive intelligence directed against Germany, then the effort not to expose the most committed officers of the German revenge, and last but not least, personal sympathy.

[20]The plane on the line Bucharest–Rotterdam–London extraordinary interlanded at 4 p.m. in a very bad weather in Prague at request of Brits. The airplane took off a quarter to five p.m. It ironically flew over Germany without lights where it flew across a heavy snow storm. It landed on London airport Croydon at 10:40 p.m. the same day. Despite the fact that it was a secret flight journalists waited the surprised group on London airport and the British press informed about the "top secret" flight the next day.

[21] [16]: No explicit trace of this dramatic operation survives in the SIS archives, although on 14 March Gibson requested London to grant him use of an emergency reserve of $1,000 and £200, and reported the same day that he had taken custody of Moravec's "most important intelligence archives" in his office. The Germans indeed entered Prague on 15 March, and over the next two weeks, with deft use of King's Messengers and diplomatic bags, Gibson managed to get the Czechoslovak intelligence archive safety to London, ...

What concerns the families of members of Moravec's eleven, captains Alois Čáslavka and František Fárek subsequently organized an illegal border crossing to Poland for them. Čáslavka with his family and families of Moravec's eleven including Moravec's wife Vlasta and two daughters Hana (born 1921) a Tatiana (born 1922) passed afoot the Moravian–Polish border on the line Radhošť, Morávka, Kotář and Cieszyn on July 2, 1939. They left Poland on the Polish ship Bathory to Denmark and from there on British ship England they arrived to Great Britain in Harwich on July 26, 1939. Some of their baggages were lost in Poland. The daughter Hana married Leo O. S. Disher, Jr. on July 29, 1942 in London.

The after war Moravec's fate was typical for those who returned from West. He returned from London to Prague on May 5, 1945. He was dismissed, disciplined and accused of leaving the position in 1939 and of leaving with a group of officers to Britain without the approval of his superiors, and without taking care of important documents which later fell in the hands of

FIGURE 2. Moravec's eleven source.
http://www.indiannet.eu/home_resistance/czpart2.html

to the British MI6 to be used against Germany.[22] In Britain, from 1940 to 1945, Moravec, code names Pavel, Fischer, Mora, Sudar, served as the head of the intelligence service of the Czechoslovak government-in-exile. He coordinated the Czechoslovak cooperation with SOE. Moravec maintained a secret radio contacts with the Czech anti-Nazi resistance groups and a number of branch offices of the Czechoslovak agents in various places in Europe and Near East. However, there was no real expert in group who could draw attention and help to overcome the difficulties connected with the short wave radio communications. Probably the most important cardinal mistake, having fatal consequences on the home resistance, has roots in Moravec's selection of the members of the group who accompanied him to London. There was no real cryptological expert in the group.

the Germans. On February 26, 1947, the disciplinary proceedings were finally terminated by a decree of the President of the Republic Beneš. On December 1, 1947 he was appointed as the interim commander of the 14th Division in Mladá Boleslav but on February 28, 1948, he was revoked from this position only three days after the communists coup d'état on February 25, 1948. On March 29, 1948 František Moravec emigrated with the help of British intelligence service for the second time. Vlasta Moravcová, his wife, was taken over by a British diplomatic car using a false passport. Their daughters left Czechoslovakia earlier following their husbands and lived at that time already in London. Moravec later worked in USA as an intelligence advisor in the Department of Defense.

[22]For instance, based on a close liaison with Moravec, Gibson inherited some intelligence assets in Hungary in the middle 1941 ([16, p. 414]).

Even if the group took several cipher systems, their practical use was tiny. One of them was [12, p. 67–68] the so-called "dictionary encryption code VA" (slovníkový šifrovací kód VA) intended for military attaches in Stockholm, London and Riga. However it was inactivated in May 1940. Another one was "encryption code I" (šifrový kód I). This was again rather a code. The code words were listed in a book and every code was enciphered by a five digit number giving page, row and column number. Some of the cipher systems were smuggled to the West by home resistance groups. The most important cipher of this group is the cipher denoted as STT (see below)[23]. It was proposed by Josef Růžek, who also designed two further square ciphers Tonda (English Tony) and Pravda (English truth). STT was originally intended for the resistance group Konšelé (English aldermen). It later motivated major Fryč when he designed the cipher systems for parachute airdrops SILVER A, SILVER B and ZINZ.

As C i g á ň' s manuscript proves, London group ignored basic rules for a secure wireless communication what had far-reaching consequences for the home resistance groups. Another example of an ignorance, the details of a proposed cipher system and its changes were distributed through the same open channel as the messages to which the cipher was applied. It is very difficult to find an explanation for such failures.[24]

In the period 1941–1945 the 2nd Department internally consisted of three units: 1. Department of Offensive Intelligence, 2. Defensive Intelligence and 3. Military Wireless Office (Czech abbreviation VRU for Vojenská rádiová ústředna). The core unit was the 1st one which head was major Emil Strankmüller, code name Malý (English: small)[25]. During the years 1941–1945 it was divided into four subdivisions: Intelligence Group (A), Study Group (B), Cipher group (C) and Special group (D). The Cipher Group C dealt with transcription of the encrypted messages from VRU and vice versa with encryption of messages intended for transmission from VRU. The head of the cipher section since 1940 was major Karel Paleček, then since 1942 or 1944 major Alois Frank and finally

[23]Its code name was Králík (English Rabbit), Normální (English normal) or Římská Dva (English Roman two). The last code name was used by intelligence officers.

[24] [13, p. 84]: "Between 1941 and 1942 there were realized 13 parachute airdrops in Protectorate involving together 30 persons. Of them, 25 fell in fights, 2 of them betrayed and were executed after the war and only 3 survived the end of the war. Losses amounted to an incredible 83 %. For comparison, the average Wehrmacht's annual losses on the front in 1941 and 1942 were less than 30 %. If we add hundreds executed civilians for a cooperation with the paratroopers and their executed family members, we must state that the balance of the losses was extremely cruel. How many of these losses can be attributed to not secure ciphers?"

[25]His nickname was Štráda among the members of the 2nd Department.

major Matěj Solanský. Major Alois Čáslavka was also active in the cipher business. Cipherers were at the beginning lieutenants Hugo Weyrich (also written as Vejrich), Rudolf Drbohlav and Rudolf Krzák.[26]

Moravec was responsible for the intelligence agenda of the Czechoslovak government-in-exile till September 1, 1944 when the Ministry of National Defence was reorganized and he become the deputy head of the General Staff for build-up of the Czechoslovak armed forces. Nevertheless, he continually took the control over the intelligence 2nd Department and its activities. The head of the 2nd Department become colonel E. Strankmüller and the head of its Intelligence section, called section A, become František Fryč, but as above it was Strankmüller who daily interfered in its activity. In the Cipher Section (so-called Section C) Fryč was responsible for the used ciphers and administration of keys. Since 1943 this role was taken over by the first lieutenant Václav Knotek. Despite the fact that both Fryč and Knotek took several cryptological courses organized by the British IS the used cipher systems were not applied properly as indicated above, and will be shown below.

Moravec was a bit controversial personality.[27] The list of personalities which had a hostile or strained relation to Moravec was long (for one sample of such persons cf. [21]). For instance, the military resistance in the occupied Czechoslovakia never recognized Moravec as the leading figure of the exile military resistance. Instead of him it was Minister of National Defense in the Czechoslovak government-in-exile general Sergěj Ingr, code names Svatopluk, Silný (English: strong), Jasan (English: ash).[28]

However, in many political aspects Moravec's intuition was correct. For instance, he disagreed with president Beneš, code name Navrátil, in the opinion about Soviet union and it its role in the future. Contrary to Beneš he did not believe the proclaimed fairness of the Soviet politicians. His mistrust was also based on his life experience. He was especially touched by the arrogance of the NKVD colonel Ivan Andrejevich Chichaev (codenamed Vladimir Tikhonov and also known as Tchitch) who served as the NKVD liaison in London from 1941 to 1945.[29] Despite this fact he was often more keen to Chichaev as it was necessary.

[26]In a very detailed report, which first volume has 330 pages, which was written for the communistic interior minister Rudolf Barák in 1957, in the cryptologic group alternated Alois Časlavka, Rudolf Drbohlav, Alois Frank, František Fryč, Miloslav Hladík, Rudolf Krzák, Karel Paleček, and Hugo Vejrich.

[27]Not a very positive description of Moravce's personality can be found in the interrogation report of general Karel Paleček after his arresting by communistic police in 1949.

[28]Ingr came to London on September 17, 1939 where he escaped from Protectorate via Paris. He was withdrawn from the position of minister on 19 September 1944 following a strong pressure of the exiled leadership of the Czechoslovak communist Party in Moscow, however.

[29]Chichaev (Čičajev) cover was the position of the counselor at the Soviet embassy. His wife Ksenia Mitrofanovna served as secretary and cipher clerk. Later the chargé d'affairs Chichaev

For instance, on Oct. 20, 1941 three men met at a lunch in one luxury restaurant in London: major Desmon Morton, an associate of Winston Churchill, Raymond E. Lee, a trustee of US government in London and Moravec. The topic of their confidential discussion were details about the prominent politician in Nazi Germany Rudolf Hess who on 10 May 1941 landed in Great Britain. The Soviets were keen to learn the real aim of his flight to Great Britain from the very beginning because they were afraid what is the goal of this unexpected visit: offer of a negotiated peace or even an anti-Bolshevik partnership. Shortly after this lunch Moravec met Chichaev and he disclosed him the details which he learned during the above conversation, e.g., that the British knew about the German plans to overfall of Soviet Union. The content of this conversation shortly afterwards reported Berija to Stalin and Molotov. This action casts a different light on Moravec activities, or perhaps activities of the whole group, since Moravec was certainly not a friend of Soviets, but a secret collaboration of the Czechoslovak in-exile goverment with Soviet Union forced him to play double game with the British. This astonishing game was started in January 1941 when colonel Píka signed on behalf of the Czechoslovak Government in exile with Soviet general Fokin in Istanbul a secret Soviet-Czechoslovak military agreement which included also the cooperation on the intelligence field.[30]The British were kept dark about this agreement.

Surprisingly, Moravec was not always down-to-earth as one would expect from an intelligence officer. He strongly overestimated the role of his top agent A-54 Paul Thümmel.[31] In this connection it is interesting to note that Beneš doubted about the role of A-54 with the words: *Do you consider his reports to be correct, are they not a part of a well-dressed bluff?* (cf. [11, p. 316–317]). As already mentioned, it is almost sure that Thümmel was a double agent or even worse

under ambassador Valerián Alexandrovič Zorin on the Soviet embassy in Prague drove the Soviet spies in Czechoslovakia where he used his experience gained in his prewar participation on the Sovietization of the Baltic states.

[30]Heliodor Píka was a Czechoslovak army officer. In 1941 he was appointed chief of the Czechoslovak Military Mission to the Soviet Union in Moscow. He was loyal to the in-exile London-based government and supported their democratic policies despite Soviet opposition. During his stay in Soviet Union he was under constant pressure from the Soviets to betray the Czechoslovak in-exile government. Moravec who preferred to contact Chichaev instead to send material via Píka's office in Moscow, prepared Píka many annoying moments in this way. On the other hand, also the behavior of NKVD was not very friendly (opening the post in Stockholm, office-breaking in his office in Moscow, blocking of his sender, etc.) in attempts to obtain some intelligence material ([29, p. 252–253]). Píka was executed by communist regime after a show trial in 1949. In 1992 he was posthumously promoted to the rank of general.

[31]In 1975 in New York there appeared Moravec's memoirs *Master of Spies*, which Czech edition was issued by Czech emigrant Josef Škvorecký under the title *A spy who was not believed* in 1977 (cf. [23]). In these memoirs Moravec portrays his Agent A-54 as one of the greatest spies during WWII.

a German Abwehr agent of operation camouflage — as C i g á ň tried to prove in [6], [7]. Thümmel besides these aspects of his activity without doubt used the willingness of the Czechoslovak intelligence authorities to pay for his "selected" information, parts of which was beyond his "official duty in the intelligence game". The money he needed to cover his above standard way of life.[32] Nevertheless, each of his motives opens questions which are hard to answer today. For instance the author of [13, p. 65–66] has the following comment:

> In the book [20] the authors argue that Agent A-54 was an agent of the operation camouflage, who worked for both parties and used our resistance led by colonel Moravec in London to disinform the British. I am not a historian, but the following question crosses my layman mind which strongly impugns the truth of their claim: Why have the Germans got rid of such a source of disinformation so soon? At the beginning of 1942, they were far from not having grounds to disinform the British. On the battlefields it was not yet decided. In addition, most of the messages heading to London were under their control using this channel. What better one would wish? By the liquidation of the resistance group ÚVOD and of the agent A-54 they lost an important channel for sending their disinformation. This engagement of the Germans could be reasonably justified a year later when they were beaten at Stalingrad. Is it still possible to find a true answer on this questions today?

The reader interested about agent A-54 should also consult [22].

3. Technical remarks to the radio communications during WWII

K. C i g á ň starts his manuscript [8] with the following comments in the introduction:

> The significance of cryptology has increased considerably with the development of radiotelegraphy. Already in the first and especially in the 2nd World War, the struggling powers had powerful units in the structures of their armies involved in this activity. From our point of view, it must be mentioned that the fascist Germany built up the so-called Funkabwehr which was directly subordinated to Oberkommando des Heeres (OKH). It was very well equipped both with the material and with numerous personal staff consisting of radio reconnoiters, gonio troops and decipherers.

[32]Thümmel had a weakness for women. For instance, Thümmel, aka Dr. Holm, met with many representatives of the Film Club in Lucerna Palace in Prague which owner was Miloš Havel. To Thümmel's circle of friends also belonged the well known Czech actress Lída Baarová (1914–2000) known for her contacts with the Nazis. The most known is her alleged affair with Reich Minister of Propaganda Joseph Goebbels. She also met four times with Adolf Hitler. Nevertheless, Baarová was followed by the Gestapo and the Sicheheitsdienstin in the Protectorate. Thümmel helped her when she had problems with Gestapo. She said about him: "He never told me what he was doing and who he was. From his comments and some of his opinions, however, I had a feeling that he was not an enemy of the Czechs." Another remarkable story says that Paul Thümmel tried to recruit her for a collaboration with Nazis. A-54 also introduced her to Admiral Canaris who apparently tried to achieve the same.

> The importance of this field of activity was not sufficiently recognized by the commanders of the Czechoslovak army before the Second World War. This reflected in its activity levels and potentialities. The cryptology group included 3–4 cryptologists, who otherwise enjoyed the trust but were regarded as witty beings. In reality they could not handle all the tasks that had to be solved in this respect, however. Therefore, no one can blame the army group in London, which took control over the cipher services after March 15, 1939, that they introduced and adopted such a dangerous cipher system which we shall treat here in more details.
>
> After World War II, various experts rumbled that the Gestapo had decimated the Czech resistance taking advantage of their breaking of the ciphers used by London MND. This claims were based on a testimony given by captured German cryptologists who revealed that they solved two cipher systems. Their claims are not completely confirmed when compared with the archived cipher keys used by the London head office. To their solution there were often needed desirable requirements and assumptions, which could occur only occasionally, and in long periods. Nor the second system in their presented operating instructions was so unambiguous, for the cryptographic keys of the described character were not found in the London materials. It was based on a simple substitution with a simple transposition followed by a super-encryption. Nobody had the idea at that time what monstrous unfortunate simplifications the governing authorities of the in London MND introduced. To say truth I alone realized these facts not before 1989.
>
> From the testimonies of German cryptologists we also learned that in the Funkabwehr headquarters in Berlin they were engaged in solving the Czech ciphers by a "mathematical method". And right this very knowledge, along with other facts, has led me to try to get at the bottom of this method. It took me a year of work.[33] I have to thank to A. T i c h ý for writing the book [30]. In it I found valuable cipher data about the cipher keys used by the parachute groups Antimony that helped me to understand something beyond all understanding — to divide a complex cipher system into three separate simple ones.
>
> The fact that the Abwehr knew the content of the London MND radio communication for five years has to be declared as a national disaster. The extent of damage should be evaluated by historians using the archived radiotelegrams. There should be more than 22,000 of them. I could only recommend that a specialist for the radio reconnaissance and a cryptologic expert will be co-opt to do this job.

To the words of C i g á ň concerning non-preparedness of the Czechoslovak radio reconnaissance it should be added that solely the wartime experience showed not only the importance of interception and decryption of transmitted information but also the necessity to establish permanent agency conspiracy net of units abroad addicted to this and similar tasks for gathering various strategic information. Besides traditional courier links, personal connections, various impersonal links, or postal links using diverse secrecy tricks under specific conditions etc., the build up of a reliable agency network based on a radio communication was

[33]Consult [24] for more details. ŠP

a necessary assumption for a successful intelligence work. Nevertheless, it must be said that Czechoslovak intelligence did not pay sufficient attention to the importance of the build-up of a reliable network based on radio wireless connection for intelligence purposes. On the other side there were also objective technical problems connected with such a task. Wireless communication using short waves was discovered only in the first half twenties of the 20th century. The difficulty with their usage was connected with the fact that short waves behave erratically because the propagation conditions of radio shortwave signals are very variable. They depend on the height of the ionosphere, on the power of solar radiation, particularly of the ultraviolet light, the condition of the earth's magnetism to mention some of them. In the early thirties a number of scientific institutions started to study the laws by which it would be possible to plan the optimal operating frequencies. For instance, only in June 1942 the British Admiralty issued service tables *Optimum Frequency Band Tables* based on the methodology proposed by the Inter-service Ionosphere Bureau.

Thus Czechoslovakia was not alone, the outbreak of war found France or Great Britain unprepared too — without any agency stations, no organization providing operating agency networks, and basically no experts and no systematic experience with the shortwave transmission traffic. Contrary to the military intelligence service of the Red Army which in a close cooperation with the Comintern built up a network of "sleeping agents" equipped with suitable radio transmitters.[34] Unfortunately till the occupation of Czechoslovakia in 1939 the competent authorities did not succeed to build up such wireless agency network abroad. The corresponding authorities began to be seriously interested in such project only around 1937, and this was too late. It is reported that Růžek took great care in the radio interception that allowed a retrieval of encrypted messages from potentially hostile networks, mainly German and Hungarian ones. The only specialist with extensive technical knowledge and operational experience for radio connection in the 2nd Department was Jan Budík[35], since 1936 a civilian employee of the 2nd Department, who for family reasons (concerns about the rest of his family), however, refused later to join Moravec in London (as, by the way, did also Růžek). Thus in the group of intelligence officers leaving Czechoslovakia was no expert in the radio communications and in cryptology, what also subsequently contributed to some fatal consequences in the radio communication. British SIS build a transmitter for the Czechoslovak intelligence on Dukes Hill

[34]For instance, the qualified radio-telegraphic staff equipped with cipher instructions and radio transmitters was sent to Czechoslovakia in advance. As it is noted in [11, p. 43] the connection from Prague was planned to be held in the German language to ensure the connection also with Austrian communist party. The traffic was launched on the Comintern impuls probably on June 7, 1939.

[35]Ironically enough the name Budík means *alarm clock* in Czech and his code name was "Inženýr Hodina" (engineer Hour). He was an amateur radio operator with call sign OK 1 AU.

at Woldingham near London, which was used for radio communication with intelligence branch offices abroad an with the domestic resistance since April 1940. Here was the residence of VRU. However, an autonomic Czechoslovak center for radio traffic was established on 1 September 1939 in London on West Dulwich, Rosedalo Road. It had to disposal one borrowed radio transmitter [12, p. 46].

The first radio communication where the home resistance succeeded to establish a permanent connection was via Warsaw branch office, code name Marie, in the period 1–10 August 1939. Once in the night and once during the day they (operators sergeants Karel Broukal and Václav Retich) communicated using the so-called Q-codes. Otherwise the traffic between Warsaw and London has been mediated by the British radio transmitters. However, for the transmission of Czechoslovak radiograms the Czechoslovak ciphers were used details of which were not given to the Brits. They simple obtained the enciphered messages for the transmissions. Actually in August 1939 five British wireless radiotransmitters were smuggled to Hájíček, four of which he located in Warsaw, Brno, Prague and Bratislava. As already mentioned in the same time brought also major Emil Strankmüller a transmitter and a cipher system from Britain to agent Vaněk living in Stockholm.[36] The wireless communication with the branch office in Jerusalem started on 5 September 1939.

Poland, and especially Warsaw, had a key position in the mutual connection between the outland and the home. For instance, some sources mention that around 25.000 written messages for families and friends of emigrants went through the Poland. This all was done despite discrepancies between Polish and Czechoslovak authorities. After the defeat of Poland, the intelligence branch office in Warsaw moved to Bucharest in September 1939.

On October 28, 1939 (20th anniversary of establishment of Czechoslovakia) the first wireless connection between Prague and Paris (code name for the branch office in Paris was Karel), and one month later also with London, was established.

4. Description of the STP cipher

The Czechoslovak exile government in London used over 50 different ciphers during the war years. One of the cipher systems used by the in-exile MND in London in the period 1940 till 1945 was proposed by Josef Růžek and was in a conspiratory way (see the details see below) transferred to Paris to major Fryč who used it in the wireless radiotelegraphic communication with the home resistance, the foreign branch offices and the parachutists groups dropped in Protectorate. Technically the particular ciphers were composed from a combination of substitutions, transpositions and a periodic super-encryption. The code

[36] V. Vaněk used an STT cipher.

names of their concrete instances were encoded using the initial characters S, T and P of the used particular cryptographic transformations. Here the characters S, T and P stand for substitution, transposition and for an addition of a periodically repeated keyword, respectively. More precisely:

Step of type S: A substitution in which the plaintext characters are replaced by their numeric (two digit) equivalents. As characters of the plaintext were accepted the characters of the Czech alphabet (including the characters with diacritical marks) usually extended by three German umlauts, that is 31 letters, say encoded by numbers from 01 to 31. Then the set of allowed characters contained 5 punctuation marks, say encoded by numbers 32 to 36, and finally 10 digits, say encoded by numbers 40 to 49.

Step of type T: A column-wise transposition based on a passphrase of a prescribed length which was taken from a part of a piece of text from a prearranged source (book, song, etc.).

Step of type P: A super-encryption using a passphrase of a prescribed length which was again taken from a piece of text from a prearranged source (book, song, etc.). Here the passphrase characters are replaced by their numerical equivalents in such a way that the tens digits were not used. This key consisting of simple digits was then periodically added (or subtracted) without carrying to (from) the string obtained in Step T.

For instance, the used ciphers were denoted as ST, TTS, STT, SP or STP ciphers. Thus the abbreviation STP denotes a cryptographic transformation consisting of a cascade of three cryptographic transformations applied step by step: in the first one the characters of the plaintext are replaced by their numerical equivalents, then there followed an application of a transposition in such a way that in every column always stays only one digit (that is the tens and units are separated when divided in columns). Finally the resulting chain of digits is super-encrypted by adding digit by digit a numerical equivalent of the second passphrase in such a way that the addition is done without carrying.

Concretely, the particular steps S, T and P were modified as follows:

Step S: It seems that the substitution table was not uniquely determined. In general, the characters of the plaintext were substituted by two digit numbers. In [14, p. 307] it is mentioned that the western branch offices of the 2nd Department and STP users used the alphabet containing besides Czech characters with diacritic caron sign (háček, haček or hachek from Czech) also three German umlauts Ä, Ö and Ü. In Czech and Slovak alphabet "CH" denotes in script a consonant understood as one character (in International Phonetic Alphabet /x/). But in the substitution step it was sometimes (depending on instructions) taken as one character (as in the footnote below) or its characters were taken separately as "C"

followed by "H". The basic form of the substitution table as given in [14] is [37]

A	Ä	B	C	Č	D	E	Ě	F	G	H	I	J	K	L	M	N	O	Ö	P
01	02	03	04	05	06	07	08	09	10	11	12	13	14	15	16	17	18	19	20
Q	R	Ř	S	Š	T	U	Ü	V	W	X	Y	Z	Ž	.	:	-	/	?	0
21	22	23	24	25	26	27	28	29	30	31	32	33	34	35	36	37	38	39	40
1	2	3	4	5	6	7	8	9											
41	42	43	44	45	46	47	48	49											

Hyphen "-" was substituted for the space between words. This alphabet was valid for the first day in month. It was usually shifted by the date. On the 20th day of the month it started with A = 20. In some keys the shift 15 was used for the 1st, 11th, 21st and 31st day of the month, shift 23 for the 2nd, 12th, 22nd day, etc. Other keys used a 10×10 square pattern, or a 5×10 rectangular fields for generation of the substitution key. To scramble the substitution pattern in a more complex fashion a deranged substitution table was generated using a passphrase which letters were filled in a geometric pattern in an agreed manner and the unfilled boxes were filled with the remaining unused characters. For instance, the passphrase "KDYBYCH MĚL JÍT NA KRAJ SVĚTA"[38] used by the parachute airdrop BARIUM gave the following substitution table

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

In keys based solely on alphabet letters, the digits and punctuation marks, were coded using the following table

WA	dot	WF	exclamation mark	WI	1	WL	4	WO	7
WC	comma	WG	question mark	WJ	2	WM	5	WP	8
WE	division slash	WH	zero	WK	3	WN	6	WQ	9

[37] Compare with a modification used in communication with Heliodor Píka in Moscow were a system STT was used [12, p. 130]

A	B	C	Č	D	E	Ě	F	G	H	CH	I	J	K	L	M	N	O	P	Q	R
51	41	27	17	43	90	82	35	07	36	08	72	64	63	80	19	93	81	37	42	28
Ř	S	Š	T	U	V	W	X	Y	Z	Ž				.	?	:	!	,	-	/
18	71	25	62	65	50	52	37	46	73	59				47	74	38	83	29	92	56
1	2	3	4	5	6	7	8	9	0					separation signs codes						
11	22	33	44	55	66	77	88	99	00							01	23	45	67	89

Further examples of substitution tables are given in [11, p. 320–321].

[38] If I had to go to the brink of the world.

There were also other modifications in use, e.g., the alphabet used for the super-encryption in Step P was coded differently as that used for substitution of the plaintext characters.

The final length of the ciphertext after the substitution was adjusted by adding a suitable group of arbitrary digits in such a way that the total length of the ciphertext is divisible by 5. It was recommended to use digits 5, 6, 7, 8, or 9 in this padding.

C i g á ň uses the following substitution table in [8]:

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

Step T: The length of the passphrase used in step T was between 15 and 25 characters.

Step P: The descriptions how the passphrase used in this step is chosen differs in the quoted sources. For instance, in [14] or [15, p. 139] it is required that the length of the passphrase in Step P is 10, while in [30] no length limit is mentioned. In his manuscript [8] C i g á ň also does not require a bound for the key length in Step P. Actually he takes a key of length 15 in one of his demonstrating examples (cf. [24]). Nevertheless, as it follows from his critics of the system (cf. [24]) the length 10 is optimal. C i g á ň [8] takes for the passphrase used in step P the same piece of text which was used as the passphrase in Step T. However, according to [30] the passphrase for Step P is generated from a text which does not coincide with that used in Step T.[39]

What concerns the mentioned differences notice that as it seems the original description with usage instructions of the STP system is lost in the meantime, and so it is not possible to decide between some published descriptions of its usage. At this occasion it must be mentioned, that in the night 14/15 March 1939 before arrival of German troops in Prague all intelligence material in the deposits of GS in Prague was reduced to ashes in the yard of GS. However, the corresponding material in subordinated branch offices outside Prague remained mostly untouched. An interesting fact can be found in the interrogation of Jaroslav Hájíček (code name Petr), in that time already in the rank of a colonel, by the communistic police in April 1950. Hájíček was member of the 2nd Department since 1937. He first worked in the so-called German section and

[39]In the interrogation after WWII Jaroslav Hájíček was confronted with some complaints in office in Belgrade. Without specifying the cipher system he said that the cipherer was allowed to select the passwords. The first transposition passphrase was recommended to be of length 12 till 20 characters, the length of the second transposition passphrase was limited to 10–15 characters. The cipherer usually did not know to whom the passphrases were assigned.

after being promoted to major he served as head of the Hungarian section. In the interrogation protocol after the war[40] he mentioned that when he together with Růžek burned the cipher keys as it was ordered, Růžek decided not to burn those used with communication with military attaches in Paris, London and Warsaw, where the attaches still were in their positions. These three keys were then kept by Hájíček in his home for a possible later use.[41] Then he gives a detailed report on how several functional radio transmitters were constructed and used in radio communication with Paris, London and Warsaw. He also mentioned here that it was Růžek who trained Vladimír Krajina[42] and some students[43] how to encrypt documents for broadcasting.[44] He also writes that the person who in-

[40]What concerns Hájíček note that he was one of the key figures of the Czech anti-Nazi resistance in the Protectorate in 1939. He participated, among other things, in the organization of the radiotelegraphic connection with the West and the organization of the espionage network of the anti-Nazi resistance organization Obrana Národa (English: Defence of the Nation) that existed from 1939 to 1945. On 25 November 1939, when the Nazis learned of Hájíček's activities he succeeded illegally to left the Protectorate. (Hájíček with colonel Čeněk Kudláček left Bohemia with the help of conductor Zeman. The route led through Slovakia, Hungary to Yugoslavia.) He then served as a Czechoslovak intelligence officer in Czechoslovak military missions in Belgrade and Haifa. From 1942 till 1946 he led the Czechoslovak Intelligence Office in Istanbul (he came here in contact with the US intelligence officer and the legend of the first Czechoslovak foreign resistance — captain Viktor Emanuel Voska). At the beginning of 1946, after his return to Czechoslovakia, already in the rank of lieutenant colonel, he was deployed back to the Second Department, but after half a year he was sent to garrison town Tábor. On June 4, 1949, he was arrested and sentenced to 11 months of imprisonment for a careless keeping of the state secrets. He was arrested again on June 2, 1956 and accused of organizing a leaflet anti-communistic campaign to support student demands during demonstrations in May 1956. On September 26, 1956, he was found guilty and sentenced to 3 years unconditionally.

[41]In [15, p. 128] it is mentioned that Hájíček proposed to use the cipher system called Mode 30 (Czech: Způsob 30) in August 1939 in the first wireless communication between Prague, Warsaw and Paris. It was an SP cipher.

[42]Vladimír Krajina (1905–1993) was a graduate of the Charles University in Prague, where he graduated with the earned degree of D.Sc. cum laude in 1927. He was the leader of the Czech underground resistance group "Central Leadership of Home Resistance" (abbr. ÚVOD). After being captured in January 1943, he was suspected that he unveiled the encryption keys to Gestapo. After the war, he returned to Charles University as a professor. He was elected to the Czech parliament in 1945 and served as General Secretary of the largest democratic party––Socialist Party. When the communists took over the political power in February 25, 1948, he immigrated to Canada and joined the UBC Botany Department in Vancouver in 1949 where he taught plant ecology for 24 years.

[43]For the list of Krajina's cipherers and radio telegraphists see [22, p. 91].

[44]According to [15, p. 129] Krajina used a TTS cipher system (a concrete example is given here for demonstration purposes), which, as stated here, was used by the in-exile MND in London since autumn 1939 till the middle of 1941 (and occasionally till the middle of 1942). However, according to [19] Krajina used the cipher given him by major Havlíček(?) in November 1939 till his detainees by Gestapo on 31 January 1943.

After the German occupation the first exchange of intelligence messages was done using courier services. For instance, in 1939 the surface mail abroad was sent through the French embassy

troduced him to Krajina (and consequently Krajina with Růžek) was Professor Jan Bělehrádek.[45] He also mentioned that Růžek helped him in preparation of ciphers for wireless radiotransmitters.

The mostly published version of the origin of the STP cipher says that its author was Růžek after an initiative of the home resistance and that it was subsequently smuggled to London. Nevertheless, there are many differences in details about the first ciphers proposed for the use in the communication between the home resistance and the in-exile groups. For instance, in [17] using a tendentious and unbalanced language loyal to the communist anti-Beneš ideology of that time it is mentioned that the group of "Beneš followers" tried to prepare for communication a vocabulary code based on a French vocabulary. One such "follower" — the later secretary of Beneš during his in-exile presidency in London — Dr. Jaromír Smutný since November 1938 Czechoslovak general counselor in Istanbul[46], sent at the end of March 1939 through Dr. Jiří Hejda[47], former director of ČKD (Českomoravská Kolben-Daněk), one of the largest engineering companies in the former Czechoslovakia, during one of his business trips in Istanbul a cipher stashed in a toothpaste tube to Prague. The tube ended in the hands of another "Beneš follower" Prokop Drtina[48] who writes in

where it was brought by Hájíček, or it was smuggled to Warsaw by the sleeping car conductor Zeman (cover name Černý Turek; English Black Turk). Zeman was generally used as a courier on the sleeping cars of Wagons-Lits. Till the fall of Poland on the line Prague–Warsaw, after the fall of Poland on the line Prague–Belgrade–Istanbul. He was also used to deliver the correspondence to the Yugoslav General Consulate in Prague, where Božidar Stefanovič an official of this consulate collaborated with the Czechoslovak resistance. After an intervention of German authorities Zeman was fired from this position in May 1940. He was executed by Gestapo in 1942.

[45]Jan Bělehrádek (1896–1980) was professor of medicine at Charles University since 1935. He emigrated after the communistic coup d'etat in 1948.

[46]After German occupation Smutný went to Paris and joint the foreign resistance. After return of president Beneš to London from USA he became his assistant and finally his chancellor, a position he held till Beneš' abdication in 1948. In June 1949 he succeeded to emigrate to the West.

[47]Jiří Hejda (1895–1985) was a Czech writer, publicist, politician and national economist. He participated in the anti-Nazi resistance. After 1945 he became an important representative of the Czechoslovak National Socialist Party. He was a member of the Central Planning Commission, which prepared a biennial plan for the years 1947–1948. After the communistic coup in February 1948 he was included in the political trial with Milada Horáková and others and was sentenced to life in 1950. In 1962 he was conditionally released. Milada Horáková (1901–1950) in the same trial was sentenced to death on fabricated charges of conspiracy and treason.

[48]Prokop Drtina (1900–1980) was a Czech lawyer and politician. Before World War II, he was Secretary of President Edvard Beneš and during WWII he was active as his close associate. He left Protectorate on 26 December 1939. After the war he became Minister of Justice and was one of the democratic ministers who resigned on 20 February 1948. The demission of the part of the government opened the door for the communistic coup d'etat eight days later. In December 1953 he was sentenced to 15 years imprisonment on the basis of fabricated accusations.

his memoirs [9, p. 356]: *The cipher was used for some messages, but soon this cipher amateurism was replaced by a perfect cipher of military and other experts.* Within two months Drtina got into contact through the middleman Dr. Drábek with Krajina, who offered him a collaboration. After 28 October, when the first wireless transmission with London was established, both met almost daily because Krajina enciphered the messages in the Botanic Institute where he worked which was close to the Supreme Administrative Court where Drtina worked.[49]

An additional involution appears on the scene with the person of Dr. Jaroslav Císař, a former secretary of president Masaryk.[50] In [27, p. 227–228] it is claimed that using his mathematical knowledge he designed a cipher system and he trained a group of students how to use it. On 5 July 1939 he left Czechoslovakia and through Yugoslavia he reached London where he on 18 July handed over the cipher in the office of the President Beneš. The author of [27, p. 228] also says that Císař before his departure introduced Krajina to Hájíček and Růžek, who subsequently instructed him how to encrypt and decrypt messages. It is opinion of the author of this paper that this was not the cipher system proposed by Císař, but that proposed by Růžek. In [12, p. 43] we can read that Císař brought a cipher to Paris on 16 July 1939 (!). The cipher is not closely specified. In the interrogation reports written by Hajíček after the war he says that after the German occupation in March 1939 he organized that some cipher systems from those rescued by Růžek before Germans were sent to Paris to establish a wireless connection between home and branch offices abroad. Thus everything indicates that Císař brought a cipher proposed by Růžek.

On the same page [12, p. 43] we can also read that the resistance group Konšelé sent a letter to Paris on 28 July 1939 containing a "square" cipher designed by Růžek, and that Konšelé sent another new cipher called Pravda to London office at the beginning of November.

[49]On the other hand, Hájíček gave the messages for encryption to Krajina or one of his friends in the building of the technical university on the Charles Square in Prague, or in a box in a book sellers shop. The received messages were deciphered by Krajina and given by Krajina exclusively to Hájíček, and only seldom to his deputy colonel Sázavský.

[50]Dr. Jaroslav Císař (1894–1983) was a Czech astronomer, publicist, poet, translator, manager and linguist. In 1912 he left Austrian Empire to USA. Here he devoted himself to various activities within the Czech vereins. He collaborated with Emanuel Voska and through him with the later President Masaryk. Besides this he visited the lectures of mathematics and physics on Columbia University in New York and finally graduated from The College of New York City in 1917. During the First World War he was active in the foreign resistance. Since September 1916 he was involved in the preparation of the Czechoslovak troops in the Canadian Army and he enrolled the Canadian army in October 1916 and later in May 1917 the Army of the United States. In May 1918 he joined the Czechoslovak Legion in France. In period 1918 to 1919 he worked as a personal secretary of T. G. Masaryk. In 1938 he emigrated to London where he joined the Czechoslovak Army on 17 January 1940. After WWII he returned back to Czechoslovakia which he again left on 13 July 1949. He worked as an astronomer at the University of St. Andrews. He returned to his homeland in 1980.

Back to the STP cipher. In this direction C i g á ň writes: It [i.e., the STP cipher] is exhaustively described in [30]. In addition, there are several cipher keys designed on its basis. They can be found in the intelligence archive of the GS. I myself took part in their archiving in the fifties.

The STP system was used in the period 1940–1945 in the wireless communications between branch offices abroad and since July 1941 also in the correspondence with underground resistance groups. The concrete used keys were changed from case to case. For instance, in [14, p. 190, 244,] two code names are mentioned for sets of the passphrases used with STP encryption: Anna was used in connections with Slovakia in 1944, and Běta was used in connections with Protectorate in the same year.

Shortly before Moravec's departure to London Růžek allegedly acquainted him with the encryption and decryption rules and with the requirements for a safe usage of cipher systems which Růžek proposed to use. One of these systems was the TTS cipher system [15, p. 127]. Růžek's recommendation was not to use it regularly. Nevertheless, everything suggests that Moravec (and not only him) ignored this and other important advices and rules. Principles how to break both components of such systems and their simple combination was well known in that time.

For instance, from the time of the US Civil war it was known that two or more intercepted cipher texts of the same length and both enciphered by the same transposition cipher can be used to decipher them. Consequently, a cipher system of type TTS is not secure. However, the double transposition of the cipher system of type STT causes separation of the decimal digits from the unit ones, and the anagramming method applicable for a solution of the TTS system does not work in this case, i.e., STT cipher systems are under certain circumstances more secure in general than the TTS ones. Thus in cryptographic circles it was widely known that these systems should be used only occasionally, subject to certain safety rules (e.g., to prevent messages of the same length enciphered by the same key). Such strict rules are also valid for usage of the STP cipher systems because they are also predisposed for cracking if similar rules are not strictly kept. As it seems the authorities of the in-exile MND ignored these facts.

A typical head of the Czech enciphered radiotelegram consisted of three numbers: the first number was the serial number of the telegram, the second one gave the number of the sent cipher symbols (characters or numbers)[51], and the third one represented the day number. Then followed the cipher text in which the symbols were grouped in groups of five. The last quintuple was an identification one which usually also contained the number of the sent cipher symbols in the middle group [14, p. 28, 306]. In [14] several real examples of telegram encrypted using a STP cipher are given. One of the telegrams on p. 394 is:

[51]In Cigáň's examples the second number gives the number of pentagraphs.

7134-345-17

39801	41857	16328	56717	50443	06190	28393	05407	57208	41049
96521	50797	57725	52968	49504	42955	51301	85110	31322	97410
67410	55580	23361	77882	63340	17914	30462	97307	44161	75680
23271	54386	77897	50035	67015	59807	56502	46746	99792	41952
28006	51958	47819	31756	33133	85403	30200	57602	23360	55492
37360	75409	23242	15314	58361	74482	20261	75296	31310	55981
96396	48908	77801	56058	97806	41925	47501	48072	73458	

In the book one possibility how to break the telegram is shown. It is based on the fact that on the same day several telegrams having the same length were sent. Unfortunately, a complete cipher passphrases reconstruction is not finished. The textual versions of the passphrases (or even from where they were taken) is not given. It deciphered wording says: **7134**: *10. března skončen v Marseille náklad lodí: ROUSSILLON TONKINOIS. V sete lodí: S.V.A.7. Officielní cíl Alžír vskutku pro Janov. Charakteristiky lodí žádejte v Bureau VERITAS.*[52]

Another method of a complete solution of a STP cipher can be found in [24]. Its author is C i g á ň and it presents the mentioned "mathematical" method. The tag "mathematical" has roots in the interrogation of two German cryptologists in summer 1945 in a camp for POW near Brno. The method using which they solved Czechoslovak ciphers they characterized as a mathematical method. As already mentioned, C i g á ň spent several decades to (re)discover the essence of this method. He described the corresponding method in [8], and its details were reproduced in [24].

For the convenience of the reader we describe shortly the conversion of passphrases to their digital form used for encryption. Suppose that our passphrase is the already mentioned one: KDYBYCH MĚL JÍT NA KRAJ SVĚTA.[53]

A. Generation of the numerical form of passphrase 1: Let the length of the used segment of the passphrase be 21. It does not mean that we take the specified number of characters (in this case 21) from the passphrase. For, firstly, if the last letter fell within a word, the passphrase was taken till the end of the word. Secondly, the total length of the passphrase should be odd. In details, we start to write the numbers under the letters from left to right keeping their lexicographic order. Thus we start with numbering at the first A in word NA, then continue with A in KRAJ, and SVĚTA (diacritic signs are not taken into account). With B we start from the beginning, because there is no B after the

[52]On March 10 end of shipload in Marseilles: ROUSSILLON TONKINOIS. In boat set: S.V.A.7. Official goal Algiers, really Genoa. Request characteristics of the ships in Bureau VERITAS.

[53]Cigáň [8] used for a conversion example (cf. also [24]) the passphrase system used by parachute airdrop ANTIMONA which was based on the Czech folk song *Nešťastný šafářův dvoreček* [30, p. 228].

last occurrence of A, etc. Number 19 and 20 is S and T in SVĚTA, 21 is T in JÍT. Not yet numbered letter V, and twice Y are not numbered even if they are within the initial segment of 21 letters from the beginning, due to the rule that complete words are taken at the start of the numbering.

K	D	Y	B	Y	C	H	M	Ě	L	J	Í	T	N	A	K	R	A	J	S	V	Ě	T	A
←								minimal length 21												→			
				–										1			2						3
			4		5																		
	6							7													8		
						9					10							11					
									12						13								
14										15													
							16						17			18			19			20	
												21								–			
		–		–																			

14	6	–	4	–	5	9	16	7	15	12	10	21	17	1	13	18	2	11	19	–	8	20	3

This yields the transposition key:

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

B. Generation of the numerical form of passphrase 2: Now we proceed in a similar way but from the right to the left. Let the length of the passphrase 2 is set to be 10. Now is the real length, but taken from the end

K	D	Y	B	Y	C	H	M	Ě	L	J	Í	T	N	A	K	R	A	J	S	V	Ě	T	A
														←			length 10						→
														1	6	7	2	5	8	10	4	9	3

After deletion of tens digits we obtain the key "1 6 7 2 5 8 0 4 9 3" for the final super-encryption "perturbation" of the cipher text obtained after the preceding transposition. This operation was called "cutworm" by German decoders.

5. Excerpts from Cigáň's manuscript [8] on STP cipher

This section is based on C i g á ň' s manuscript [8] which is written in Slovak. A free translation of selected parts has been made by the author of the present paper, who takes the full responsibility for the translation and the selection of the translated material. The footnotes made by him are denoted by ŠP.

In [8] C i g á ň gives a cryptanalysis of weak points of the STP cipher system (cf. [24] for more details). As the Cigáň notes it is very surprising that a cryptanalysis of the system was not done neither by Czechoslovak nor by British cryptanalysts.

5.1. Scope of usage and the entities using the STP cipher system

Czechoslovak intelligence officers in London used the STP cipher system for 5 years. They introduced it successively into the radio traffic communication. Exact time determination when this cipher system was introduced into the communication with concrete objects would only be possible after a long study of the archived telegrams of the MND in London. For this moment we take the data published by various authors and by retired František Fryč himself.

a) In the home resistance the system was used by the following resistance groups:
   - group "Central Leadership of Home Resistance" (ÚSTŘEDNÍ VEDENÍ ODBOJE DOMÁCÍHO, abbreviated ÚVOD)[54] — since the establishment of the first connection London–Prague using the radio transmitter SPARTA 1 in 1940,
   - group "Nation's Defence" (OBRANA NÁRODA, abbr. ON) — since establishment of connection with agent A-54 and lieutenant colonel Balabán in the second half of 1940, or since establishing a direct connection with radio transmitter SPARTA 2 by March 28, 1941,
   - group JINDRA[55] — from 31 May till 22 June 1942;

b) External radio-telegraphic branch offices of the resistance:
   – Geneva – lieut. col. K. Sedláček,

[54]The Central Leadership of Home Resistance was an important resistance group which served as the principal intermediary between Beneš and the Protectorate. It was established in 1941. The three major resistance groups that consolidated under ÚVOD were the "Political Centre" (POLITICKÉ ÚSTŘEDÍ, abbr. PÚ), the "Committee of the Petition 'We Remain Faithful' " (PETIČNÍ VÝBOR "VĚRNI ZŮSTANEME", abbr. PVVZ), and the Nation's Defence (OBRANA NÁRODA, abbr. ON). These groups represented the democratically and pro-west oriented part of inhabitants. Most of their members were former officers of by the German occupants disbanded Czechoslovak Army. They opposed the fourth official resistance group organized by the Communist Party of Czechoslovakia (KSČ) from Moscow. ŠP

[55]JINDRA was a cover name of a resistance group, which was part of the Sokol network called "The Sokol community in the resistance" (OBEC SOKOLSKÁ V ODBOJI, abbr. OSVO). They were mainly engaged in intelligence activities, but also in propaganda and sabotage ones. Its head was Ladislav Vaněk, code name Jindra. OSVO members were recruited from the forbidden Sokol. Sokol is a Czech gymnastic association rooted on ideas of nationalism. However [28]: Vaněk played undoubtedly a leading role in Sokol resistance organization JINDRA. He admonished London to organize the assassination of Heydrich, but when his objections were not accepted, he got involved in its preparation and due of his extraordinary intelligence he participated in it. He also knew about the paratroopers' hiding in the church crypt and even visited them there. However there is no evidence up to now, that he has betrayed or collaborated with the Gestapo at that time. But it is already proven that after his arrest in September 1942 he denounced many people. He was nevertheless sentenced to death but never executed because the Gestapo used him as a secret witness in other trials. For instance, it placed him in cells with other prisoners to acquire information from them. ŠP

  - Stockholm – Vladimír Vaněk (Waldemar van Eck) till March 1942,
  - Istanbul – col. Kumpošt and since January 1942 lieut. col. J. Hájíček,
  - Moscow – gen. Píka since April 22, 1941;

c) Parachute airdrops (Table 1).

d) Radio transmitters in the preparation and during the combats in the Slovak National Uprising:
  - Slovak National Council (Slovak: SLOVENSKÁ NÁRODNÁ RADA, abbr. SNR) had the radio transmitter named OTO,
  - Military Centre of SNR (Slovak: VOJENSKÉ ÚSTREDIE SNR) communicated using radio transmitter LEO,
  - Intelligence officer of MND in Slovakia captain Krátky had radio transmitters IVO and VÍT,
  - Parachute airdrop MANGANESE dropped on 10 June 1944 at Veľké Uherce had at disposal radio transmitter MARIENKA.

This statistics shows that the STP cipher system was used in 35–40 variants of the in-exile MND in London. Such a mass application of a cryptographic system should also have a corresponding quality!

5.2. Modifications of the STP cipher system implemented by the authorities of cryptologic section of the in-exile MND in London

Besides the weaknesses of the STP cipher system inherited in its design, a more serious culpability presented the inconceivable dismemberment of its integrity as it was implemented by the cipher section of in-exile MND in London. Instead of changing the cipher key by transmuting the passphrase sources (books, poems, song, etc.) while preserving the compactness of the STP system as such, the original STP system was fractionalized into three cryptographic systems which were used separately

- The first used system consisted only of a simple substitution. With such system there were provided the wireless-operators of parachute airdrops. The other parts of the cipher systems were unknown to them. They used it to encrypt traffic short reports intended for the GS in London. This cipher was used to encrypt the time schedules of future transmissions supplemented by a warning system. Wireless operator was the only member of the airdrop who could use it. The data concerning transmissions were in addition super-encrypted using prearranged parts of the ciphertext. Funkabwehr therefore had big problems with radio playback game.[56]
- The second cipher system was composed from a simple substitution and a simple transposition, i.e., from the first two cipher operations of the

[56]This cipher was called "small cipher key" (in Czech "malý šifrklíč") in jargon used in cipher group in London. ŠP

TABLE 1. The table was compiled using the book J. KOUTEK, *Tichá fronta*, Naše vojsko, Prague 1985.

Name	Commander	Dropping day	Note
PERCENTAGE	Fr. Pavelka	4.10.1941	trnsmttr. and cipher at Gestapo
SILVER A	A. Bartoš	29.12.1941	trnsmttr. LIBUŠA
OUT DISTANCE	A. Opálka	28.3.1942	trnsmttr. and cipher at Gestapo
ZINC	O. Pechal	28.3.1942	trnsmttr. and cipher at Gestapo
BIOSKOP	Fr. Pospíšil	28.4.1942	?
BIOUVAC	B. Kouba	28.4.1942	?
STEEL	O. Dvořák	28.4.1942	trnsmttr. and cipher at Gestapo
INTRANSITIVE	V. Kindl	30.4.1942	radio playback game HERMELÍN-DUPLEX
ANTIMONY	Fr. Závorka	21.10.1942	radio playback game HERMELÍN-SRAZIL
BARIUM	J. Šandera	4.4.1944	trnsmttr. MARTA
SULPHUR	A. Horák	9.4.1944	radio playback game WALLENSTEIN
CHALK	B. Bednařík	9.4.1944	radio playback game SENI
GLUCINIUM	?	9.4.1944	?
POTASH	J. Brandejs	5.5.1944	radio playback game MOLDAU
CLAY	A. Bartoš	13.4.1944	trnsmttr. EVA – intelligence radio playback game till 9 March
CARBON	Fr. Bogotaj	13.4.1944	lost trnsmttr.
SPELTER	?	5.5.1944	trnsmttr. LENKA
EMBASSY	?	22.12.1944	trnsmttr. KAREL
CALCIUM	J. Odstrčil	4.4.1944	trnsmttr. ZDENA and MILADA
WOLFRAM	J. Otiska	13.9.1944	trnsmttr. OLGA in hands of Gestapo
TUNGSTEN	R. Pernický	22.12.1944	?
PLATINIUM-PEWTER	J. Nechanský	17.2.1945	trnsmttr. ANNA in hands of Gestapo; new trnsmttr.'s HELENA and BETY
BAUKIT	P. Hromek	23.3.1945	trnsmttr. JARKA

original STP system. It was designated for the cipherer of the airdrop. He used it to encrypt his own intelligence reports, both his own ones or of the entire airdrop. The preserved instructions of the in-exile MND in London state that the cipherer was not allowed to know other parts of the cipher system.

- Third cipher system was actually the complete original STP system. It consisted of all three cipher transformations forming the original STP cipher. It was used by the airdrop commander. If necessary, he could use the super-encryption password to add it to the ciphers processed by the cipherer using the first two keys. Any other members of the parachute group was not allowed to know the super-encryption password. This system was also tailored to the encryption training of the airdrop. At the same time it was emphasized that the encryption system must be kept secret from the paragliding assistants.

Introduction of so many cipher systems required a special numbering of the telegrams to make it clear who sent them. To do this the heads of the telegrams were divided into three groups: the first one numbered in the range 000–699 was used for so-called "standard" radiograms, the range 700–899 for "secret" ones, and range 900–999 was used for the so-called "relational" ones. Radiograms with a head from the first group were sent by the cipherer who used the second cipher system. That from the second range were sent by the commander who used the third cipher system. Finally the last group was used for radiograms sent by wireless-operators using the first cipher system. These rules were generally used for the parachute airdrops, but there were exceptions always adapted by the cipher. Within these groups, even closer specifications were used. Numeration was selected arbitrarily, consecutive numeration was used for radiograms composed from several parts.[57]

The German interception monitoring stations against Czechoslovak resistance made every month summaries of the deciphered radiograms encrypted by the 1st and 2nd cipher system. They were delivered to the corresponding administration centers by couriers. Reports about Czech radiograms were delivered to Abwehrstelle in Prague and to K. H. Frank. Until the Abwehr was absorbed by SD in 1944, the solved radiograms encrypted by the 3rd cipher system were only known to Funkabwehr Headquarter and the Abwehr Headquarter at the OKH in Berlin. The fragmentation of the STP cipher system into three systems and their use for "standard" and "secret" radiograms presents a flagrant violation of elementary rules for secure usage of cipher systems.

C i g á ň gives a number of examples which confirm his conclusions about the fragmentation of the STP ciphers and the fact that the partial subsystems were

[57]See also [30, p. 162]. For the numeration of radiograms sent from external intelligence branch offices consult [15, p. 132–133].

solved by Germans. We refer the interested reader to original manuscript [8] for more details in this direction.

5.3. A method for a complete solution of the STP cipher

In the stationary radio-intercept stations of Funkabwehr in Münster the following two messages were intercepted:

788-37-17

23909	79826	33350	35132	33414	14187	10579	88053	64369	02912
11789	47442	50527	48135	67508	73660	95103	92146	15805	33859
70515	07295	97293	35593	74280	25894	88135	87089	98001	97138
09398	88106	30071	66069	83215	24040	03295			

789-58-17

23689	49916	15306	18183	87785	04353	50586	92233	65891	53627
97977	97324	64455	28111	90408	83976	08183	10501	61899	72963
43511	42269	43992	77001	07501	27594	70328	71135	49863	06650
86358	87505	42140	25595	89314	85541	15245	157117	37808	41522
18137	99988	36455	64600	25699	79794	96140	46091	98630	93387
49316	20471	06073	87236	64504	91705	51857	74653		

C i g á ň gives the following characteristics of the network traffic:[58]

- There were 2 stations in the network. Call signs: ING the control one, DON the subordinate one. The system of call changes is irregular.
- The networks worked on a wave of 6500 kc. Long session. The stations do not understand each other when they switch to auxiliary frequencies.
- Goniometric check as of June 12: Master – unchanged – London, subordinate – new position – South of PARDUBICE.
- Operator on master station: A well-known manuscript of a permanent radio operator. subordinate: new radio operator, transmission of digits 100/min., letters 60/min.
- Ciphers recognition – unknown to us.

5.3.1. A method how to break the super-encryption key

Based on the network characteristics and own experience with Czech cryptographic systems, the decipherer assumes that used complex cipher is based on 2 or 3 basic ciphers. This is also suggested by the following symbol frequency of the ciphertext:

0	1	2	3	4	5	6	7	8	9	
24	19	15	24	13	21	11	15	21	22	= 185

[58]It is not clear from the text whether this is a real protocol from the radio-intercept station. Some technical details about the used frequencies can be found in [30, p. 47–49]. ŠP

Since solely the numbers from 0 till 9 cannot encode a complete alphabet, a digraph substitution cipher must be used in the substitution step. In this case the frequencies of some digits have to appear more frequently than the other ones. As we see this is not the case in our example. However, the digits appear with a small variance around the mean. Consequently, the substitution was overwritten by an super-encryption.

The super-encryption must be the last operation of the encryption. Let's try first to determine the length of its encryption passphrase. Divide the ciphertext into lines of length of 15, 17, 19, 21, 23, and 25 digits and calculate the frequencies of digits in the resulting columns. We can exclude the even length passphrases because they greatly simplify the solution thereby decreasing the safety of the used cipher.[59]
Passphrase length 15:

1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
2	3	9	0	9	7	9	8	2	6	3	3	3	5	0
3	5	1	3	2	3	3	4	1	4	1	4	1	8	7
1	0	5	7	9	8	8	0	5	3	6	4	3	6	9
0	2	9	1	2	1	1	7	8	9	4	7	4	4	2
5	0	5	2	7	4	8	1	3	5	6	7	5	0	8
7	3	6	6	0	9	5	1	0	3	9	2	1	4	6
1	5	8	0	5	3	3	8	5	9	7	0	5	1	5
0	7	2	9	5	9	7	2	9	3	3	5	5	9	3
7	4	2	8	0	2	5	8	9	4	8	8	1	3	5
8	7	0	8	9	9	8	0	0	1	9	7	1	3	8
0	9	3	9	8	8	8	1	0	6	3	0	0	7	1
6	6	0	6	9	8	3	2	1	5	2	4	0	4	0
0	3	2	9	5										

Frequencies of digits in columns 1 till 15:

	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
0	4	2	2	2	2	–	–	2	3	–	–	2	2	1	2
1	2	–	1	1	–	1	1	3	2	1	1	–	4	1	1
2	1	1	3	1	2	1	–	2	1	–	1	1	–	–	1
3	1	3	1	1	–	2	3	–	1	3	3	1	2	2	1
4	-	1	–	–	–	1	–	1	–	2	1	3	1	3	–
5	1	2	2	–	3	–	2	–	2	2	–	1	3	1	2
6	1	1	1	2	–	–	–	–	–	2	2	–	–	1	1
7	2	2	–	1	1	1	1	1	–	–	1	3	–	1	1
8	1	–	1	2	1	3	4	3	1	–	1	1	–	1	2
9	–	1	2	3	4	3	1	–	2	2	2	–	–	1	1

[59]Notice that in case of an even digits keys we have the same number of tens (on the odd places) and units digits (on even places) in every row of the transposition table.

Passphrase length 17:

1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17
0	3	9	0	9	7	9	8	2	6	3	3	3	5	0	3	5
1	3	2	3	3	4	1	4	1	4	1	8	7	1	0	5	7
9	8	8	0	5	3	6	4	3	6	9	0	2	9	1	2	1
1	7	8	9	4	7	4	4	2	5	0	5	2	7	4	8	1
3	5	6	7	5	0	8	7	3	6	6	0	9	5	1	0	3
9	2	1	4	6	1	5	8	0	5	3	3	8	5	9	7	0
5	1	5	0	7	2	9	5	9	7	2	9	3	3	5	5	9
3	7	4	2	8	0	2	5	8	9	4	8	8	1	3	5	8
7	0	8	9	9	8	0	0	1	9	7	1	3	8	0	9	3
9	8	8	8	1	0	6	3	0	0	7	1	6	6	0	6	9
8	3	2	1	5	2	4	0	4	0	0	3	2	9	5		

Frequencies of digits in columns 1 till 17:

	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17
0	–	1	–	3	–	3	1	2	2	2	2	2	–	–	4	1	1
1	2	1	1	1	1	1	1	–	2	–	1	2	–	2	2	–	2
2	1	1	2	1	–	2	1	–	2	–	1	–	3	–	–	1	–
3	2	3	–	1	1	1	–	1	2	–	2	3	3	1	1	1	2
4	–	–	1	1	1	1	2	3	1	1	1	–	–	–	1	–	–
5	1	1	1	–	3	–	1	2	–	2	–	1	–	3	2	3	1
6	–	–	1	–	1	–	2	–	–	3	1	–	1	1	–	1	–
7	1	2	–	1	1	2	–	1	–	1	2	–	1	1	–	1	1
8	1	2	4	1	1	1	1	2	1	–	–	2	2	1	–	1	1
9	3	–	1	2	2	–	2	–	1	2	1	1	1	2	1	1	2

Passphrase length 19:

1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19
2	3	9	0	9	7	9	8	2	6	3	3	3	5	0	3	5	1	3
2	3	3	4	1	4	1	4	1	8	7	1	0	5	7	9	8	8	0
5	3	6	4	3	6	9	0	2	9	1	2	1	1	7	8	9	4	7
4	4	2	5	0	5	2	7	4	8	1	3	5	6	7	5	0	8	7
3	6	6	0	9	5	1	0	3	9	2	1	4	6	1	5	8	0	5
3	3	8	5	9	7	0	5	1	5	0	7	2	9	5	9	7	2	9
3	3	5	5	9	3	7	4	2	8	0	2	5	8	9	4	8	8	1
3	5	8	7	0	8	9	9	8	0	0	1	9	7	1	3	8	0	9
3	9	8	8	8	1	0	6	3	0	0	7	1	6	6	0	6	9	8
3	2	1	5	2	4	0	4	0	0	3	2	9	5					

Frequencies of digits in columns 1 till 19:

	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19
0	–	–	–	2	2	–	3	2	1	3	4	–	1	–	1	1	1	2	1
1	–	–	1	–	1	1	2	–	2	–	2	3	2	1	2	–	–	1	1
2	2	1	1	–	1	–	1	–	3	–	1	3	1	–	–	–	–	1	–
3	6	5	1	–	1	1	–	–	2	–	2	2	1	–	–	2	–	–	1
4	1	1	–	2	–	2	–	3	1	–	–	–	1	–	–	1	–	1	–
5	1	1	1	4	–	2	–	1	–	1	–	–	2	3	1	2	1	–	1
6	–	1	2	–	–	1	–	1	–	1	–	–	–	3	1	–	1	–	–
7	–	–	–	1	–	2	1	1	–	–	1	2	–	1	3	–	1	–	2
8	–	–	3	1	1	1	–	1	1	3	–	–	–	1	–	1	4	3	1
9	–	1	1	–	4	–	3	1	–	2	–	–	2	1	1	2	1	1	2

Passphrase length 21:

1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21
2	3	9	0	9	7	9	8	2	6	3	3	3	5	0	3	5	1	3	2	3
3	4	1	4	1	4	1	8	7	1	0	5	7	9	8	8	0	5	3	6	4
3	6	9	0	2	9	1	2	1	1	7	8	9	4	7	4	4	2	5	0	5
2	7	4	8	1	3	5	6	7	5	0	8	7	3	6	6	0	9	5	1	0
3	9	2	1	4	6	1	5	8	0	5	3	3	8	5	9	7	0	5	1	5
0	7	2	9	5	9	7	2	9	3	3	5	5	9	3	7	4	2	8	0	2
5	8	9	4	8	8	1	3	5	8	7	0	8	9	9	8	0	0	1	9	7
1	3	8	0	9	3	9	8	8	8	1	0	6	3	0	0	7	1	6	6	0
6	9	8	3	2	1	5	2	4	0	4	0	0	3	2	9	5				

Frequencies of digits in columns 1 till 21:

	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21
0	1	–	–	3	–	–	–	–	–	2	2	3	1	–	2	1	3	2	–	2	2
1	1	–	1	1	2	1	4	–	1	2	1	–	–	–	–	–	–	2	1	2	–
2	2	–	2	–	2	–	–	3	1	–	–	–	–	–	1	–	–	2	–	1	1
3	3	2	–	1	–	2	–	1	–	1	2	2	2	3	1	1	–	–	2	–	1
4	–	1	1	2	1	1	–	–	1	–	1	–	–	1	–	1	2	–	–	–	1
5	1	–	–	–	1	–	2	1	1	1	1	2	1	1	1	–	2	1	3	–	2
6	1	1	–	–	–	1	–	1	–	1	–	–	1	–	1	1	–	–	1	2	–
7	–	2	–	–	–	1	1	–	2	–	2	–	2	–	1	1	2	–	–	–	1
8	–	1	2	1	1	1	–	3	2	2	–	2	1	1	1	2	–	–	1	–	–
9	–	2	3	1	2	2	2	–	1	–	–	–	1	3	1	2	–	1	–	1	–

Passphrase length 23:

1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23
2	3	9	0	9	7	9	8	2	6	3	3	3	5	0	3	5	1	3	2	3	3	4
1	4	1	4	1	8	7	1	0	5	7	9	8	8	0	5	3	6	4	3	6	9	0
2	9	1	2	1	1	7	8	9	4	7	4	4	2	5	0	5	3	7	4	8	1	3
5	6	7	5	0	8	7	3	6	6	0	9	5	1	0	3	9	2	1	4	6	1	5
8	0	5	3	3	8	5	9	7	0	5	1	5	0	7	2	9	5	9	7	2	9	3
3	5	5	9	3	7	4	2	8	0	2	5	8	9	4	8	8	1	3	5	8	7	0
8	9	9	8	0	0	1	9	7	1	3	8	0	9	3	9	8	8	8	1	0	6	3
0	0	7	1	6	6	0	6	9	8	3	2	1	5	2	4	0	4	0	0	3	2	9
5																						

Frequencies of digits in columns 1 till 23:

	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23
0	1	2	–	1	2	1	1	–	1	2	1	–	1	1	3	1	1	–	1	1	1	–	2
1	1	–	2	1	2	1	1	1	–	1	–	1	1	1	–	–	–	2	1	1	–	2	–
2	2	–	-	1	–	–	–	1	1	–	1	1	–	1	1	1	–	2	–	1	1	1	–
3	1	1	–	1	2	–	–	1	–	–	3	1	1	–	1	2	1	–	2	1	2	1	3
4	–	1	–	1	–	–	1	–	–	1	–	1	1	–	1	1	–	1	1	2	–	–	1
5	2	1	2	1	–	–	1	–	–	1	1	1	2	2	1	1	2	1	–	1	–	–	1
6	–	1	–	–	1	1	–	1	1	2	–	–	–	–	–	–	–	1	–	–	2	1	–
7	–	–	2	–	–	2	3	–	2	–	2	–	–	–	1	–	–	–	1	1	–	1	–
8	2	–	–	1	–	3	–	2	1	1	–	1	2	1	–	1	2	1	1	–	2	–	–
9	–	2	2	1	1	–	1	2	2	–	–	2	–	2	–	1	2	–	1	–	–	2	1

Passphrase length 25:

1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25
2	3	9	0	9	7	9	8	2	6	3	3	3	5	0	3	5	1	3	2	3	3	4	1	4
1	4	1	8	7	1	0	5	7	9	8	8	0	5	3	6	4	3	6	9	0	2	9	1	2
1	1	7	8	9	4	7	4	4	2	5	0	5	2	7	4	8	1	3	5	6	7	5	0	8
7	3	6	6	0	9	5	1	0	3	9	2	1	4	6	1	5	8	0	5	3	3	8	5	9
7	0	5	1	5	0	7	2	9	5	9	7	2	9	3	3	5	5	9	3	7	4	2	8	0
2	5	8	9	4	8	8	1	3	5	8	7	0	8	9	9	8	0	0	1	9	7	1	3	8
0	9	3	9	8	8	8	1	0	6	3	0	0	7	1	6	6	0	6	9	8	3	2	1	5
2	4	0	4	0	0	3	2	9	5															

Frequencies of digits in columns 1 till 25:

	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25
0	1	1	1	1	2	2	1	–	2	–	–	2	3	–	1	–	–	2	2	–	1	–	–	1	1
1	2	1	1	1	–	1	–	3	–	–	–	–	1	–	1	1	–	2	–	1	–	–	1	3	–
2	3	–	–	–	–	–	–	2	1	1	–	1	1	1	-	–	–	–	–	1	–	1	2	–	1
3	–	2	1	–	–	–	1	–	1	1	2	1	1	–	2	2	–	1	2	1	2	3	–	1	–
4	–	2	–	1	1	1	–	1	1	–	–	–	–	1	–	1	1	–	–	–	–	1	1	–	1
5	–	1	1	–	1	–	1	1	–	3	1	–	1	2	–	–	3	1	–	2	–	–	1	1	1
6	–	–	1	1	–	–	–	–	–	2	–	–	–	–	1	2	1	–	2	–	1	–	–	–	–
7	2	–	1	–	1	1	2	–	1	–	–	2	–	1	1	–	–	–	–	–	1	2	–	–	–
8	–	–	1	2	1	2	2	1	–	–	2	2	–	1	–	–	2	1	–	–	1	–	1	1	2
9	–	1	1	2	2	1	1	–	2	1	2	–	–	1	1	1	–	–	1	2	1	–	1	–	1

A brief look at the frequency tables of each password length indicates that some regularity appears for length 19 in comparison with the others. Check this observation in radiogram 789 using the same approach. We obtain for length 19 a similar result

1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19
2	3	6	9	8	4	9	9	1	6	1	5	3	0	6	1	8	1	8
3	8	7	7	8	5	0	4	3	5	3	5	0	5	8	6	9	2	2
3	3	6	5	8	9	1	5	3	6	2	7	9	7	9	7	7	9	7
3	2	4	6	4	4	5	5	2	8	1	1	1	9	0	4	0	8	8
3	9	7	6	0	8	1	8	3	1	0	5	0	1	6	1	8	9	9
7	2	9	6	3	4	3	5	1	1	4	2	2	6	9	4	3	9	9
2	7	7	9	7	5	0	7	5	0	1	2	7	5	9	4	7	0	3
2	8	7	1	1	3	5	4	9	8	6	3	0	6	6	5	0	8	8
3	5	8	8	7	5	0	5	4	2	1	4	0	2	5	5	9	5	8
9	3	1	4	8	5	0	4	1	1	5	2	4	5	1	5	7	1	1
3	7	8	0	8	4	1	5	2	2	1	8	1	3	7	9	9	9	8
8	3	6	4	5	5	6	4	6	0	0	2	5	6	9	9	7	9	7
9	4	9	6	1	4	0	4	6	0	9	1	9	8	6	3	0	9	3
3	8	7	4	9	3	1	6	2	0	4	7	1	0	6	0	7	3	8
7	2	3	6	6	4	5	0	4	9	1	7	0	5	5	1	8	5	7
7	4	6	5	3														

Frequencies of digits in columns 1 till 25 in the second radiogram:

	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19
0	–	–	–	2	1	–	4	1	–	4	4	–	5	2	1	1	3	1	–
1	–	–	1	1	2	–	4	–	3	3	4	2	3	1	1	3	–	2	1
2	3	3	–	–	–	–	–	–	3	2	1	4	1	1	–	1	–	2	1
3	7	4	1	–	2	2	1	–	3	–	1	1	1	1	–	–	1	–	2
4	–	2	1	3	1	6	–	5	2	–	2	1	1	–	–	3	–	–	–
5	–	1	–	2	1	5	4	5	1	1	1	3	1	4	2	3	–	2	–
6	–	–	4	5	1	–	1	1	2	2	1	–	–	3	5	1	–	–	–
7	3	2	5	1	2	–	–	1	–	–	–	3	1	1	1	1	5	–	3
8	1	3	2	1	5	1	–	1	–	2	–	1	–	1	1	–	3	2	6
9	2	1	2	1	1	1	1	1	1	1	1	–	2	1	4	2	3	6	2

We can observe a similar regularity as it was the case in the previous radiogram. The differences in the frequency of the digits in columns are more pronounced with the increasing number of columns.

Merge the frequencies of both radiograms to obtain

	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19
0	–	–	–	4	3	1	7	3	1	7	8	–	6	2	2	2	4	3	1
1	–	–	2	1	3	1	6	–	5	3	6	5	5	2	3	3	–	3	2
2	6	4	1	–	1	–	1	–	6	2	2	7	2	1	–	1	–	3	1
3	12	9	2	–	3	2	1	–	5	–	3	3	2	1	–	2	2	–	3
4	1	3	1	5	1	8	–	8	3	–	2	1	2	–	–	4	–	1	–
5	1	2	1	6	1	7	4	6	1	2	1	3	3	7	3	5	1	2	1
6	–	1	6	5	1	1	1	2	2	3	1	–	–	6	6	1	1	–	–
7	3	2	5	2	2	2	1	2	–	–	1	5	1	2	4	1	6	–	5
8	1	3	5	2	6	2	–	2	1	5	–	1	–	2	–	–	6	5	7
9	2	2	3	1	4	1	4	2	1	3	1	–	4	2	5	4	4	7	4

Draw out the most frequent digits of the columns from the merged frequency table:

1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19
2	2	6	4	8	4	9	4	1	8	0	1	9	5	5	4	7	8	7
3	3	7	5	9	4	0	5	2	9	1	2	0	6	6	5	8	9	8
	4	8	6	0		1		3	0	2	3	1		7		9	0	9
		9						4	1	3				8		0	1	
														9			2	

The first line of digits taken from each column should represent the number form of the passphrase.

We can check whether this is really true. According to the rules of the letter-to-digit transformation of passwords, the password should contain one zero and the other 9 digits should be used twice (remember we work with a 19-digit password).

Passphrase digit	Stands in column
0	11
1	9, 12
2	1, 2
3	–
4	4, 6, 8, 16
5	14, 15
6	3
7	17, 19
8	5, 10, 18
9	7, 13

A look on the table shows that the digits 0, 1, 2, 5 and 9 satisfy the above rule. However, digit 3 does not occur at all, while digit 4 appears 4 times. We have to select two of them for the passphrase digit 3. A closer look on the frequency table for columns indicates that for 4 we have to take the columns 4 and 8 because there are empty spaces before them, as in other columns. Then for 3 columns 6 and 16 could be used. These columns there also precedes an empty space or a low-frequency digit cipher.

There remains to solve the position of digits 6, 7 and 8. Put 8 in columns 10 and 18, for there stands free places before them. Then column 5 begins with digit 7, and finally from the three columns with digit 7 we put 6 in column 17.

This yields the following digital form of the super-encryption passphrase

1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	– column
2	2	6	4	7	3	9	4	1	8	0	1	9	5	5	3	6	8	7	– passphrase

Thus we have completed the last, most important step of the London MND encryption system. Note that this procedure for its solution has not been published by anyone yet, as C i g á ň writes. The presented solution of the MND cipher was used only at Funkabwehr in Berlin, and it was top-secret. The encrypted radiograms were passed only to supreme commanders of Wehrmacht. The Prague SD and Gestapo did know nothing about the algorithms used.

The next encryption steps we present here only for the sake of completeness. The presented procedures are published in various sources devoted to solution of ciphers. Note that everything that is mentioned below was known to the lowest levels of Funkabwehr in Prague and perhaps even to the Gestapo in Prague.

5.3.2. A method how to break the transposition passphrase

a) Subtract without carry the decrypted super-encryption passphrase from the radiogram No. 788. Thus $1 - 9 = 2$, etc.

b) Enumerate the obtained columns of digits by numbers 1 till 185.

c) In the next line put a cross "×" under each digit 4, 5, 6, 7, 8, and 9.

d) In the next line write a bullet "•" between the already existing crosses "×", and alternate the signs "•" and "×" in the whole text. Spots where an irregularity of alternation appear mark by a color.

e) Count the frequencies of all digits.

f) We obtain the following scheme:

1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28
0	1	3	6	2	4	0	4	1	8	3	2	4	0	5	0	9	3	6	0	1	7	0	4	1	2	0	0
			×		×		×		×		•	×		×		×		×	•		×		×				
•	×	•		•		•		•					•		•		•					•		•	×	•	×

29	30	31	32	33	34	35	36	37	38	39	40	41	42	43	44	45	46	47	48	49	50	51	52	53	54
0	7	0	1	0	2	6	2	0	3	3	1	0	0	6	3	0	6	1	1	1	1	2	6	2	5
	×	•			•	×								×		•	×						×		×
•							•	×	•	×	•	×	•					•	×	•	×	•		•	

55	56	57	58	59	60	61	62	63	64	65	66	67	68	69	70	71	72	73	74	75	76	77	78	79	80
3	6	0	2	2	6	1	3	2	3	3	3	0	1	2	6	1	2	2	4	0	0	1	4	0	6
	×				×										×				×				×		×
•		•	×	•		•	×	•	×	•	×	•	×	•		•	×	•		•	×	•		•	

81	82	83	84	85	86	87	88	89	90	91	92	93	94	95	96	97	98	99	100	01	02	03	04	05
2	2	2	6	2	1	2	0	5	1	6	2	2	2	8	1	1	2	1	2	4	1	1	0	7
			×	•	×			×		×				×						×				×
•	×	•							•		•	×	•		•	×	•	×	•		•	×	•	

06	07	08	09	110	11	12	13	14	15	16	17	18	19	120	121	22	23	24	25	26	27	28	29
0	6	3	9	0	6	1	4	2	1	1	9	1	2	0	8	0	1	0	0	1	6	3	4
	×		×		×		×				×				×						×		×
•		•		•		•		•	×	•		•	×	•		•	×	•	×	•		•	

130	31	32	33	34	35	36	37	38	39	140	41	42	43	44	45	46	47	48	49	150	151	52	53
1	2	0	4	1	3	2	3	3	5	0	5	7	2	0	0	0	2	6	0	7	2	2	1
			×						×		×	×						×		×			
•	×	•		•	×	•	×	•		•			•	×	•	×	•		•		•	×	•

54	55	56	57	58	59	160	61	62	63	64	65	66	67	68	69	170	71	72	73	74	75	76	77	78
7	2	4	1	8	1	2	2	2	0	6	2	1	1	7	0	1	1	1	0	5	1	5	1	1
×		×		×						×				×						×		×		
	•		•		•	×	•	×	•		•	×	•		•	×	•	×	•		•		•	×

79	180	181	182	183	184	185
0		2	3	1	0	0
	×					
•		•	×	•	×	•

The frequencies:

0	1	2	3	4	5	6	7	8	9	digits frequencies
40	42	36	17	12	7	17	7	4	3	$= 185$
				×	×	×	×	×	×	$= 50$

g) Remember that we are working with a text after a transposition that has been created in such a way that we sequentially chose the columns with digits of the password numbers 1, 2, 3, ..., ? from the substitution table. Here the length of the transposition passphrase 15, 17, 19, 21, 23 or 25 is understood under the sign ?

Since we have 185 signs in the cipher, we get the following patterns of the substitution text for each length of the transposition passphrase:

Passphrase length	Calculation	Number of columns and signs	
		short columns	long columns
15	$185 : 15 = 12$ 35 5	10 at 12	5 at 13
17	$185 : 17 = 10$ 14	5 at 9	14 at 10
19	$185 : 19 = 9$ 17	5 at 9	17 at 10
21	$185 : 21 = 8$ 17	4 at 8	17 at 9
23	$185 : 23 = 8$ 1	22 at 8	1 at 9
25	$185 : 25 = 7$ 10	15 at 7	10 at 8

h) In the first row of the substitution text table we have ten digits on odd positions and on even places the unit digits of the digraph substitution numbers. In total $H/2 + 1$ tens and $H/2$ unit digits. However, in the second row, the ratio is reversed — $H/2 + 1$ unit and $H/2$ ten digits.

As a result an irregularity appears where alternate the ten and unit digits in the columns. We use this to simplify the text using • and × signs in place of digits.

The regular alternation is interrupted when after the last sign of a column there follows a column with the same sign at the beginning. In our case, we can use this rule only for digits that are unambiguous.

i) Since the ciphertext has 185 signs where digraph substitution was used, the last row of the substitution figure was completed by one arbitrary number, to get a total number of cipher signs divisible by five (radiograms were broadcasted in pentagraph groups).

j) There must be 92 ten and 92 unit digits among the 184 digits of the cipher text. However, we have uniquely identified only 50 unit digits, while the reminding 134 digits represent both the ten and unit digits.

k) Since there is an interruption of the alternation at the 141st and 142nd sign, the ciphertext breaks into two segments having 141 and 44 signs. This corresponds to a passphrase of length 17 (11 columns each with 11 signs and a 2 columns each with 10 ones = 141 and 4 columns each with 11 signs = 44).

Having the length of the passphrase we can substitute for digit number 12 a bullet, as we can do also for digit number 20.

In the third colored group of slots the digits number 31 and 34 must be bullets. In the fourth one the digit no. 45 must be again a bullet. In the sixth one slot 85 is again a bullet and slot 86 is a cross.

l) Thus from 185 cipher signs we determined already 178 ones in this way:

Text row	Determined as		Not determined
	"•"	"×"	
1	14	14	2 signs: 11 a 21
2	14	13	3 signs: 32–32 a 44
3	14	14	2 signs: 87 a 88
4	15	15	
5	14	16	
6	15	15	
7	3	2	
In total 185 cipher sings	89	89	7
To be detrmined	3	$3-1$	

Now we can easily substitute for 11 a bullet, for 32 a cross, for 33 a bullet, for 44 a cross, for 87 a cross and for 88 a bullet. Since the 2nd column

12–21 cannot be a short one (in opposite case the 3rd one would have 12 signs, what is impossible having passphrase length 17), we conclude that the arising duplication "××" appears on the end of a long columns and thus it contains the number added to complete the last group to a pentagraph. It remains to determine the 2nd short column in segment 44–86. Its signs must be reversed to those of the 4th column (signs 34–43). This is possible only for slots 44–52 or 66–75. Let us take the second possibility, because it is not very probable that both two short columns follow each other (passphrase 4 and 5).

m) We obtained the following result:

1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	transposition passphrase
0	2	0	2	3	3	3	0	2	2	4	0	2	7	1	6	1	
1	4	4	6	0	6	0	1	0	1	0	8	0	2	7	2	5	
3	0	1	2	6	0	1	4	5	2	6	0	4	0	2	1	1	
6	5	2	0	1	2	2	0	1	4	1	1	1	0	4	1	1	
2	0	0	3	1	2	6	6	6	1	4	0	3	0	1	7	0	colored slots =
4	9	0	3	1	6	1	2	2	1	2	0	2	2	8	0	9	unit digit
0	3	0	1	1	1	2	2	2	0	1	1	3	6	1	1	2	
4	6	7	0	2	3	2	2	2	7	1	6	3	0	2	1	3	
1	0	0	0	6	2	4	6	8	0	9	3	5	7	2	1	1	
8	1	1	6	2	3	0	2	1	6	1	4	0	2	2	0	0	
3	7	0		5	3		1	1	3	2	1	5	2	0	5	0	

n) Columns 2, 7 and 4 are unambiguously on the end of the table. It remains to put together 7 suitable couples of columns and order them into a table. Suppose that we succeeded to do this and that we obtained the following transposition key:

3	5	15	8	12	16	10	13	6	11	17	9	1	14	2	7	4
0	3	1	0	0	6	2	2	3	4	1	2	0	7	2	3	2
4	0	7	1	8	2	1	0	6	0	5	0	1	2	4	0	6
1	6	2	4	0	1	2	4	0	6	1	5	3	0	0	1	2
2	1	4	0	1	1	4	1	2	1	1	1	6	0	5	2	0
0	1	1	6	0	7	1	3	2	4	0	6	2	0	0	6	3
0	1	8	2	0	0	1	2	6	2	9	2	4	2	9	1	3
0	1	1	2	1	1	0	3	1	1	2	2	0	6	3	2	1
7	2	2	2	6	1	7	3	3	1	3	2	4	0	6	2	0
0	6	2	6	3	1	0	5	2	9	1	8	1	7	0	4	0
1	2	2	2	4	0	6	0	3	1	0	1	8	2	1	0	6
0	5	0	1	1	5	3	5	3	2	0	1	3	2	7		

5.3.3. A method how to break the substitution key

a) Count the frequencies of the digit digraphs in the last table:

	0	1	2	3	4	5	6	7	8	9
0	–	10	–	3	1	4	11	3	–	–
1	2	3	3	3	2	2	3	3	4	–
2	4	2	5	1	8	–	3	–	–	3
3	2	1	3	1	1	1				

Rewrite the last table into the ciphertext grouping numerical digraphs representing the substitutions (cf. the table below). Then in the next step separate vowels and consonants represented by digraphs using the following considerations reflecting the basic rules of alternation of vowels and consonants in written words: frame the most frequent digraph 06 as a vowel and strike from the ciphertext the surrounding it digraphs (10, 22, 21, 05 etc. — they are candidates for consonants). In the 2nd row frame the digraph 11 and strike out its neighbors. In the 4th row frame the digraph 11 and 17 and in the next one the digraphs 17 and 29.

03	10	06	22	34	12	07	23	24	07	18	21	06	05	01	24	06
c	h	e	s	.	j	ě	š	t	ě	p	ř	e	d	a	t	e
16	24	01	24	06	15	30	01	22	14	01	14	12	11	16	15	20
n	t	a	t	e	m	z	a	s	l	a	l	j	i	n	d	r
01	16	07	13	24	06	20	06	30	18	20	01	26	29	24	29	13
a	n	ě	k	t	e	r	e	z	p	r	a	v	y	t	y	k
01	12	11	03	11	22	06	32	17	22	26	17	33	13	24	06	20
a	j	i	c	i	s	e	–	o	s	v	o	,	k	t	e	r
06	26	31	05	29	18	17	04	01	22	24	06	03	10	18	21	06
e	v	ž	d	y	p	o	č	a	s	t	e	c	h	p	ř	e
05	01	15	35	32	01	32										
d	á	m	:	–	a	–										

Try to substitute 06 = *e*, 01 = *a*, etc. We obtain the following substitution table:

	0	1	2	3	4	5	6	7	8	9
0		a	b	c	č	d	e	ě	f	g
1	h	i	j	k	l	m	n	o	p	q
2	r	ř	s	š	t	u	v	w	x	y
3	z	ž	–	,	.	:				

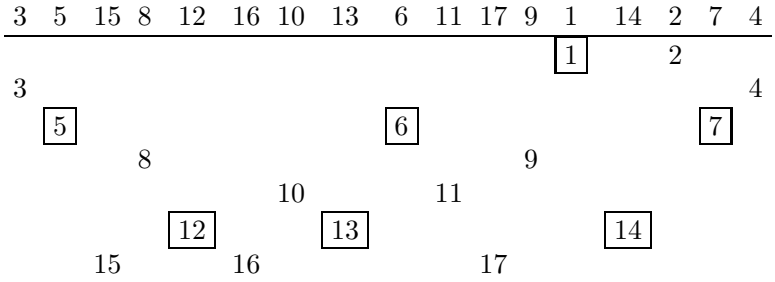
C i g á ň used here a plaintext of a real radiogram received by MND in London on June 6, 1942. The used transposition and super-encryption passphrases are taken from other sets of passphrases used at different occasions, although C i g á ň writes that they are his figment. The substitution table is a real one designed for the mentioned Vaněk = JINDRA.

5.3.4. Reconstruction of the used passphrases

We can also try to convert the obtained numeric form of the passphrase into verbal text. In the positive case it is possible even to reveal the used book. To do this it is usually necessary to decipher passphrases used during several days, however.

a) We will first recover the transposition passphrase. First we split it into segments determined by the breakpoints. Here under a breakpoint we understand a place where the letters of the passphrase change, these are the places where a greater number is located to the left of a smaller one.

At the same time we can frame successive numerical series, which could represent vowels. There should be from 6 till 8 of them among the total number of 17 letters.



If we start with 1 = a, 5, 6, 7 = e and 12, 13, 14 = o, 2 = b and 3, 4 = c or d, we obtain "ce" at the beginning and "sobe$\frac{\text{d}}{\text{c}}$" at the end. Numbers 8 and 9 must belong to the group of letters FGHIJK, 10 and 11 to the group LMW and 15, 16, 17 to the group PRST.

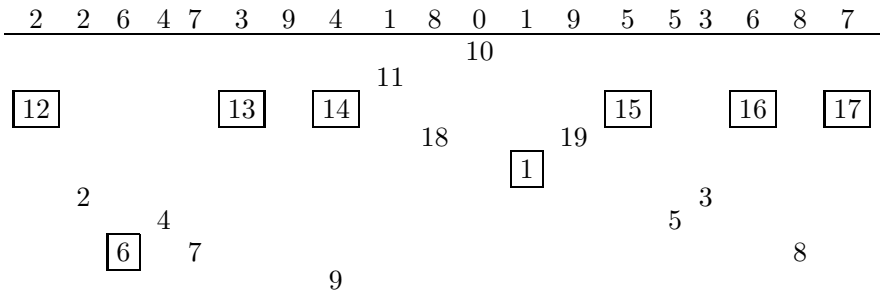
If we substitute 15 = s, then 8 = k, and there unfolds almost the whole passphrase "ceskoslo enskaobec", up to a one missing letter. This is "v" the 18th letter of the passphrase, a letter which can be completed immediately by anybody who understands Czech.[60]

b) To reveal the super-encryption passphrase we proceed similarly. We know that it originally consisted from the numbers 1–9 and 10–19 where in the last case the ten digits were omitted. We face a problem how to divide them into two groups accordingly.

[60] "československá obec" means in Czech "Czechoslovak community". ŠP

We start with 10, which is clearly identified. Number 1 to the left represents 11. In 3rd row we have a long series 12–17 and in 4th row numbers 18 and 19.

The remaining numbers 1 till 9 we place in the bottom part of table in accordance with breakpoint rules. Finally we divide the text into vowels and consonants (12–17, 1 and 6).



Let us try the substitutions: 1 = a, 2 = b, 3 = b, 4 = c, 5 = d, 6 = e, 12 − 17 = o, 19 = v, 9 = k, 10 = k, 11 = 1 and 18 = s. Checking the text we discover an error with the classification of 7 and 17. Change 17 on the 5th position to "s" and substitute for 7 the letter "i". We got the whole passphrase "obec sokolská v odboji".[61]

5.4. "Express" method for breaking the super-encryption passphrase

C i g á ň also presents some other ideas how to break ciphers based on STP cipher steps and used in the wireless communication between MND in London and home resistance or external branch offices.

Neither the first nor the second cipher step of the STP cipher guaranteed the security of the enciphered messages. This fact is mentioned as known to authorities of the cipher department of MND in London in [30]. What led them to fragmentize the whole STP cipher is not mentioned in the book.

The cryptanalysts of Funkabwehr easily solved the messages enciphered by the first cipher system – it was a simple substitution. After breaking it and the reconstruction of the enciphering tables of the first radiogram they immediately detected whether the cipher is used or not used in the next intercepted telegram. Though the radiograms of this class were not important, they contained information about the radio traffic, and so reading of the radiograms of this class simplified the work of the radio reconnaissance.

[61]The couple of passphrases "obec sokolská v odboji" and "jindra vaníček" was used by Vaněk=JINDRA [13, p. 82]. ŠP

The cryptanalysts of Funkabwehr also did not have problems with the second cipher system. They also knew how to convert numerical form of the passphrases to their verbal form. Simultaneously they found out that the same substitution is used as in the first cipher.

In Funkabwehr Headquarter in Berlin, where the solved but also unsolved radiograms were gathered, quickly detected that the components of cipher systems are in relation to each other. Therefore suppose that the step S and T are broken, and to unfold also the key of step P we can proceed using the following algorithm:

a) Write down the known (numerical form) transposition password on a grid paper. Take the radiogram to be solved and divide the number of its digits by the passphrase length to obtain the format of the cipher matrix and draw it under the password.

b) Fill successively the message digits in the cells in order indicated by the password numbers 1, 2, 3, etc.

c) Mark the digits on the unit places in the following way. In the first row there will be the digits on the places labeled by even "letter numbers", in the second one those with odd numbers, etc.

d) Then write the columns 1, 2, 3, etc. in rows of length 15 under each other. Check whether the span of non-marked digits in each column does not exceed the number of ten digits in the substitution table. If it is greater, do not continue and go over to the next length 17. Repeat the above procedure until we obtain coincidence between the span of the ten digits in the substitution table and the span of non-marked digits obtained columns. Then fill the rest of the message into the matrix, if its end is not reached.

e) Finally, write down the smallest digit from the used ten digits in each column. When you are lucky enough you obtain the super-encryption passphrase in numerical form. If not you got one of its 9 variants, and the STP cipher is broken completely.

5.5. Further solution methods for breaking the transposition and substitution keys

Above we reproduced a method how to break the transposition passphrase. It is C i g á ň' s original method. Its advantage it that we could work with a single intercepted radiogram. It was based on an idea which employed the role of unit digits of the substitution table. The step associated with the determination of short and long columns is also his invention. As he notes the cryptanalysts of Funkabwehr used a different method.

Their method derived benefit from the appearance of ten digits and not of unit digits as above. We know that among them there are also some unit digits. To separate both groups they used 2–3 messages of the same length. The solution

then uses the fact that they are based on an unchangeable (fixed) ordering of numbers a fact which enabled the solver to distinguish between ten and unit digits.[62] The remaining parts of a solution were then principally the same as mentioned above. If no messages of the same length were intercepted in one day, the method was not applicable. The occurrence of such groups of radiograms could also be a result of a forgery of the adversary intelligence service or planted agents (Thümmel Agent A-54?), however.

It was also possible to exploit more advantageous shapes of transposition tables. The simplest ones are the complete rectangular tables-grids with the columns of the same length. Another case are tables number with a small number of long columns, or contrariwise with a small number of short columns. In such case the so-called "hat method" is suitable, a method which is known to every beginner.[63]

REFERENCES

[1] *Svědecká výpověď plukovníka Jaroslava Hájíčka.* [Testimony of colonel Jaroslav Hájíček.] Archiv bezpečnostních složek 302_1_429_3. (In Czech)

[2] *Protokol výpovědě Dr. Aloise Hornischera.* [Deposition taken on oath with Dr. Alois Hornischer.] Archiv bezpečnostních složek 302_20_10. (In Czech)

[3] *Svědecká výpověď generála Karla Palečka.* [Testimony of general Karel Paleček.] Archiv bezpečnostních složek 302_57_2. (In Czech)

[4] BAUER, F. L.: *Decrypted Secrets. Methods and Maxims of Cryptology* (4th revised and extended ed.), Springer-Verlag, Berlin, Heidelberg, 2007.

[5] BECKMAN, B.: *Codebreakers. Arne Beurling and the Swedish Crypto Program During World War II.* American Mathematical Society, Providence, RI, 2002.

[6] CIGÁŇ, K.: *Paul Thümmel - agent operačného zastierania Wehrmachtu.* [Paul Thümmel - Agent of an Operational Camouflage of Wehrmacht], Unpublished manuscript, Komárno, 1967. (In Slovak)

[7] CIGÁŇ, K.: *Posledná akcia "Zradcu X".* [The last action of "traitor X"], Armádní revue (abbreviated A revue) **21** (1968), no. 24, 26–30; no. 25–26, 39–42; **22**, (1969), no. 1, 43; no. 2, 41. (In Slovak)

[8] CIGÁŇ, K.: *Dopady lúštenia šifrovacieho systému čs. londýnskeho MNO z rokov 1940––1945 na domáci odboj.* [Impacts of the Decryption of the Cipher System of the Czechoslovak Ministry of Defence in London from the Years 1940–1945 on the Resistance Movement], Archive of the Slovak National Uprising, Banská Bystrica, Slovakia, Document collection (Fond) V, manuscript no. S36/90, 46 pp.; also in Military Historical Archive (Vojenský historický archív) Prague, signature VÚA-VHA 207/89. (In Slovak)

[62] No further details are given. ŠP

[63] No closer explanation of the "hat method" is given in text. A lottery kind method of sampling is probably meant. ŠP

[9] DRTINA, P.: *Československo můj osud: kniha života českého demokrata 20. století. Přes Mnichov do emigrace*. [Czechoslovakia my Destiny: A Book of Life of a 20th Century Czech Democrat. Through Munich to Emigration.] Book 1, Part 1, Melantrich, Praha, 1991. (In Czech)

[10] FENNER, W.: *Interrogation of Min. Rat Wilhelm Fenner of OKW/Chi*, TICOM, Report I-200, 1946.

[11] GEBHART, J.—KUKLÍK, J.—KOUTEK, J.: *Na frontách tajné války*. [On the Secret War Fronts], Panorama, Praha, 1989. (In Czech)

[12] HANÁK, V.: *Muži a radiostanice tajné války*. [Men and Radio Stations of the Secret War], ELLI print, Dvůr Králové nad Labem, 2002. (In Czech)

[13] JANEČEK, J.: *Gentlemani (ne)čtou cizí dopisy*. [Gentlemen Do (Not) Read Each Other's Mail], Books - Bonus A, Brno, 1998. (In Czech)

[14] JANEČEK, J.: *Válka šifer (Výhry a prohry československé vojenské rozvědky 1939–1945)*. [War of Ciphers (Victories and Failurs of Czechoslovak Military Intelligence 1939–1945], Votobia, Olomouc, 2001. (In Czech)

[15] JANEČEK, J.: *Rozluštěná tajemství (Luštitelé, dešifranti, kódy a odhalení)* (2nd ed.), [Decyphered Mysteries (Solutionist, Decoders, Codes and Revelations)], Nakladavatelství XYZ, Praha, 2002. (In Czech)

[16] JEFFERY, K.: *MI6 (The History of the Secret Intelligence Service, 1909–1949)*. Bloomsbury, London - Berlin - New York - Sydney, 2010.

[17] KAHAN, V.—KAŠPAR, V.: *Klíč přichází z Cařihradu*. [The Key Comes from Constanipole], Signál, April 13, 1967. (In Czech)

[18] KAHN, D.: *The Codebreakers (The Story of Secret Writing)*. Scribner, New York, 1996.

[19] Zpráva o činnosti dr. Vladimíra Krajiny [Report on activities of Dr. Vladimír Krajina], Czech National Archive, Document Collection (Fond) Československá strana národně socialistická -ústřední sekretariát, Praha [Czechoslovak National Socialist Party-Central Secretariat, Prague] 46-35-105/3.

[20] KOKOŠKA, J.—KOKOŠKA, S.: *Spor o agenta A-54 (Kapitoly z dějin československé zpravodajské služby)*. [Dispute About Agent A-54 (Chapters from the History of Czechoslovak Intelligence)], Naše vojsko, Praha 1994. (In Czech)

[21] KREISINGER, P.: *Personální krize v Moravcově zpravodajské "jedenáctce"* [Personel crisis in Moravec' intelligence "eleven"], in: Válečný rok 1941 v československém domácím a zahraničním odboji (L. Kudrna, ed), Sborník k mezinárodní konferenci, Ústav pro studium totalitních režimů. Praha, 2012, pp. 11–19. (In Czech)

[22] KURAL, V.: *Vlastenci proti okupaci: ústřední vedení odboje domácího 1940–1943*. [Patriots Against the Occupation: Central Leadership of Home Resistance 1940–1943], Karolinum, Ústav mezinárodních vztahů, Praha, 1997. (In Czech)

[23] MORAVEC, F.: *Špión jemuž nevěřili*. [A Spy Who Was Not Believed], Leda, Praha, 2014. (In Czech)

[24] PORUBSKÝ, Š.: *STP cipher of the Czechoslovak in-exile Ministry of Defence in London during WWII,* in: Proceedings of EuroHCC '17, 3rd European Historical Ciphers Colloquium, 2017, Smolenice Castle, Slovakia (J. von zur Gathen et al., eds.), Slovak University of Technology in Bratislava, 2017, pp. 47–66.

[25] ——— *Lieutenant colonel Karol Cigáň—an embittered cryptologist* (in preparation).

[26] ——— *Colonel Josef Růžek—the father of Czechoslovak cryptology* (in preparation).

[27] POUSTA, Z.: *Jaroslav Císař—Astronom a diplomat v Masarykových službách.* [Jaroslav Císař—Astronomer and Diplomat in Masaryk's Services], Vyšehrad, Praha, 2016. (In Czech)

[28] ŘEBOUN, O.: *Atentát na Heydricha: Konečně vyjde úřední zpráva.* [Assassination of Heydrich: Official report finaly released], Literární noviny, Saturday May 28, 2011. (In Czech)

[29] ŠOLC, J.: *Po boku prezidenta (František Moravec a jeho zpravodajská služba ve světle archivních dokumentů)* [Alongside of the President (František Moravec and his Intelligence Service in the Light of Archival Documents)], Naš vojsko, Praha 1994.

[30] TICHÝ, A.: *Nás živé nedostanou.* (Historie parašutistické skupiny Antimony) [They Will Not Got Us Alive. (History of the Parachute Group Antimony)], Severočeské nakladatelství, Liberec, 1969. (In Czech)

Received October 22, 2017

Institute of Computer Science
Academy of Sciences of the Czech Republic
Pod Vodárenskou věží 2
CZ–1802-07 Prague
CZECH REPUBLIC
E-mail: sporubsky@hotmail.com