Overview of Ciphers Used by the Czechoslovak "Maffie"

Jozef Krajčovič
Ministry of Justice
Bratislava
Slovakia
kryptosvet@gmail.com

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

Abstract

This paper provides an overview of encryption systems and steganographic techniques used by the Czechoslovak Maffie, which was an anti-Austrian underground resistance organization in 1914-1918.

1 Introduction

Austria-Hungary (1867 – 1918) was a constitutional monarchy and great power in Central Europe and basically a multi-ethnic state entity. Czechs and Slovaks were two of the nations that made up Austria-Hungary. They felt oppressed and their voice were often not heard in the administration of public affairs. The *Maffie* was an underground organization of Czech politicians and leaders formed in Prague during World War I (1914 – 18) and an anti-Austrian resistance organization that engaged in intelligence activities.

In this work, we studied the cryptographic and steganographic techniques used by the representatives of Czechoslovak Maffie. In section 2 we shortly describe the historical background of the organization. Next, in Section 3 we shortly describe the used ciphers and steganographic techniques, and in Section 4 we bring insight into the biggest affair of the resistance called "Button Affair", which is also related to cryptology.

2 Secret Political Organisation Called "Maffie"

Maffie[1] was founded after the emigration of Tomáš Garrigue Masaryk in 1914 by Czech politician Edvard Beneš, who later became the second president of Czechoslovakia, and other (mainly) anti-royalists[2] (Hlaváč, 2008). During the years of the Great World War, it was a central part of the First Czechoslovak Resistance. Its main objective was to overthrow the Emperor of Austria and to cause the disintegration of his country. Their goal was to tirelessly seek all kinds of information of a political, economic, and military nature, and deliver it to Masaryk abroad in a conspiratorial way.

The *Military Maffia*[3] was an armed component of the Czech domestic anti-Austrian resistance in 1914-1918 and was part of a broader movement that led to the establishment of the Czechoslovak Republic. Its main task was to undermine the morale of the Austro-Hungarian army, organize sabotage actions, and prepare for an armed uprising. The Military Maffia played a key role in the preparations for the coup of 28 October 1918, which led to the establishment of the Czechoslovak Republic (Hálek, 2018).

3 Overview of Used Ciphers and Steganographic Techniques

The Czechoslovak Maffie, as well as other secret societies, used various steganographic techniques and a wide range of cryptographic methods for their communication as: hand ciphers, codes, and encryption devices.

One of the simplest methods used[4] was a simple substitution using a field postcard (the so-called "feldpostkarta") with irregularly cut out windows. This card served as an encryption table, also a second card was used with the alphabet. The encryption process was based on changing the relative position of the window part and the alphabet part (Valenta, 1993).

A classical Vigenère cipher (adapted to the

[1] The name 'Maffie' was only a nickname of the group, and has no real connection or reference to the Sicilian crime group called Mafia (Paulová, 1937; Hlaváč, 2008).

[2] Karel Kramář, Alois Rašín, Josef Scheiner and their "boss", Přemysl Šámal.

[3] The main figures of the Military Mafia were František Sis, Vladimír Slavík, Jindřich Čapek and Jaroslav Rošický.

[4] For example used by Karel Locher, a member of the Maffie resistance organization in charge of liaison with the Poles and later served in various political and journalistic positions.

Proceedings of the 8th International Conference on Historical Cryptology, pages 76-79
Poznań, Poland, 16-18 June, 2025

Czech alphabet) was the main cipher used by the organization (Werstadt, 1931), also see Figure 1. This encryption method was, however, easily broken by the Austrian secret service Evidenzburo, which allowed them to monitor communications between the domestic resistance and the emigration (Paulová, 1939). After discovering that the modified Vigenère cipher had apparently been broken, a new, more robust encryption method was selected, based on a reworded alphabet, longer passwords, and shorter blocks of text. The cipher was available in two forms: a ciphering device named *Kryptograf*[5] and its paper version called the "autoclave ruler" according to Josef J. Frič (Kučera, 2003). The cipher was based on the Vigenére autokey.

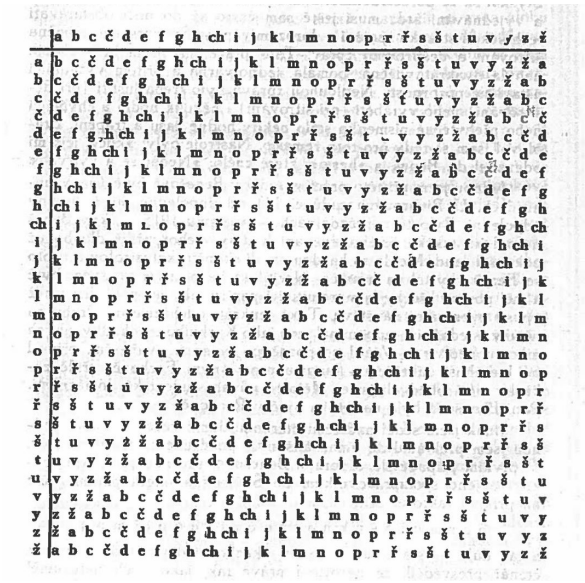


Figure 1: Modified Vigenère / Tabula Recta (Werstadt, 1931)

A different (simple) encryption device was found in (Butyrskij et. al., 2018), however, we were unable to identify the machine (see Figure 2).

At least two different codes were used, one to hide the names of the resistance members in the communication (cover names, see Figure 3) and one classical code book for encryption. The second one encrypts words and phrases to another words and phrases and was marked as *Allegoric Code* (orig. Allegorický kod Československé zahraniční revoluce, see Figure 4).

[5]Created by P. J. Baráček. This ciphering device could be a predecessor of the Condenser PBJ cipher machine, see (Antal et. al., 2024).

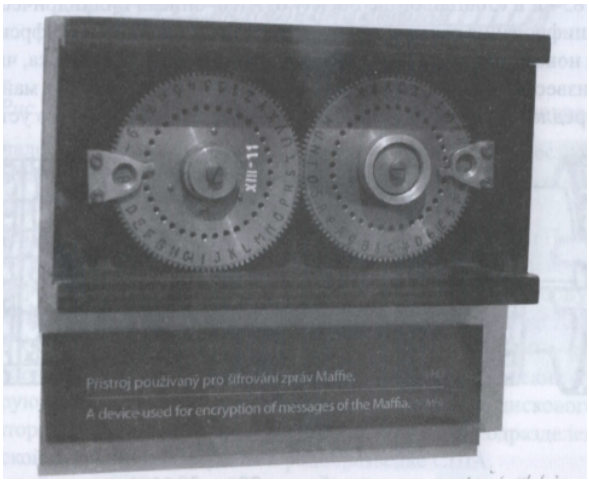


Figure 2: Unidentified encryption device allegedly used by Maffie's spies (Butyrskij et. al., 2018)

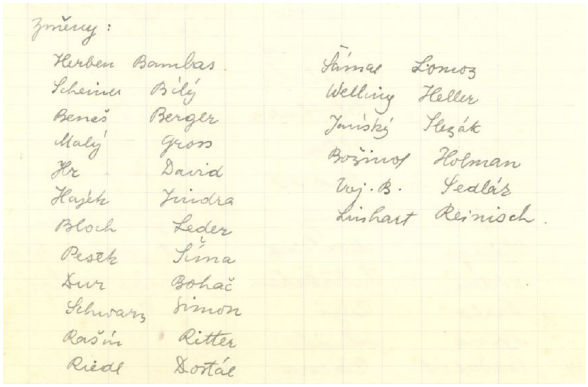


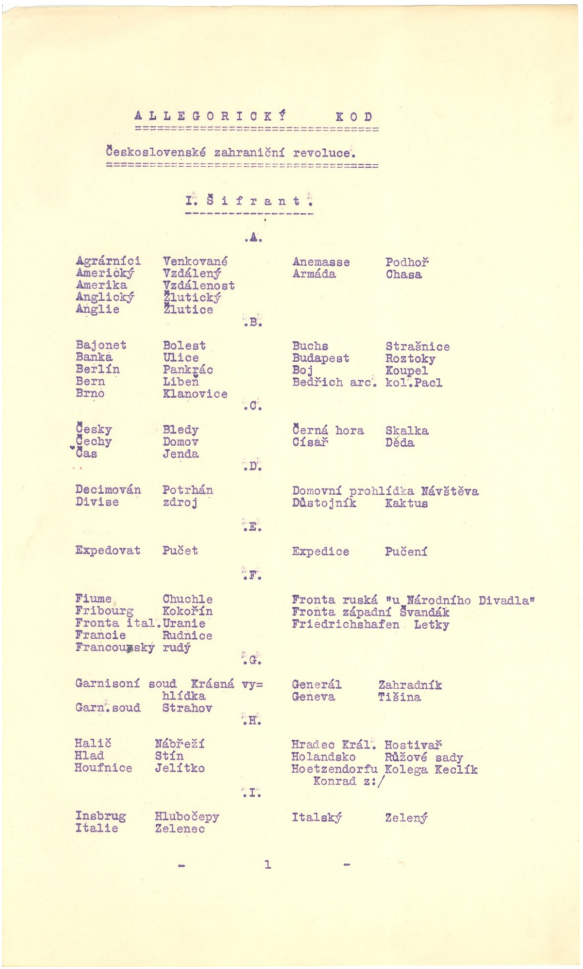
Figure 3: List of cover names of the members of Maffie

Various steganographic techniques were used by the resistance (Stanek, 1931; Očenášek, 1991; Kučera, 2003):

- Invisible ink - developed by Dr. Vladimír Staněk a prominent Czech chemist and scientist. He was the administrator of the chemical department of the Sugar Research Station (see Figure 5).

- Based on a geographical map of Switzerland, different cantons meant different fronts. The order of the letters in the text of the postcard signified an assessment of the overall situation (politically and militarily).

- Two identical metal plates with holes that looked like a sieve. Each hole corresponds to one letter of the alphabet according to a secret key.



ALLEGORICKÝ KOD

Československé zahraniční revoluce.

I. Šifrant.

.A.

Agrárníci	Venkovaný	Anemasse	Podhoř
Americký	Vzdálený	Armáda	Chasa
Amerika	Vzdálenost		
Anglický	Žlutický		
Anglie	Žlutice		

.B.

Bajonet	Bolest	Buchs	Strašnice
Banka	Ulice	Budapest	Roztoky
Berlín	Pankrác	Boj	Koupel
Bern	Liben	Bedřich arc.	kol.Pacl
Brno	Klanovice		

.C.

Česky	Bledy	Černá hora	Skalka
Čechy	Domov	Císař	Děda
Čas	Jenda		

.D.

Decimován	Potrhán	Domovní prohlídka	Návštěva
Divise	zdroj	Důstojník	Kaktus

.E.

Expedovat	Pučet	Expedice	Pučení

.F.

Fiume	Chuchle	Fronta ruská	"u Národního Divadla"
Fribourg	Kokořín	Fronta západní	Švandák
Fronta ital.	Uranie	Friedrichshafen	Letky
Francie	Rudnice		
Francouzsky	rudý		

.G.

Garnisoní soud	Krásná vyhlídka	Generál	Zahradník
		Geneva	Tišina
Garn.soud	Strahov		

.H.

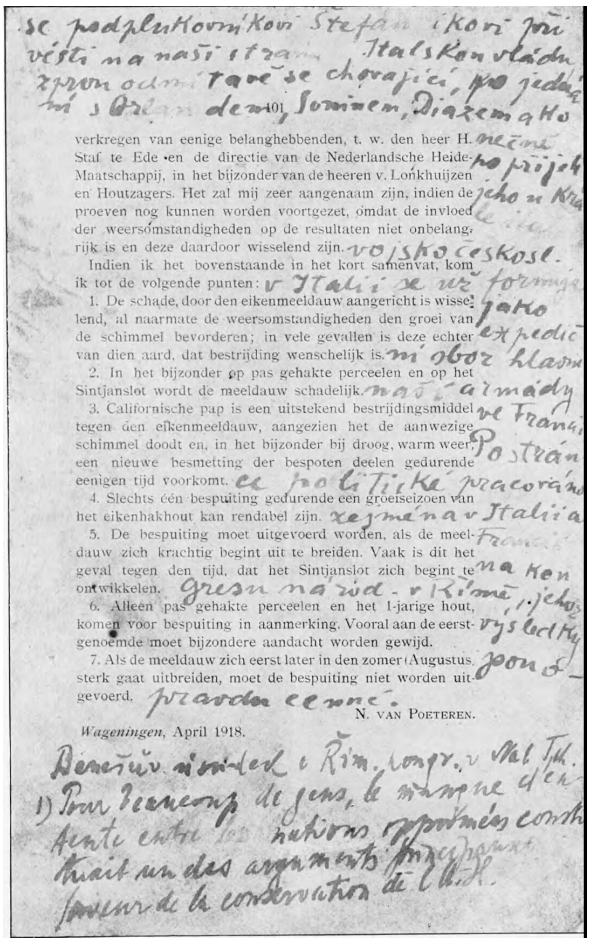
Halič	Nábřeží	Hradec Král.	Hostivař
Hlad	Stín	Holandsko	Růžové sady
Houfnice	Jelítko	Hoetzendorfu	Kolega Kecílk
		Konrad z:/	

.I.

Insbrug	Hlubočepy	Italský	Zelený
Italie	Zelenec		

- 1 -

Figure 4: First page of the Allegoric Code (VHA, 1915)



401

verkregen van eenige belanghebbenden, t. w. den heer H. Staf te Ede en de directie van de Nederlandsche Heide-Maatschappij, in het bijzonder van de heeren v. Lonkhuijzen en Houtzagers. Het zal mij zeer aangenaam zijn, indien de proeven nog kunnen worden voortgezet, omdat de invloed der weersomstandigheden op de resultaten niet onbelangrijk is en deze daardoor wisselend zijn.

Indien ik het bovenstaande in het kort samenvat, kom ik tot de volgende punten:

1. De schade, door den eikenmeeldauw aangericht is wisselend, al naarmate de weersomstandigheden den groei van de schimmel bevorderen; in vele gevallen is deze echter van dien aard, dat bestrijding wenschelijk is.
2. In het bijzonder op pas gehakte perceelen en op het Sintjanslot wordt de meeldauw schadelijk.
3. Californische pap is een uitstekend bestrijdingsmiddel tegen den eikenmeeldauw, aangezien het de aanwezige schimmel doodt en, in het bijzonder bij droog, warm weer, een nieuwe besmetting der bespoten deelen gedurende eenigen tijd voorkomt.
4. Slechts één bespuiting gedurende een groeiseizoen van het eikenhakhout kan rendabel zijn.
5. De bespuiting moet uitgevoerd worden, als de meeldauw zich krachtig begint uit te breiden. Vaak is dit het geval tegen den tijd, dat het Sintjanslot zich begint te ontwikkelen.
6. Alleen pas gehakte perceelen en het 1-jarige hout, komen voor bespuiting in aanmerking. Vooral aan de eerstgenoemde moet bijzondere aandacht worden gewijd.
7. Als de meeldauw zich eerst later in den zomer (Augustus) sterk gaat uitbreiden, moet de bespuiting niet worden uitgevoerd.

N. VAN POETEREN.

Wageningen, April 1918.

Figure 5: Magazine "Prager Zuckermarkt" with a steganographic message written with Dr. Staněk's original invisible ink (Stanek, 1931)

- Newspaper advertisements were used to confirm the successful delivery of encrypted messages.

- Furthermore, a special case/luggage/shoes with double walls and hidden compartments were used to carry the messages.

A combination of encryption and steganography was used in a network in Genoa, Italy, to transmit confidential information (Kučera, 2003). It consisted of three layers. The message was first encrypted, then written with invisible ink, and concealed in scrolls or other inconspicuous objects. The sent messages passed through the hands of the Austrian censors, but thanks to the precision of the encryption, their contents remained undetected (Paulová, 1939).

4 The "Button Affair"

A very famous (espionage) affair of the Czechoslovak resistance was the so-called *Button Affair*. It was one of the biggest blows during the war when the Czechoslovak resistance was fighting against Austria-Hungary. The affair had serious consequences for the Czechoslovak resistance, including the arrest of many prominent figures. The case became well-known and was discussed after the establishment of Czechoslovakia, becoming the subject of political controversy.

We shortly describe the events of the affair. In September 1915, Edvard Beneš and Jan Kyjovský decided to send Aloysia (Lola) Linhart to a specific mission. As a courier, she was responsible to deliver a secret message (see Figure 6) from Switzerland to Prague. She hid the message in a button on her dress, which was considered a safe way of transporting the information. Lin-

hart successfully crossed the border and arrived in Prague, where she was to deliver the message. However, due to a conspiratorial error and the incompetence[6] of some members of the Resistance, and the report fell into the hands of the wrong people, leading to the exposure and arrest of several people. (Paulová, 1937; Paulová, 1939; Lukeš, 2016)

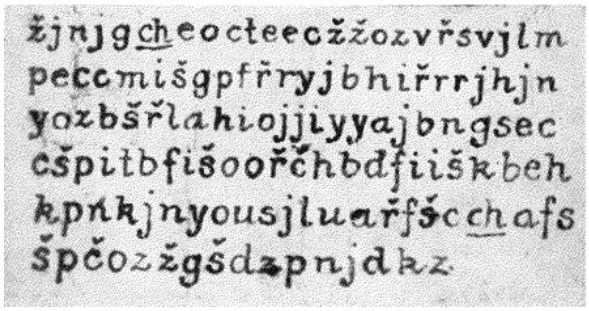


Figure 6: Encrypted message from Aloysia (Lola) Linhart's button (Pichlík, 1991)

The message was encrypted using the modified Vigenère cipher (adapted to the Czech alphabet). The Austrian military authorities had already deciphered the key to the Maffian alphabet during the affair, which gave them access to sensitive information and allowed them to intervene more effectively against the resistance (Kárník, 1995).

Acknowledgments

This work was supported by grant VEGA 2/0054/24.

References

Eugen Antal, Paul Reuvers and Pavol Zajac. 2024. The Condenser PBJ cipher machine. Cryptologia. https://doi.org/10.1080/01611194.2024.2372254.

L.S. Butyrsky, D.A. Larin, G.P. Shankin 2018. *Kriptograficheskiy front Velikoy Otechestvennoy.*. Moskva, Gelios ISBN: 978-5-85438-220-5.

Jan Hálek. 2018. Vojenská Maffie. K pramenum a interpretaci ozbrojené složky české domácí protirakouské rezistence. In *Historie a vojenství*, pages 4 - 13. Vojenský historický ústav, 2018.

Miroslav Hlaváč. 2008. *Čeští mafiáni 1914-1918*. Paris, Karviná ISBN 978-80-87173-00-8.

Zdeněk Kárník. 1995. Edvard Beneš a Maffie v nejtěžším období Velké války. Řídila politická emigrace domácí odboj? (červenec 1917 – říjen 1918). In *Historie a vojenství*, pages 3 - 22. Vojenský historický ústav, 1995.

Martin Kučera. 2003. *Zprávy tajným inkoustem: kapitola z dějin českého zpravodajství za první světové války (1914-1918)*. Masarykův ústav AV ČR, Praha ISBN 80-86495-18-3.

Michal Lukeš. 2016. *Špionážní případy. První republika*. Academia, Praha ISBN 978-80-200-2529-6.

Ludvík Očenášek. 1919. *Na pomoc dohodě: tajná činnost několika českých vlastenců za války*. Tiskem Pražské akciové tiskárny, nákl. vlastním, 1919.

Karel Pacner. 2002. *Československo ve zvláštních službách: pohledy do historie československých výzvědných služeb 1914-1989*. Themis, Praha ISBN 80-7312-002-X.

Milada Paulová. 1937. *Dějiny Maffie: odboj Čechů a Jihoslovanů za světové války 1914-1918, I.díl*. Československá grafická Unie, Praha.

Milada Paulová. 1939. *Dějiny Maffie: odboj Čechů a Jihoslovanů za světové války 1914-1918, I.díl, 2.část*. Československá grafická Unie, Praha.

Karel Pichlík. 1991. *Bez legend.*. Praha, Panorama ISBN 80-7038-217-1.

Vladimír Staněk. 1931. Z maffiánské laboratoře. *Naše revoluce VII. pp. 59-79.*

Jaroslav Valenta. 1934. Český Wallenrod. (Politický důvěrník české Maffie Karel Locher v Krakově v r. 1918.). *Slovanské historické studie. 19, (1993,) pp. 50-70.*

Jaroslav Werstadt. 1931. Ze vzpomínek Starckových. *Naše revoluce VII. pp. 210-222.*

VHA 1915. Alegorický kod československé zahraniční revoluce. Spojovací klíče. *ČSNR V PAŘÍŽI III-5 – (1915) 1916-1918.* Inv. n. 5464 Karton varia

[6]In Prague, Aloysia (Lola) Linhart contacted Bohumil Mareš, who was to deliver the message onwards. Mareš tried to pass the message on to the editors of Čas, but he was unsuccessful. Then he contacted the deputy František Soukup, who knew nothing about the mission and refused to accept the report. Mareš's suspicious behavior led Soukup to inform the police. The police arrested Mareš, Linhart, and others involved, including the editors of Čas.