universität wien

MASTERARBEIT / MASTER'S THESIS

Titel der Masterarbeit / Title of the Master's Thesis

Die Entwicklung der Chiffriertechnik in der zweiten Hälfte des 19. Jahrhunderts

verfasst von / submitted by

Willibald Zibuschka, BA

angestrebter akademischer Grad / in partial fulfilment of the requirements for the degree of

Master of Arts (MA)

Wien, 2017 / Vienna 2017

Studienkennzahl lt. Studienblatt / degree programme code as it appears on the student record sheet:	A 066 803
Studienrichtung lt. Studienblatt / degree programme as it appears on the student record sheet:	Masterstudium Geschichte
Betreut von / Supervisor:	Univ.-Prof. Dr. Peter Becker

A

Inhaltsverzeichnis

1 Einleitung 1

2 Frühe Methoden der Verschlüsselung 10

2.1 Geheimschriften seit der Antike bis zum Mittelalter 10

2.2 Die monoalphabetische Verschlüsselung und die Statistik 14

2.3 Kryptographische Verfahren vom 16. bis zum 18. Jahrhundert 16

2.4 Zweistellige und dreistellige Chiffren–Schlüssel 23

2.5 Vierstellige Chiffren–Schlüssel 27

3 Chiffrierung und Dechiffrierung im Hause Habsburg 31

3.1 Die Wiener Briefüberwachung 32

3.1.1 Die geheime Ziffernkanzlei bis 1848 33

3.1.2 Geheime Ziffernsektion unter Kaiser Franz Joseph 37

3.2 Postlogen und ihre Bedeutung 39

3.2.1 Dienstverrichtung in den Postlogen 44

3.3 Organisation der „Sektion“ für Chiffrenwesen 47

4 Presse und Geheimdienst im Neo–Absolutismus 54

4.1 Telegraphie, Diplomatie und Pressepolitik 55

4.2 Netzwerk der Agenten 58

5 Technische und organisatorische Entwicklungen im 19. Jahrhundert. 63

5.1 Informationswege durch Post, Telegraphie und Telephon 64

5.2 Die Entwicklung der Konstruktion der Telegraphie–Geräte 65

5.2.1 Nadel–Telegraph von Cooke und Wheatstone 66

5.2.2 Telegraph von Alexander Bain 67

5.2.3 Druck–Telegraph von Morse 68

5.3 Ausbau des Telegraphie–Netzes in Europa und weltweit 71

5.4 Das Telephon in Österreich 73

5.5 Drahtlose Telegraphie zur Jahrhundertwende 75

5.6 Gründung nationaler und internationaler Telegraphenvereine 77

5.6.1 Deutsch–Österreichischer Telegraphen–Verein 78

5.6.2 Der Internationale Telegraphen–Verein 79

5.7 Feldtelegraphenwesen der österreichisch–ungarischen Armee 81
6 Entwicklung der Chiffren–Schlüssel für die Telegraphie 84
6.1 Chiffren–Tafeln aus Braunschweig und Preußen 84
6.2 Chiffrieranleitungen und Methoden in Wien 88
6.3 Verschlüsselung für das Militär 99
6.3.1 Militärschlüssel für untergeordnete Zwecke 99
6.3.2 Die Transponiermethode 103
7 Zusammenfassung 109
8 Verwendete Quellen und Literatur 112
8.1 Quellenverzeichnis 112
8.2 Nachschlagewerk 112
8.3 Literatur 112
8.4 Internetressourcen 115
9 Tabellen- und Abbildungsverzeichnis 116
9.1 Tabellen 116
9.2 Abbildungen 116
10 Abstract 119

1 Einleitung

Vertrauliche oder geheime Botschaften durch Verdecken oder Verschlüsseln unbeteiligten Freunden oder Feinden unzugänglich zu machen, beschäftigte die Menschen mit unter–schiedlichen Absichten seit der Antike und ist im Zeitalter des Internets aktueller denn je. In der langen Geschichte der Geheimschriften wurden viele Methoden entwickelt, Nachrichten zu verschlüsseln und vor Dritten versteckt zu halten. Genauso wurden durch Kryptoanalysten aber auch immer wieder Methoden entwickelt, die verwendeten Geheimschlüssel zum Entziffern der Botschaften herauszufinden.

Eine Zäsur für eine Verschlüsselung von Nachrichten stellte Mitte des 19. Jahrhunderts die Einführung der Telegraphie[1] dar. Im Zuge der „technischen Revolution" wurden Entfernungen durch Schiffe, Eisenbahnen und Telegraphenleitungen sozusagen ausgelöscht und der Austausch von Menschen, Produkten und Nachrichten beschleunigt.[2] Es wird der Frage nach der Entwicklung der Chiffriertechnik in der zweiten Hälfte des 19. Jahrhunderts bis zum Beginn des Ersten Weltkrieges nachgegangen, um herauszufinden, wie sich die neuen technischen Möglichkeiten der Telegraphie auf die Chiffrierung von Nachrichten auswirkten. Ein zweiter Grund, der das Augenmerk auf die zweite Hälfte des 19. Jahrhunderts lenkte, waren die politischen Aufstände, die im März 1848 ausbrachen und das verhasste Regime Metternichs zu Fall brachten, womit auch der berüchtigten *Polizeihofstelle* ein Ende bereitet wurde. Nach einer kurzen Unterbrechung wurde die geheime Briefüberwachung am Beginn des Neo–Absolutismus in der „Section für Ziffernwesen und translatorische Arbeiten" im Ministerium des Äußern wiederbelebt. Im August 1849 gelang es den Österreichern, mit Hilfe eines großen russischen Kontingents, die Aufständischen in Ungarn zu besiegen, womit das definitive Ende des revolutionären Geschehens besiegelt wurde.[3] Unmittelbar nach diesem Sieg kam die Polizei unter die Leitung des Innenministeriums unter Alexander von Bachs (1813–1893). Bach baute eine Organisation für die Sicherheit auf, die eine umfangreiche Agententätigkeit zur Überwachung der ungarischen Emigranten einschloss. Die Verschlüsselung von telegraphischen Depeschen wurde in einigen sensiblen Bereichen zu

[1] Für eine leichtere Lesbarkeit wurde die zeitgenössische Schreibweise der Begriffe „Telegraphie", „Telephonie" und artverwandter Begriffe in den Aufzeichnungen mit „ph" beibehalten und nicht abwechselnd mit der heutigen Schreibweise verwendet.
[2] Emily *Rosenberg*, Einleitung. In: Emily *Rosenberg* (Hg.), Weltmärkte und Weltkriege, 1870–1945 (München 2012) 9–32, hier 9.
[3] Pieter M. *Judson*, Habsburg, Geschichte eines Imperiums 1740–1918. (München 2017) 278.

einem wichtigen Instrumentarium, wie in der Diplomatie, in der Pressepolitik und nicht zuletzt in der Armee, vor allem in Kriegszeiten.

Wenn schon von Kriegszeiten die Rede ist, soll die Arbeit mit einer Anekdote beginnen, die sich am Beginn des Ersten Weltkrieges abgespielt haben könnte und die Jaroslav Hašek in „Die Abenteuer des braven Soldaten Schwejk“ über ein vergessenes Buch mit dem Schlüssel zur Dechiffrierung einer militärischen Depesche erzählt.

Auf der Fahrt an die Front in Galizien befand sich der Militärzug im April 1915 kurz vor der Stadt Raab in Ungarn, als im Stabswaggon, in dem die Offiziere des Marschbataillons saßen, eine sonderbare Stille eintrat. Die Offiziere waren in ein kleines Buch mit der Aufschrift: „Die Sünden der Väter“, einer Novelle von Ludwig Ganghofer (1855–1920), vertieft und alle waren gleichzeitig mit der Lektüre der Seite 161 beschäftigt. Bataillonskommandant Hauptmann Sagner hielt dasselbe Buch in der Hand, ebenfalls auf Seite 161 aufgeschlagen und überlegte, wie er den Offizieren klar machen könnte, was sie mit dem Buch, eigentlich streng vertraulich, anfangen sollten. Mit geheimnisvollem Ausdruck sagte Hauptmann Sagner: „meine Herren, vergessen Sie nie auf Seite 161!“ In diese Seite vertieft, vermochten sie aus dem Ganzen nicht klug zu werden, da eine Martha zum Schreibtisch trat und dort eine Papierrolle heraus zog. Dann tauchte auf der gleichen Seite noch Albert auf, der sich bemühte, scherzhaft zu sprechen. „Also meine Herren“ fuhr er feierlich fort, „eine ganz vertrauliche Information betreffs des neuen Systems des Chiffrierens von Depeschen im Feld. ‚Die Sünden der Väter‘, Seite 161, ist der Schlüssel zu der neuen Chiffriermethode, die aufgrund einer neuen Verordnung des Generalstabes des Armeekorps in Gültigkeit getreten ist.“ Er hatte das zweite Buch samt der Information vom Herrn Oberst persönlich bekommen.[4]

„Wenn wir zum Beispiel den Befehl erhalten sollten: „Auf Kote 228 Maschinengewehrfeuer links richten“, erhalten wir, meine Herren, diese Depesche: „Sache – mit – uns – das – wir – auf – sehen – in – die – versprachen – die – Martha – dich – das – ängstlich – dann – etc.“ Also sehr einfach, ohne jede überflüssige Kombination. Vom Stab per Telephon zum Bataillon, vom Bataillon per Telephon zur Kompanie. Der Kommandant entziffert diese chiffrierte Depesche auf folgende Weise: Er nimmt „Die Sünden der Väter“, schlägt Seite 161 auf und fängt an, oben auf der gegenüberliegenden Seite das Wort ‚Sache‘ zu suchen, das auf Seite 160 das zweiundfünfzigste Wort ist. Nun sucht er auf Seite 161 den zweiundfünfzigsten

[4] Jaroslav *Hašek*, Die Abenteuer des braven Soldaten Schwejk. Quer durch Ungarn (Berlin/Weimar 1976) 488–516.

Buchstaben von oben. Beachten Sie, dass es ‚A' ist. Das nächste Wort in der Depesche ist ‚mit', das siebente Wort, das auf gleiche Weise entschlüsselt dem Buchstaben ‚u' entspricht. Und so fahren wir fort, bis wir den Befehl feststellen: „Auf Kote 228 Maschinengewehrfeuer links richten."[5]

Außer Hauptmann Sagner fand keiner der Offiziere auf Seite 160 die Worte, denen auf Seite 161 die Buchstaben entsprachen. Einer der Offiziere entdeckte, dass der Roman von Ganghofer zwei Teile hatte. Auf der Titelseite war zu lesen: „Roman in zwei Bänden". Tatsächlich hatte Oberst Sagner den zweiten Teil vom Brigadestab. Dem Regiment hat man aber nicht angegeben, dass es sich um den zweiten Teil handelt, und so ist das Ganze geschehen.

Sofort nach Ankunft des Zuges in Raab ließ sich Oberleutnant Lukasch wie in einem Verhör von Schwejk erzählen, wie das mit den Büchern von Ganghofer einen Tag vor der Abfahrt war, die er von der Regimentskanzlei aufs Bataillon getragen hatte. Der Regimentsfeldwebel hatte Schwejk gesagt, dass man beim Bataillon wissen werde, welcher von den zwei Teilen zu nehmen sei. Schwejk hatte Oberleutnant Lukasch telephonisch darüber Mitteilung gemacht und gefragt „ob man bei Militär jetzt die Bücher in verkehrter Reihenfolge liest, zuerst den zweiten und dann den ersten Teil". Schwejk hat in seiner Überlegung von Lukasch bestärkt, den ersten Teil in die Bataillonskanzlei getragen, während der zweite Teil in der Kompaniekanzlei zurück blieb. Oberleutnant Lukasch erklärte Schwejk mit einem tiefen Seufzer: „Sie sind sich der Tragweite Ihrer Handlung nicht bewusst. Wenn Sie wüssten, was sie gemacht haben. – Aber Sie werden es nie erfahren."[6] So unterhaltsam diese Geschichte auch erzählt worden sein mag, verbergen sich darin einige ernste Themen, wie Chiffren–Schlüssel, Übertragung, geheime Nachricht, Spionage, Dechiffrierung und Auswertung, die in dieser Arbeit untersucht werden, aber auch die Weltfremdheit der Stäbe im Angesicht industrieller Massenvernichtungswaffen.

Nach dieser Einleitung wird im zweiten Kapitel ein Rückblick auf die Entwicklung der Geheimschriften seit der Antike bis ins 19. Jahrhundert gegeben, um grundsätzliche Methoden und ihre Unterschiede anhand von Beispielen zu erklären. Die Methoden für die Übermittlung geheimer Botschaften teilen sich in zwei Hauptgruppen, dem *Verbergen* einer Nachricht bzw. dem *Verschlüsseln der Schrift* einer Nachricht. Für die Bedeutung „verdecktes

[5] *Hašek*, Die Abenteuer des braven Soldaten Schwejk, 509.
[6] *Hašek*, Die Abenteuer des braven Soldaten Schwejk, 514–516.

Schreiben“ wurde der Ausdruck *Steganographie* von Caspar Schott (1608–1666), einem Jesuit, im Buch mit dem Titel „Schola Steganographica“ verwendet.[7] Diese Methode zielt darauf ab, die Existenz einer Nachricht vor Feinden zu verbergen, um diese durch „bewachte Tore“ zu schmuggeln. Die zweite Gruppe von Methoden, die eine Nachricht für Unbefugte unlesbar macht, wird *Kryptographie* genannt. Der Ausdruck *Kryptographie* wurde als „cryptographia“ für „secrecy in writing“ 1641 von John Wilkins (1614–1672), neben Wallis einem Gründer der „Royal Society“, eingeführt.[8]

Die erste Übermittlung einer verborgenen Botschaft wurde bereits vom Geschichtsschreiber Herodot beschrieben. Den Griechen, von den Persern belagert, wurde die, unter dem Wachs einer Wachstafel versteckte Nachricht, dass Xerxes einen Angriff vorbereite, zugespielt. So konnten sich die Griechen zur Vermeidung eines Überraschungsangriffes bewaffnen und sich erfolgreich verteidigen, womit die Eroberung durch Xerxes 480 v. Chr. verhindert wurde.[9] In den folgenden 2000 Jahren wurden unterschiedlichste Methoden zum Verstecken von Botschaften erdacht und in Form von verschluckten Wachskügelchen mit darin enthaltenen beschriebenen Seidenstreifen oder mit einer unsichtbaren Tinte beschriebenen Eier durch Boten befördert. Im gleichen Zeitraum, in dem die Verfahren der Steganographie angewendet wurden, entwickelten sich parallel dazu Methoden der Kryptographie, welche die Botschaft selbst unverständlich machten.[10]

Die historisch wichtigen Geheimschriften begannen mit der Substitution von Buchstaben, die durch Verschieben des Klartext–Alphabetes um drei oder mehr Buchstaben zum Geheimtext–Alphabet wurde, und die Julius Caesar (100–44 v. Chr.) im Gallischen Krieg verwendet hatte.[11] Die Schwäche dieses monoalphabetischen Verschlüsselungsverfahrens beruhte darauf, dass die Häufigkeit der Buchstaben erhalten blieb. Man müsste so verschlüsseln können, dass alle Buchstaben im Geheimtext möglichst gleichmäßig verteilt sind und keine Häufigkeiten einzelner Buchstaben oder Buchstabenkombinationen erkennen lassen. Diese Idee führte zur so genannten polyalphabetischen Verschlüsselung, die im 16. Jahrhundert in vielen Köpfen entstand. Die wichtigsten waren die Verfahren der Italiener Leon Battista Alberti (1404–

[7] Caspar *Schott*, Schola Steganographica (Nürnberg 1665).
[8] Friedrich L. *Bauer*, Entzifferte Geheimnisse. Methoden und Maximen der Kryptologie (2., erw. Aufl. Berlin/Heidelberg 1997) 9.
[9] Simon *Singh*, Geheime Botschaften. Die Kunst der Verschlüsselung von der Antike bis in die Zeiten des Internet (München/Wien 2000; Taschenbuch, München [4]2003) 12.
[10] *Singh*, Geheime Botschaften, 21.
[11] *Singh*, Geheime Botschaften, 25.

1472) und Giovanni Battista Della Porta (1535–1615), des Deutschen Johannes von Trittenheim (Trithemius, 1462–1516) und des Franzosen Blaise de Vigenère (1523–1585).[12]

Es werden einige praktisch eingesetzte Verfahren aus dem 18. und dem Beginn des 19. Jahrhunderts beschrieben, die beachtliche methodische Raffinessen enthalten. Diese Chiffren–Schlüssel wurden vermutlich von der „Ziffernkanzlei" für die eigenen diplomatischen Dienste im Ausland entworfen und sind im Faszikel 17 (alt 24) innerhalb der „Interiora" der Staatskanzlei im Wiener Haus–, Hof– und Staatsarchiv undatiert aus der Regierungszeit Maria Theresias bis Franz II./I. zu finden. An diesen Beispielen ist die stetige Entwicklung von zwei–, meist drei– bis vierstelligen Chiffren–Tabellen zu erkennen. Zur Erschwerung einer Kompromittierung wurden die Chiffren–Tabellen oft gewechselt.[13]

Ausführlich wird im dritten Kapitel die Organisation der Briefüberwachung in den Postlogen und in der „Geheimen Kabinettskanzlei" im Hause Habsburg bis 1848 bzw. in der „Ziffernsektion" unter Kaiser Franz Joseph beschrieben. Bereits Maximilian I. und Karl V. sollen die Briefspionage angewendet haben.[14] Im 17. Jahrhundert verfügten alle europäischen Mächte über geheime Dienststellen im „Cabinet Noir", oder der so genannten „Schwarzen Kammer", in denen fremde Botschaften geöffnet, in aller Eile abgeschrieben und von Kryptoanalytikern entschlüsselt wurden. Die Beförderung der Briefe durfte keine zeitliche Verzögerung erfahren, weshalb in anderen Städten Postlogen einrichtet wurden. Die geheime Kabinettskanzlei in Wien wurde, wegen der hohen Anzahl erfolgreicher Dechiffrierungen, in Fachkreisen als „schlagkräftigste Schwarze Kammer" gerühmt.[15]

Die Geschichte der „Geheimen Ziffernkanzlei" hatte durch die Märzrevolution ein Ende gefunden. Die Institution selbst aber ging, nach dem Ende der Revolutionen, in die neue „Sektion für Ziffernwesen und translatorische Arbeiten" im Ministerium des Äußern, der kurz genannten „Ziffernsektion" über. Es sollte nur etwa ein Jahr dauern, bis auch die alten Agenden der geheimen Briefüberwachung wieder aufgenommen wurden.[16] Außer der Dechiffrierung sämtlicher Interzepte, die selbst gewonnen und die von den Postlogen in

[12] Albrecht *Beutelspacher*, Geheimsprachen. Geschichte und Technik (5., aktual. Aufl. München 2012) 29.
[13] OeStA/HHStA StK Interiora 17 (alt 24), Chiffrenschlüssel, Mappe: Anonyme Schlüssel K. Franz II. (1792-1835).
[14] Franz *Stix*, Zur Geschichte und Organisation der Wiener Geheimen Ziffernkanzlei (Von ihren Anfängen bis zum Jahr 1848). In: Mitteilungen des Instituts für Österreichische Geschichtsforschung, Band 51 (1937) 131.
[15] *Singh*, Geheime Botschaften, 81.
[16] Harald *Hubatschke*, Die Wiener Geheime Ziffernkanzlei (1716-1848). In: Mitteilungen des Instituts für Österreichische Geschichtsforschung, Band 83, Heft 3 (1975) 389.

anderen Städten zugeleiteten, war eine weitere Aufgabe der „Ziffernsektion“, Ziffernschlüssel für die eigenen diplomatischen Vertretungsbehörden im Ausland zu entwerfen, die dem Ziffernkabinett der Staatskanzlei zur Verfügung gestellt wurden. Von diesen selbst entworfenen Ziffernschlüsseln sind nur wenige erhalten, weil sie vernichtet wurden, wenn es die politische Situation erforderte.[17]

Die schnelle Nachrichtenübermittlung hatte ihren Einfluss auf die Pressepolitik, die Diplomatie und das Agentennetz des Innenministers. Diese Themen werden im Kapitel vier behandelt. Der Liberalisierung des Pressegesetzes durch „die Erklärung der Aufhebung der Censur in allen Staaten, wo sie besteht“[18] durch Kaiser Ferdinand I. im März 1848 musste die staatliche Macht der politischen Öffentlichkeit, der „öffentlichen Meinung“ Rechnung tragen. Mit dem Pressepatent, das Kaiser Franz Joseph bereits im März 1849 erlassen hatte, überwogen aber repressive polizeistaatliche Methoden in der Handhabung der Presse. Reglementierung, Überwachung und präventives Verbot regierungsfeindlicher politischer Öffentlichkeit ersetzten fast zur Gänze „positive“ pressepolitische Maßnahmen.[19] Regierungsfreundliche und genehmigte Meldungen wurden chiffriert an die Außenstellen telegraphiert und an ausgewählte Redaktionen zur Veröffentlichung weitergeleitet.

Am Anfang des 19. Jahrhunderts brachte Europa zunehmend gefährliche autoritäre Systeme hervor, die in der ganzen Welt zu bedrohlichen Beispielen wurden. Alle Systeme, von der frühen „Polizeihofstelle“ der Ära Fürst Metternich bis zu dem ausgeklügelten Netzwerk des Innenministeriums von Alexander von Bach nach 1849, und der „Trete Otdelenie“ des russischen Zaren Nikolaus I. entsprangen dem Bestreben, einen umfassenden Überwachungsstaat mit gnadenloser Bespitzelung verdächtiger Personen und Zensur der Presse einzurichten.[20]

Die Arbeit der Geheimpolizei erlangte nach den niedergeschlagenen Revolutionen, während sich das neoabsolutistische System etablierte, besondere Bedeutung. Das von Alexander von

[17] Harald *Hubatschke*, Ferdinand Prantner (Pseudonym Leo Wolfram) 1817-1871. Die Anfänge des politischen Romans sowie die Geschichte der Briefspionage und des geheimen Chiffredienstes in Österreich. Buch 5 (ungedruckte philosophische Dissertation, Wien 1975) 1289.
[18] Allerhöchstes Patent vom 15. März 1848. Verleihung der Constitution und Aufhebung der Censurgesetze. Online unter: <http://alex.onb.ac.at/cgi-content/alex?aid=pgs&datum=1848&page=88&size=45>(17. Okt. 2017).
[19] Leopold *Kammerhofer*, Diplomatie und Pressepolitik 1848-1918. In: Peter *Urbanitsch*, Adam *Wandruszka* (Hg.) Die Habsburgermonarchie 1848-1918, Band VI/I: Die Habsburgermonarchie im System der Internationalen Beziehungen (Wien 1989) 460f.
[20] Tibor *Frank*, Ein Diener seiner Herren. Werdegang des österreichischen Geheimagenten Gustav Zerffi (1820–1892) (Wien/Köln/Weimar 2002) 10.

Bach geleitete Innenministerium erhielt die Aufgabe, die ins Ausland geflüchteten Ungarn geheim zu überwachen. Unter Bach (1813–1893) errichtete die Polizei ein Agentennetz, das sich über mehrere Länder erstreckte. Die Berichte der Agenten wurden unter Decknamen meistens über Adressen in Wien an die „Central–Section" im Innenministerium gesandt. Aus diesen Berichten fertigte der Innenminister politische Wochenberichte an, die er in den Sitzungen des Ministerrates dem jungen Kaiser Franz Joseph vortrug.[21]

Um die grenzüberschreitende Kommunikation zu ermöglichen, mussten Verträge geschlossen werden, in denen in administrativer und technischer Hinsicht einheitliche Bedingungen zu schaffen waren. Im fünften Kapitel widmet sich die Arbeit daher den Erfindungen und technischen Erklärungen zur Entwicklung des Transportes von Personen, Gütern und Nachrichten im 19. Jahrhundert, besonders aber der elektromagnetischen Telegraphie bis zur drahtlosen Telegraphie. Es werden die Gründungen des „Deutsch–Österreichischen Telegraphen–Vereins" auf der Konferenz vom 25. Juli 1850 und des „Internationalen Telegraphenvereins" (International Telegraph Union) anlässlich des ersten internationalen Telegraphenkongresses 1865 in Paris beschrieben.[22]

Die elektrische Telegraphie war die erste entwickelte Telekommunikations–Technologie, die eine Entmaterialisierung des globalen Informationsflusses möglich machte. Die Übermittlung einer Nachricht war somit von der Bewegung von Menschen und Tieren losgelöst. Das Wort „telecommunication" wurde erstmals von Edouard Estaumé (1862–1942) in seinem Buch „Trauté pratique de télécommunication électrique" benützt, das im Jahr 1904 erschien. Die neue Bezeichnung wurde aus dem griechischen Wort τηλε (tele) für „fern" und dem lateinischen Wort *communicare* für „gemeinsam machen" zusammengesetzt.[23]

Nachdem die Technologie eine bestimmte Reife für eine verlässliche Verwendung erreicht hatte, bildeten sich in den Ländern West– und Mitteleuropas sowie den Vereinigten Staaten von Amerika dichte Telegraphen–Netzwerke aus, die Schritt für Schritt miteinander verbunden wurden. Mit der Verlegung von Unterwasserkabeln begann die „Verkabelung der Welt", wodurch in der zweiten Hälfte des 19. Jahrhunderts ein globales Telegraphennetzwerk

[21] Tibor *Frank*, Ein Diener seiner Herren. Werdegang des österreichischen Geheimagenten Gustav Zerffi (1820–1892) (Wien/Köln/Weimar 2002) 45f.
[22] Madeleine *Herren*, Internationale Organisationen im langen 19. Jahrhundert. Internationale Organisationen seit 1865: Eine Globalgeschichte der internationalen Ordnung. Kap. II (Darmstadt 2009) 15.
[23] Roland *Wenzlhuemer*, Editorial–Telecommunication and Globalization in the Nineteenth Century. In: Global Communication: Telecommunication and Global Flows of Information in the Late 19th and Early 20th Century. (Historical Social Research, Vol. 35, 2010) 7–18, hier 9.

entstand. Durch die Verwendung der Telegraphie für den Austausch von Kultur, Börsen– und Handelsinformationen sowie für diplomatische Dienste und auch für die imperiale Administration der Kolonien nahmen die Informationsflüsse quantitativ ein enormes Ausmaß an. Die Telegraphie wurde zum Motor der Globalisierung.[24]

Bei der telegraphischen Übermittlung einer Nachricht wurde deren Inhalt mindestens den beiden Telegraphenbeamten auf der Sende– und auf der Empfangsstation bekannt. Auch wenn alle Telegraphenbeamten auf allgemeine Verschwiegenheit vereidigt werden mussten, wollte weder eine private Person, ein Geschäftsmann oder eine Behörde, trotz gebührender Anerkennung des Briefgeheimnisses, offene Briefe versenden oder von den Telegraphisten schreiben lassen. Für die Benützung des Telegraphen wurde daher die Verschlüsselung des Textes gegenüber der Methoden, die für Inhalte in verschlossenen Briefen verwendet wurden, noch erweitert und verfeinert.[25]

Im Hauptkapitel, dem sechsten Kapitel, wird die Entwicklung der Chiffren–Schlüssel für die telegraphische Übertragung beschrieben. Der Forschungsstand ist in der wenigen vorhandenen Literatur zeitgenössischer Arbeiten einigermaßen aufgearbeitet. Hingegen konnte in den Archiven dazu nicht viel gefunden werden, da die Unterlagen immer dann vernichtet wurden, wenn Gefahr einer Revolution oder eines Krieges bestand. Auch wurden beim Militär Chiffren–Tabellen nach einer bestimmten Zeit protokollarisch verbrannt. Der Mangel an ausreichenden Beschreibungen in den Archivalien des Haus–, Hof– und Staatsarchives Wiens, Kriegs– und Verwaltungsarchives aus dem Untersuchungszeitraum konnte durch zeitgenössische Literatur aus der Österreichischen Nationalbibliothek annähernd ausgeglichen werden, um einen Eindruck der Entwicklung der Chiffren–Schlüssel zu vermitteln. Besonders für das Ende des Untersuchungszeitraumes, vom Beginn des 20. Jahrhunderts bis zum Ausbruch des ersten Weltkrieges, konnten einer Literatur–Neuerscheinung, herausgegeben vom Bundesminister für Landesverteidigung und Sport, viele Angaben zu den verwendeten Geräten und Chiffriermethoden entnommen werden.

Mittels der Telegraphie konnten nur Buchstaben und Zahlen übertragen werden. Frei erfundene Graphiken, wie sie von Karl dem Großen, Maria Stewart oder den Freimaurern verwendet wurden, wären bis zur Einführung der Bildtelegraphie ausgeschieden. Die erhöhte

[24] *Wenzlhuemer*, Telecommunication and Globalization, HSR, Vol. 35, 11.
[25] C. L. *Meissner*, Die Correspondenz in Chiffern für Regierungen, Ämter, Kaufleute und Privatiers (Braunschweig 1849) 6.

Gefahr, Telegraphenleitungen abzuhören, führte zu komplizierten und umfangreichen Chiffren–Diktionären, die aus einem grammatikalischen und einem lexikalischen Teil bestanden. Ferdinand Prantner aus der Ziffernsektion entwickelte 1869 ein Zusatzverfahren, die „Transkription". Durch ein zweites Chiffren–System wurden die Ziffern einer Depesche aus den im Diktionär enthaltenen Chiffren nach einer weiteren Tabelle, die sich nach Wochentagen geordnet täglich änderte, in andere Ziffern übersetzt. Diese Transponier–Methode wurde für höhere Aufgaben bei Militär am Beginn des Ersten Weltkrieges und darüber hinaus verwendet.[26]

Bei Einführung von Telegraph und Telephon in Österreich–Ungarn konnten die Arme und die Marine auf zivile und staatliche Einrichtungen zurückgreifen und in Zusammenarbeit mit der Industrie die zivilen Apparate und Techniken für den militärischen Gebrauch modifizieren. Ab dem Jahre 1902 erfolgten Erprobungen der drahtlosen Telegraphie und erst ab 1905 setzte die Ausrüstung der Truppe mit dieser neuesten Technik ein. Bei der Marine war die Notwendigkeit der Einführung der drahtlosen Übertragung von Nachrichten mittels Radio von großer Bedeutung und begann deshalb bereits um 1903. Weil alle wichtigen Heeresdienststellen innerhalb der Monarchie mit Telegraph oder Telephon erreichbar waren, wurde die sehr teure Ausrüstung der Armee mit Radiostationen nachrangig betrieben. Die österreichische Armee hatte jedoch einen Radio–Horchdienst (RHD) eingerichtet, der an der russischen und italienischen Front im Ersten Weltkrieg hervorragende Aufklärungsdienste leistete. Der RHD verfügte über keine eigene Truppe, sodass die Radiostationen der Armee für diese Dienste herangezogen wurden.[27]

Als Erkenntnis kann festgehalten werden, dass die Verschlüsselung von Nachrichten in der Geschichte immer eine wichtige Rolle gespielt hat, in der Forschung der Chiffriermethoden und chiffrierter Depeschen aber bisher nur wenig beachtet wurde und daher vielfältige Fragen für weitere Untersuchungen und Bearbeitungen offen bleiben. Auch wenn die Anzahl der Quellen bis zum Beginn des 20. Jahrhunderts gering ist, lohnen sich weitere Recherchen nicht nur in Bezug auf die verwendeten Methoden, sondern auch zur Erforschung des Inhaltes der geheimen Nachrichten, soweit sie als Original noch auffindbar sind, sowie deren politischen und militärischen Umsetzung und Auswirkungen.

[26] Österreichisches Staatarchiv/Kriegsarchiv, NFA HHK AK 4. Armee AK 70, Chiffrentabelle 8588.
[27] Johann *Prikowitsch*, Drahtlose Telegraphie in der k. (u.) k. Armee und Marine, Band 2 (Wien 2016) 1.

2 Frühe Methoden der Verschlüsselung

Der Wunsch und die Notwendigkeit, bestimmte Botschaften geheim zu halten, die nur der eigentliche Empfänger lesen kann, führte dazu, dass Staaten ihre eigenen Verschlüsselungsdienste einrichteten, die Codes für einen sicheren Nachrichtenverkehr entwickeln sollten. Gleichzeitig versuchten die gegnerischen Codebrecher, diese Codes in Schriftstücken zu entschlüsseln, um Geheimnisse zu erfahren. Die Geschichte der Geheimschriften, der Codes und Chiffren ist die Geschichte des Jahrhunderte lang währenden Kampfes zwischen Verschlüssler und Entschlüssler, ein geistiger Wettlauf, der dramatische Auswirkungen auf den Lauf der Geschichte hatte. Codes sind in die Geschichte eingewoben, sie haben Schlachten entschieden und den Tod gekrönter Häupter herbeigeführt. Beide Seiten, um Geheimhaltung beziehungsweise um deren Zerstörung bemüht, bedienten sich einer Reihe wissenschaftlicher Disziplinen und Verfahren, von der Mathematik zur Linguistik und von der Informatik bis zur Quantentheorie.[28]

Das Wort „Code“ bezeichnet einen besonderen Fall der Kommunikation. Dabei wird ein Wort durch ein anderes Wort, eine Zahl oder ein Symbol ersetzt. So besitzen etwa Geheimagenten einen Codenamen, also Tarnnamen an Stelle ihrer richtigen Namen. Auch kann der Satz „Angriff bei Morgengrauen“ durch das Codewort „Jupiter“ ersetzt werden. Wenn das Hauptquartier und der Kommandeur sich vorher abgesprochen haben, wird dem eigentlichen Empfänger die Bedeutung von „Jupiter“ klar sein, dem Gegner jedoch wird die Meldung unverständlich bleiben. Die Alternative zum Code ist die „Chiffre“; ein Verfahren, das auf tieferer Ebene ansetzt und Buchstaben statt ganze Wörter ersetzt. So kann jeder Buchstabe in einem Satz durch den nächsten Buchstaben im Alphabet ersetzt werden, A durch B, B durch C und so weiter.[29]

2.1 Geheimschriften seit der Antike bis zum Mittelalter

Die ersten Beschreibungen von Geheimschriften finden sich bereits bei Herodot, dem „Vater der Geschichtsschreibung“, wie ihn Cicero nannte. Herodot zufolge rettete die Kunst der Geheimschrift Griechenland vor der Eroberung durch Xerxes, den despotischen Führer der Perser. Als Xerxes begann, bei Persepolis eine neue Hauptstadt seines Königreiches zu

[28] *Singh*, Geheime Botschaften, 9f.
[29] *Singh*, Geheime Botschaften, 12f.

errichten, hielten sich Athen und Sparta im Gegensatz zu den anderen angrenzenden Staaten mit Geschenken zurück. Entschlossen, diese Überheblichkeit zu rächen, stellte Xerxes während fünf Jahren die größte Streitmacht zusammen und war 480 v. Chr. zu einem Überraschungsangriff bereit. Demaratos, einem verstoßenen Griechen, der in der persischen Stadt Susa lebte, war die Aufrüstung der Perser nicht entgangen und er beschloss, den Spartanern eine Nachricht zu schicken, um sie vor Xerxes‘ Invasion zu warnen. Von einer kleinen Schreibtafel schabte er das Wachs ab und schrieb auf das Holz der Tafel, was der König vorhatte. Darauf goss er wieder Wachs über die Schrift, damit die Wachen an den Straßen die leere Tafel durchließen. Man sagt, Kleomens‘ Tochter Gorgo, die Gemahlin des Leonidas, kam dahinter und ließ das Wachs abkratzen, damit man die Schrift auf dem Holz fände. Nach dieser Warnung begannen die Griechen sich zu bewaffnen. Xerxes hatte den entscheidenden Vorteil des Überraschungsangriffs verloren, und als die persische Flotte am 23. September 480 v. Chr. auf die Bucht von Salamis bei Athen zulief, spornten die Griechen die persischen Schiffe noch an, in die Bucht einzufahren. Die Griechen starteten einen erbitterten Angriff und zerstörten binnen eines Tages die gewaltige Streitmacht der Perser auf demütigende Weise.[30] Demaratos Verfahren der geheimen Nachrichtenübermittlung bestand darin, die Botschaft zu verbergen. Die Übermittlung geheimer Nachrichten, bei der die Botschaft verborgen wird, wurde später *Steganographie* bezeichnet.[31]

In den zwei Jahrtausenden seit Herodot wurden rund um den Globus mannigfaltige Spielarten der *Steganographie* eingesetzt. Die alten Chinesen schrieben Botschaften auf feine Seide, rollten sie zu Bällchen und tauchten sie in Wachs. Der Bote schluckte das Wachskügelchen. Im 15. Jahrhundert beschrieb der italienische Wissenschaftler Giovanni Porta, wie man eine Nachricht in einem hartgekochten Ei verbergen kann. Er schrieb die Botschaft mit einer farblosen Tinte, einer Unze Alaun in einem Becher mit Essig gelöst, auf die Eierschale. Die Lösung drang durch die poröse Schale und hinterließ eine Botschaft auf der Oberfläche des gehärteten Eiweißes, die erst nach Entfernung der Schale gelesen werden konnte. Dass sich die *Steganographie* so lange gehalten hat, zeigt, dass sie ein gewisses Maß an Sicherheit bot. Doch hat sie unter einer entscheidenden Schwäche gelitten: Wenn die Kleidung und das Gepäck des Boten durchsucht und die Botschaft gefunden wurde, trat der Inhalt der geheimen Mitteilung sofort zutage.[32] Es entstand daher gleichzeitig mit der *Steganographie* auch die *Kryptographie,* bei der nicht die Existenz der Botschaft zu verschleiern das Ziel war, sondern

[30] *Singh*, Geheime Botschaften, 18f.
[31] *Bauer*, Entzifferte Geheimnisse. 9.
[32] *Singh*, Geheime Botschaften, 20.

ihren Sinn mittels eines Verfahrens der Verschlüsselung zu verbergen beabsichtigte. Um eine Botschaft unverständlich zu machen, musste sie nach einem bestimmten Verfahren „verwürfelt“ werden, was zwischen dem Sender und dem Empfänger abgesprochen werden musste. Der Vorteil einer kryptographisch verschlüsselten Nachricht war, dass der Gegner, der sie abfing, nichts damit anfangen konnte. *Kryptographie* und *Steganographie* sind zwar unabhängige Disziplinen, aber es ist auch möglich, eine Nachricht sowohl zu verschlüsseln als auch zu verbergen, um ein hohes Maß an Sicherheit zu gewinnen.[33]

In der Kryptographie selbst werden zwei Verfahren angewendet, die *Transposition* und die *Substitution*. Bei der Transposition werden die Buchstaben einer Botschaft anders angeordnet, was ein Anagramm ergibt. Eine Form der Transposition ist das erste Kryptographie–Verfahren, die *Skydale*, wie sie im fünften Jahrhundert die Generäle der Spartaner verwendeten. Die *Skydale* ist ein Holzstab, um den ein Streifen Leder oder Pergament gewickelt wird. Der Sender schreibt die Nachricht der Länge des Stabes nach auf den Streifen und wickelt ihn dann ab. Der Streifen scheint nur eine sinnlose Aufreihung von Buchstaben zu enthalten. Der Bote übernahm den Streifen und trug ihn als Gürtel mit den Buchstaben auf der Innenseite. Um die Nachricht wieder herzustellen, wickelte der Empfänger den Lederstreifen um eine Skydale mit demselben Durchmesser, den der Sender benutzt hatte.[34]

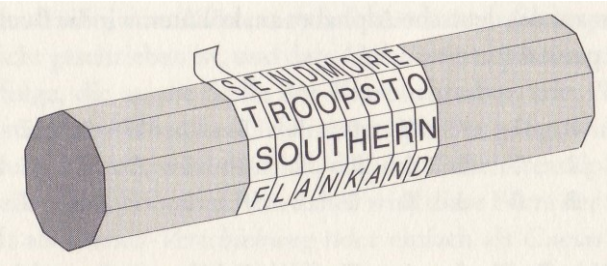


Abbildung 1: Wenn der Lederstreifen von der Skydale (Holzstab) des Absenders gelöst wird, scheint er mit einer willkürlichen Reihe von Buchstaben bedruckt; STSF…

Eine Alternative zur Transposition ist die *Substitution*, bei der jeder Buchstabe im Klartext durch einen anderen Buchstaben ersetzt wird. Diese Form der Verschlüsselung setzte Julius Caesar im „Gallischen Krieg“ ein. Caesar tauschte die Buchstaben des römischen Alphabets mit griechischen und machte damit die Botschaft für den Gegner unlesbar. Caesar benutzte so häufig Geheimschriften, dass Valerius Probus eine Abhandlung darüber schrieb, die leider nicht erhalten geblieben ist. Allerdings verdanken wir dem im zweiten Jahrhundert verfassten

[33] *Singh*, Geheime Botschaften,21.
[34] *Singh*, Geheime Botschaften, 23f.

„Caesarleben“ des Sueton die Beschreibung der von Caesar eingesetzten Substitutions–Chiffre. Der Kaiser ersetzte einfach jeden Buchstaben der Nachricht durch den Buchstaben, der drei Stellen weiter im Alphabet folgte (Abbildung 2). Diese Form der Substitution wird oft als *Caesar-Verschiebung* bezeichnet. Geheimschrift oder Chiffre wird das Ergebnis einer Substitution genannt, bei der jeder Buchstabe durch einen anderen Buchstaben ersetzt wird. Eine Caesar-Verschiebung ist mit einer Verschiebung zwischen einer und 25 Stellen möglich.[35]

Klartextalphabet:	a b c d e f g h i j k l m n o p q r s t u v w x y z
Geheimtextalphabet:	D E F G H I J K L M N O P Q R S T U V W X Y Z A B C
Im Klartext:	v e n i, v i d i, v i c i
Im Geheimtext:	YHQL, YLGL, YLFL

Abbildung 2: Die Caesar-Verschiebung, auf einen kurzen Text angewendet. Die ursprüngliche Botschaft, der Klartext, wird klein, und die verschlüsselte Botschaft, der Geheimtext, groß geschrieben.

Anstatt die Buchstaben des Klartextalphabetes einfach zufällig anzuordnen, wählt der Sender ein *Schlüsselwort* oder einen *Schlüsselsatz,* mit dem das Geheimtextalphabet verschoben wird. Wird zum Beispiel „JULIUS CAESAR“ als Schlüsselwort an den Beginn gesetzt, werden im ersten Schritt die Wortzwischenräume und die wiederholten Buchstaben weg gelassen (JULISCAER), wodurch das Geheimtextalphabet wie folgt aussehen würde:

Klartextalphabet:	a b c d e f g h i j k l m n o p q r s t u v w x y z
Geheimtextalphabet:	J U L I S C A E R T V W X Y Z B D F G H K M N O P Q

Dies hat den Vorteil, dass man sich das Schlüsselwort oder den Schlüsselsatz und damit das ganze Geheimalphabet leicht merken kann. Diese Verbindung von Einfachheit und Stärke ließ das Substitutionsverfahren im ersten Jahrtausend zur Königin der Verschlüsselungskunst werden.[36]

Ein berühmtes Beispiel des Substitutionsverfahrens sind die Geheimzeichen, die im neunten und zehnten Jahrhundert von keinem Geringeren als Karl dem Großen verwendet wurden (siehe Abbildung 3).[37]

Abbildung 3: Geheimzeichen Karls des Großen.

[35] *Singh*, Geheime Botschaften, 25f.
[36] *Singh*, Geheime Botschaften, 29.
[37] *Bauer*, Entzifferte Geheimnisse, 46.

Auch die Freimaurerchiffre (englisch auch *pigpen cipher*) fällt in diese Kategorie der Substitution und lautet in der moderneren Form: [38]

a b c d e f g h i j k l m n o p q r s t u v w x y z

Sie kann durch folgende Schemata in Erinnerung behalten werden:

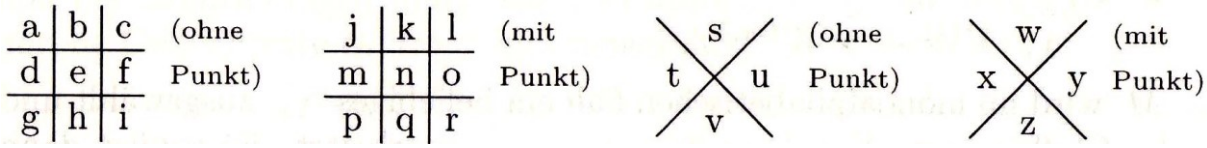


Abbildung 4: Freimaurerchiffre

Am Zarenhof wurde noch im Jahre 1728 eine heterogene Substitution mit einem bizzaren Geheimtextzeichenvorrat verwendet.[39]

2.2 Die monoalphabetische Verschlüsselung und die Statistik

In einer monoalphabetischen Chiffrierung wird jeder Buchstabe des Alphabets stets mit dem gleichen Geheimtext–Buchstaben chiffriert. Es konnten daher mit Hilfe der Statistik Gesetzmäßigkeiten in Texten ermittelt werden, die zur Entschlüsselung geheimer Nachrichten führten und damit die *Kryptoanalyse* zum Leben erweckten.

Die Erkenntnis dieser Gesetzmäßigkeiten ist arabischen „Kryptoanalytikern“ zu verdanken. Ein geordnetes Gemeinwesen der abbasidischen Kalifen war nur mit einer effizienten Verwaltung möglich, bei der man auch schon Verschlüsselungsverfahren anwandte. Nicht nur geheime Angelegenheiten der Obrigkeit unterlagen der Verschlüsselung, sondern auch die Beamten machten zum Schutz der Steuerunterlagen regelmäßig davon Gebrauch, um die Korruption einzudämmen. Allerdings waren die arabischen Gelehrten nicht nur in der Lage, Geheimschriften zu verwenden, sondern konnten deren Gebrauch auch wertlos machen. Sie erfanden die *Kryptoanalyse*, die Wissenschaft von der Entschlüsselung ohne Kenntnis des Schlüssels. Den arabischen Kryptoanalytikern gelang es, ein Verfahren zu entwickeln, mit dem sie die monoalphabethische Verschlüsselung, die mehrere Jahrhunderte lang als unlösbar gegolten hatte, aufzulösen, indem sie die Häufigkeit der Buchstaben in Texten entdeckten.[40]

[38] *Bauer*, Entzifferte Geheimnisse, 46.
[39] *Bauer*, Entzifferte Geheimnisse, 46.
[40] *Singh*, Geheime Botschaften, 30f.

Die Religionsgelehrten studierten in den theologischen Schulen in Basra, Kufa und Bagdad die Offenbarungen Mohammeds, wie sie im Koran standen. Die Theologen wollten die zeitliche Reihenfolge dieser Offenbarungen erkunden und taten dies, indem sie die Häufigkeit der einzelnen Wörter in den Schriften zählten. Es stand der Gedanke dahinter, dass bestimmte Wörter erst in jüngerer Zeit entstanden waren. Wenn eine Offenbarung eine höhere Zahl dieser seltenen Wörter enthielt, dann würde dies darauf hindeuten, dass sie chronologisch später einzuordnen waren. Die Gelehrten überprüften auch einzelne Buchstaben und entdeckten, dass die Buchstaben »a« und »l« im Arabischen am häufigsten vorkommen, während »j« zehnmal weniger oft verwendet wurde. Diese scheinbar harmlose Beobachtung führte zum ersten großen Durchbruch in der Kryptoanalyse. Die früheste bekannte Beschreibung dieser Technik stammt von einem Gelehrten des neunten Jahrhunderts mit dem Namen Abū Yūsūf Ya'qūb ibn Is-hāq ibn as-Sabbāh ibn 'omrān ibn Ismaīl al-Kindī († um 870). Seine bedeutenste Abhandlung, die erst 1987 im Istanbuler Süleiman–Osman–Archiv wieder entdeckt wurde, trägt den Titel „Abhandlung über die Entzifferung kryptographischer Botschaften".[41]

Das Verfahren von Al-Kindī soll anhand des deutschen Alphabets erläutert werden. Um die Häufigkeit des Vorkommens eines jeden Buchstabens im Alphabet festzustellen, müssen Texte in der Länge eines Buches untersucht werden. Im Deutschen kommen die Buchstaben, wie in jeder natürlichen Sprache, nicht gleich häufig vor. Im Deutschen ist das »e« der häufigste Buchstabe. Ihm folgt das »n«, dann das »i« und so weiter. Eine charakteristische Häufigkeit der Buchstaben ist in Tabelle 1 aufgelistet. Solche Tabellen werden durch Auszählen der Buchstaben in langen und verschiedenartigen Texten erstellt.[42]

Tabelle 1: Häufigkeitsverteilung der Buchstaben des deutschen Alphabets

Buchstabe	Häufigkeit	Buchstabe	Häufigkeit	Buchstabe	Häufigkeit
a	6,51 %	j	0,27 %	s	7,27 %
b	1,89 %	k	1,21 %	t	6,15 %
c	3,06 %	l	3,44 %	u	4,35 %
d	5,08 %	m	2,53 %	v	0,67 %
e	17,4 %	n	9,78 %	w	1,89 %
f	1,66 %	o	2,51 %	x	0,03 %
g	3,01 %	p	0,79 %	y	0,04 %
h	4,76 %	q	0,02 %	z	1,13 %
i	7,55 %	r	7,00 %		

[41] *Singh*, Geheime Botschaften, 32f.
[42] Albrecht *Beutelspacher*, Kryptologie. Eine Einführung in die Wissenschaft vom Verschlüsseln, Verbergen und Verheimlichen (3., behutsam verb. Aufl, Braunschweig 1993) 17.

Als nächstes wird der Geheimtext untersucht und die Häufigkeit jedes Buchstaben festgestellt. Ist der Buchstabe mit der größten Häufigkeit »N«, kann vermutet werden, dass »N« der dem Klartextbuchstaben »e« entsprechende Buchstabe ist. Und wenn der zweithäufigste Buchstabe im Geheimtext »R« ist, steht er wahrscheinlich für »n«, und so weiter. Man sollte aber alles was auf Statistik beruht, nicht vorbehaltslos anwenden. Insbesondere bei kurzen Texten kann die Suche nach dem häufigsten Buchstaben in eine Sackgasse führen. In einem weiteren Schritt werden daher die *Bigramme*, das heißt Paare aufeinanderfolgender Buchstaben, gezählt. Die häufigsten *Bigramme* der deutschen Sprache sind in der Tabelle 2 aufgelistet.[43]

Tabelle 2: Häufigkeiten der Bigramme in der deutschen Sprache

Buchstabenpaar	Häufigkeit	Buchstabenpaar	Häufigkeit
en	3,88 %	nd	1,99 %
er	3,75 %	ei	1,88 %
ch	2,75 %	ie	1,79 %
te	2,26 %	in	1,67 %
de	2,00 %	es	1,52 %

Damit lassen sich die nächsthäufigen Buchstaben isolieren. Das Paar »en« hat eine sehr große Häufigkeit, während alle anderen Kombinationen der kritischen Buchstaben mit »e« weniger oft vorkommen. Das Paar »ei« könnte eine Konkurrenz sein. Dieses kann man aber dadurch ausschalten, dass man das inverse Paar »ie« testet. Im letzten Schritt können die noch „weißen Felder“ im Text durch den intelligenten Entschlüssler erraten werden, um zu einem gut lesbaren Text zu gelangen. Mit diesem Vorgang kann gezeigt werden, dass mono–alphabetische Chiffrierungen bemerkenswert unsicher sind.

2.3 Kryptographische Verfahren vom 16. bis zum 18. Jahrhundert

Für die arabischen Gelehrten waren die Jahre von 800 bis 1200 n. Chr. eine Epoche großartiger intellektueller Leistungen. Während Al-Kindī die Kyptoanalyse erfand, kämpften die Europäer immer noch mit den grundlegenden Verfahren der Kryptographie. Die europäischen Institutionen, die das Studium der Geheimschriften vorantrieben, waren die Klöster. Die Mönche des Mittelalters fanden heraus, dass das Alte Testament absichtlich einige leicht durchschaubare kryptographische Elemente enthielt. Es wies Textstellen auf, die mit *Atbasch* verschlüsselt sind, einer traditionellen Form der hebräischen Substitutions–Geheimschrift. Bei diesem Verfahren wird festgestellt, wie weit jeder Buchstabe der

[43] *Beutelspacher*, Kryptologie, 25.

Geheimschrift vom Beginn des Alphabetes entfernt ist, dann ersetzt man ihn durch einen Buchstaben, der die gleiche Anzahl von Stellen vom letzten Buchstaben des Alphabets entfernt ist. Im Deutschen bedeutet das, dass »a«, eine Stelle vom Beginn des Alphabets, durch »Z«, eine Stelle vom Ende des Alphabets, ersetzt wird, »b« durch »Y« und so weiter.[44]

Im 14. Jahrhundert fand die Kryptographie zusehends Verbreitung. Dem englischen Schriftsteller und Dichter Geoffrey Chaucer (um 1342–1400) verdanken wir eines der berühmtesten Beispiele der frühen Verschlüsselung. Chaucer ersetzte Buchstaben aus dem Klartext durch Symbole, wie zum Beispiel den Buchstaben »b« durch das Symbol »δ«. Im 16. Jahrhundert war die europäische Kryptographie ein Dienst, der sich zunehmend verbreitete. Die wuchernden politischen Intrigen lieferten gute Gründe für die Geheimhaltung des Nachrichtenverkehrs. Die Höfe legten sich kryptographische Dienste zu und bald hatte jeder Botschafter seinen eigenen Geheimsekretär.[45]

Ein Versuch, die Sicherheit der monoalphabetischen Chiffrierung zu verbessern, war die Einführung von Codewörtern. Bisher wurde die Substitution auf ein Verfahren beschränkt, bei dem jeder Buchstabe durch einen anderen Buchstaben, einer Zahl oder einem Symbol ersetzt wurde. Allerdings ist es auch möglich, diese Methode auf höherer Ebene anzuwenden und jedes Wort durch ein anderes Wort oder Symbol zu ersetzen.

Kryptographen führten die Bezeichnung *Codierung* als Substitution auf der Ebene der Wörter oder Sätze, die *Chiffrierung* hingegen als Substitution auf Ebene der Buchstaben ein. Auf den ersten Blick bieten Codes größere Sicherheit als Chiffren, weil Wörter der Häufigkeitsanalyse weniger zugänglich waren als Buchstaben.[46]

Ein Beispiel, in dem Wörter durch Codes ersetzt werden:

Ermorden	= D,	General	= Σ,	sofort	= 08,
Erpressung	= P,	König	= Ω,	heute	= 73,
Gefangennahme	= J,	Minister	= Ψ,	heute Nacht	= 28,
beschützen	= Z,	Prinz	= θ,	morgen	= 43,

Klarbotschaft: Ermordet den König heute Nacht.
Codierte Botschaft: D – Ω – 28[47]

Im 16. Jahrhundert erkannten die Kryptographen die unvermeidlichen Schwächen der Codes und verwendeten überwiegend Chiffren und manchmal *Nomenklatoren*. Ein Nomenklator ist

[44] *Singh*, Geheime Botschaften, 43.
[45] *Singh*, Geheime Botschaften, 44.
[46] *Singh*, Geheime Botschaften, 47f.
[47] *Singh*, Geheime Botschaften, 47.

ein Verschlüsselungssystem, das aus zwei Teilen besteht; einem Geheimtextalphabet, mit dem der Großteil der Nachricht chiffriert wurde, sowie eine begrenzte Zahl von Codewörtern.

Der Fall der schottischen Königin Maria Stuart im 16. Jahrhundert ist ein berühmtes Beispiel für die Schwäche der Substitutionschiffren mit der 1:1 Beziehung zwischen verschlüsselten und Klartext–Buchstaben. Die Entschlüsselung der Chiffren, die Maria Stuart und ihre Mitverschwörer für ihre Geheimnachrichten benutzten, führte dazu, dass Maria Stuart des Hochverrats beschuldigt und schließlich hingerichtet wurde, weil man ihr die Absicht der Ermordung der Königin Elizabeth I. von England unterstellen konnte.

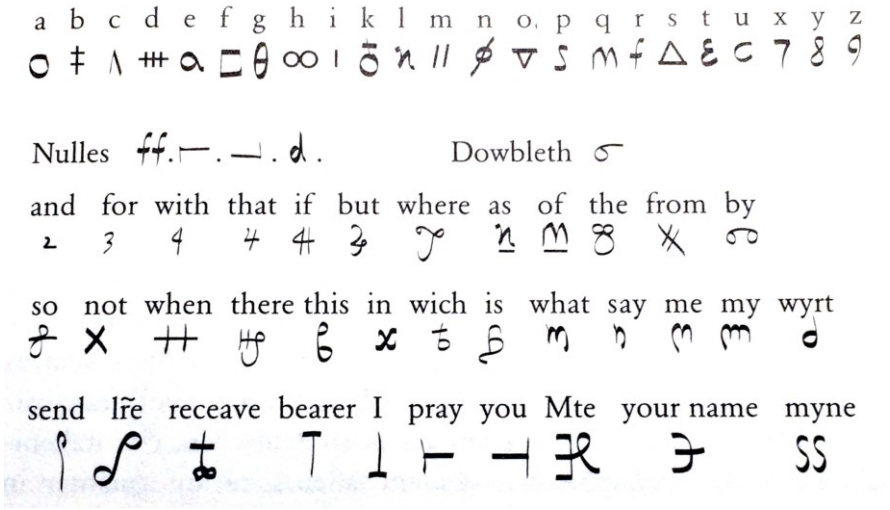


Abbildung 5: Maria Stuarts Nomenklator. Er besteht aus einem Geheimtextalphabet und Codewörtern.

Neben 23 Symbolen für die Buchstaben des Alphabets (ohne j, v und w) enthielt der Nomenklator auch 36 Symbole für ganze, häufig verwendete Wörter. Das setzte voraus, dass der Sender und der Empfänger ein Codebuch besaßen, den Schlüssel zu diesem Algorithmus. Die Entschlüsselung dieser Chiffre war durch die Anwendung eines Nomenklators schwieriger als die ihrer Vorgänger, aber nicht unmöglich; Maria Stuart wurde am 8. Februar 1587 in der großen Halle von Fotheringhay Castle enthauptet.[48]

Ein weiteres praktisches Beispiel einer Nomenklator–Liste, das von der Harrach Familie, einem Hochadels–Geschlecht aus dem südböhmischen und oberösterreichischen Uradel, in der zweiten Hälfte des 17. Jahrhunderts verwendet wurde, bestand ebenfalls aus einem Titelteil mit einem Geheimschriftalphabet und einem zweiten Teil mit einer Liste von

[48] *Singh*, Geheime Botschaften, 50–64.

Codewörtern. Das im Titelteil verwendete Alphabet veränderte die Reihenfolge der Buchstaben und begann mit den Selbstlauten A, E, I, O, U gefolgt von den Mitlauten B, C, D, F bis Z, jedoch ohne den Buchstaben J und V. Die Chiffrierung der 24 Buchstaben erfolgte bereits durch zwei Stellvertreter aus zweistelligen Zahlen, einer *polyalphabetischen Verschlüsselung*. In der Codierung von Wörtern, wurden Buchstabenpaare eingesetzt, die systematisch wieder die Selbstlaute a, e, i, o, u am Beginn beinhalteten.[49] Es handelte sich um eine wesentlich bessere Methode als die *monoalphabetische Verschlüsselung* und bot damit eine größere Sicherheit gegen die Häufigkeitsanalyse. Für die Chiffrierung und Dechiffrierung war allerdings eine Aufstellung von Codes erforderlich, die ein Codebuch mit mehreren Seiten ergeben konnten. Die Erstellung eines Codebuches war eine langwierige Angelegenheit und hatte verheerende Folgen, wenn es in die Hände des Gegners fiel.

Die zwei Zahlenreihen unter dem Klartextalphabet, gehen auf den Florentiner Mathematiker Leon Battista Alberti (1404–1472) zurück. Er schlug vor, anstatt des bis dahin im Substitutionsverfahren verwendeten einzigen Geheimtextalphabets zur Verschlüsselung der Botschaft, zwei oder mehr Geheimtextalphabete zu verwenden und während der Verschlüsselung zwischen ihnen hin und her zu springen.[50]

Titelteil der Nomenklator–Liste:

A	E	J	O	U	B	C	D	F	G	H	K	L	M	N	P	Q	R	S	T	W	X	Y	Z
21	22	23	24	25	26	27	28	41	42	43	44	45	46	47	48	61	62	63	64	65	66	67	68
31	32	33	34	35	36	37	38	51	52	53	54	55	56	57	58	71	72	73	74	75	76	77	78

Codes der Nomenklator–Liste:

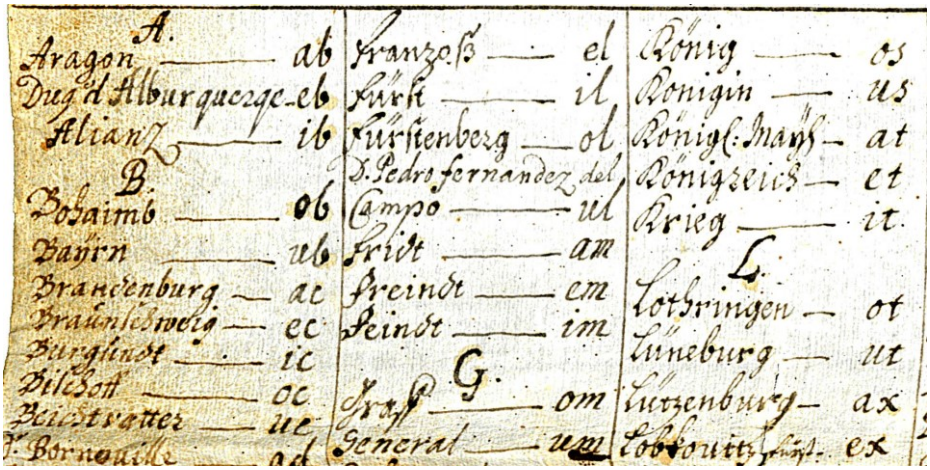


Abbildung 6: Auszug aus dem Nomenklator mit einigen Codes mit wiederkehrenden Selbstlauten a e i o u.[51]

[49] OeStA/AVA FA Harrach Fam. in spec 206.1 Chiffrenschlüssel, Allgemeines, Instructionen etc. 1658-1677.
[50] *Singh*, Geheime Botschaften, 66.
[51] OeStA/AVA FA Harrach Fam. in spec 206.1 Chiffrenschlüssel, Allgemeines, Instructionen etc. 1658-1677.

Im gegenständlichen Beispiel gibt es zwei mögliche Geheimtextalphabete bestehend aus Zahlen, und eine Botschaft wird verschlüsselt, indem die Zahlen abwechselnd verwendet werden. Um die Botschaft »Hallo« zu verschlüsseln, würde der erste Buchstabe mit der ersten Zahlenreihe chiffriert werden, so dass aus »H« die Zahl 43 wird. Der zweite Klarbuchstabe wird dann anhand der zweiten Zahlenreihe chiffriert, und aus »a« wird 31. Beim dritten Buchstaben wird wieder zur ersten und beim vierten wiederum zur zweiten Zahlenreihe zurückgegriffen. Der gesamte Geheimtext lautet 43-31-45-55-24. Der entscheidende Vorteil von Albertis Verfahren besteht darin, dass der gleiche Buchstabe im Klartext nicht immer mit dem gleichen Buchstaben oder der gleichen Zahl im Geheimtext chiffriert wird.[52]

Auf dieser ursprünglichen Idee von Alberti, dem der bedeutendste Durchbruch in der Kryptographie seit über einem Jahrtausend gelungen war, baute eine Gruppe von Gelehrten auf, von denen schließlich der französische Diplomat Blaise de Vigenère (1523–1596) um 1562 das mächtigste Chiffren–System entwickelte. Die Stärke der Vigenère–Verschlüsselung beruht darauf, dass sie nicht nur ein, sondern 26 verschiedene Geheimtextalphabete benutzt, um eine Botschaft zu verschlüsseln. Im ersten Schritt zeichnet man ein so genanntes Vigenère–Quadrat. Unter einem Klartextalphabet sind 26 Geheimtextalphabete aufgelistet, jedes davon um einen Buchstaben gegenüber dem vorhergehenden verschoben. So enthält Zeile 1 ein Geheimtextalphabet mit einer Caesar-Verschiebung von 1, Zeile 2 stellt ein Geheimtextalphabet mit einer Caesar-Verschiebung von 2 dar, und so weiter. Bei der Verschlüsselung einer Botschaft wird jeder Buchstabe anhand einer anderen Zeile des Vigenère–Quadrates verschlüsselt. Um die Botschaft zu entschlüsseln, musste der Empfänger wissen, welche Zeile des Vigenère-Quadrates für den jeweiligen Buchstaben benutzt wurde.[53]

Bei einer Verschlüsselung mit dem Schlüsselwort »LICHT« in Verbindung mit dem Vigenère–Quadrat wird das Schlüsselwort »LICHT« über die Nachricht geschrieben und so lange wiederholt, bis jeder Buchstabe der Nachricht mit einem Buchstaben des Schlüsselwortes »LICHT« verknüpft ist. Um den ersten Buchstaben zu verschlüsseln wird festgestellt, dass über ihm der Buchstabe »L« steht, der auf eine bestimmte Zeile des Vigenère-Quadrates verweist, die mit »L« beginnt. Die mit »L« beginnende Reihe 11 enthält das Geheimtextalphabet, das für den ersten Buchstaben benutzt wird, um den Stellvertreter des Klarbuchstabens zu finden. In gleicher Weise wird vorgegangen, um den zweiten und

[52] OeStA/AVA FA Harrach Fam. in spec 206.1 Chiffrenschlüssel, Allgemeines, Instructionen etc. 1658-1677.
[53] *Singh*, Geheime Botschaften, 68.

jeden weiteren Buchstaben der Botschaft zu verschlüsseln. Ein längeres Schlüsselwort würde noch mehr Zeilen in den Chiffren–Vorgang einbeziehen. [54]

Tabelle 3: Vigenère–Quadrat.

Klartext	a	b	c	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z
	0	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
Chiffretext 0	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
1	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A
2	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B
3	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C
4	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D
5	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E
6	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F
7	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G
8	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H
9	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I
10	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J
11	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K
12	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L
13	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M
14	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N
15	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O
16	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P
17	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q
18	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R
19	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S
20	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T
21	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U
22	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V
23	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W
24	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X
25	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y

Es würde nicht überraschen, wenn sich die Vigenère–Verschlüsselung wegen ihrer Stärke und ihrer großen Sicherheit rasch in den Geheimdienstkabinetten ganz Europas verbreitet hätte. Das Gegenteil war der Fall: Die Geheimdienstkabinette legten die Vigenère–Verschlüsselung schlicht beiseite.[55]

Die Kryptographen zögerten, die polyalphabethische Verschlüsselung einzusetzen, weil sie sehr kompliziert war. Vor allem der militärische Nachrichtenverkehr musste schnell und einfach von statten gehen. Wenn ein Befehl telephonisch erteilt wurde, wie in der Anekdote vom braven Soldat Schwejk erzählt, mit Maschinengewehren in eine bestimmte Richtung zu feuern, durfte keine Verzögerung durch die Übermittlung eintreten, um die Operation erfolgreich durchzuführen. Die Zeit spielte in einer Kampfhandlung eine entscheidende Rolle.

[54] *Singh*, Geheime Botschaften, 68–71.
[55] *Singh*, Geheime Botschaften, 73.

Eine diplomatische Vertretung, in der täglich Hunderte von Botschaften gesendet und empfangen wurden, musste den Nachrichtenverkehr ohne wesentliche Verzögerung durchführen. Die Kryptographen suchten daher nach einem Mittelweg, einer Verschlüsselung, die schwerer zu entschlüsseln war als die monoalphabetische aber in der Anwendung einfacher als die polyalphabetische war. Von verschiedenen Möglichkeiten bot sich die *homophone Verschlüsselung* an, bei der alle Geheimtextzeichen mit der gleichen Häufigkeit auftraten.[56] Die Chiffriervorschrift ordnete jedem Buchstaben nicht nur ein Zeichen, sondern mehrere Zeichen zu. Im folgenden Beispiel einer *homophonen Verschlüsselung* bestehen die Geheimtextzeichen aus 100 Ziffernpaare von 00 bis 99, deren Anzahl den Buchstaben entsprechend dem Prozentsatz nach Tabelle 1 auf Seite 15 zugeordnet wird. Die Anzahl der Geheimtextzeichen, die zu einem Klartextbuchstaben gehören, entsprechen damit der Häufigkeit dieses Buchstaben in einem Text. Wird eine Nachricht anhand des unten stehenden Geheimtextalphabets verschlüsselt, wird jede Zahl mit einer Häufigkeit von durchschnittlich einem Prozent vorkommen.[57]

Tabelle 4: Ersetzungstabelle für eine homophone Chiffre. Häufigkeit gemäß Tabelle 1, Seite 15.

a	b	c	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z
10	20	28	04	09	00	08	07	14	57	23	16	27	30	02	31	25	17	15	13	29	37	22	44	48	64
21	34	06	19	18	41	12	24	39			03	11	35	05			36	26	32	01					
52		80	70	33		97	47	46			84	49	43	82			51	45	90	58					
59			81	38			89	50					62				69	56	91						
71			87	40				65					63				74	61	95						
				42				76					67				78	73	98						
				53				88					68				83	96							
				54				94					72												
				55									77												
				60									79												
				66																					
				75																					
				85																					
				86																					
				92																					
				93																					
				99																					

Für den findigen Kryptoanalytiker war aber immer noch eine Analyse möglich, die auf der Beobachtung basiert, dass zwar die Häufigkeiten der Geheimtextzeichen, also der Ziffernpaare gleich sind, dass man aber aus der Betrachtung von Paaren im Geheimtext weitere Informationen gewinnen konnte. Dem Buchstaben »q« folgt im Deutschen immer der Buchstabe »u« (siehe auch Tabelle 2 auf Seite 16).[58]

[56] *Singh*, Geheime Botschaften, 74.
[57] *Beutelspacher*, Kryptologie, 36.
[58] *Beutelspacher*, Kryptologie, 36f.

2.4 Zweistellige und dreistellige Chiffren–Schlüssel

Ein mechanischer Chiffren–Schlüssel mit zwei– und dreistelligen Ziffern, in französischer Sprache, stammt aus der Regierungszeit Kaiser Franz‘s II./I., (1792–1835) und ist im Faszikel 22 des „Handarchiv Kaiser Franz“ im Haus–, Hof– und Staatsarchiv zu finden.[59] Von den verschiedenen Ausführungen der Zirkularscheiben mit den Bezeichnungen 10/100 und 50/500 soll das Modell 10 bzw. 100 ausführlich beschrieben werden, da dieses offensichtlich eine längere Zeit in Verwendung war, was an den Abnützungsspuren zu erkennen ist.

Die aus Messing gefertigte Zirkularscheibe hat einen Durchmesser von 123 mm und mit dem Handgriff eine Gesamtlänge von 228 mm. Eine Seite trägt am Ansatz des Handgriffes zur Identifizierung der Chiffren die Zahl 10 und die andere Seite 100. Jede Seite enthält sechs konzentrisch angeordnete kreisförmige Reihen mit je 24 korrespondierenden Segmenten, von denen die Kreise eins, drei, vier und sechs starr sind. Die Kreise zwei und vier sind beweglich und haben eine rote Beschriftung. So bilden je drei Kreise ein System aus einem Schieber in der Mitte, in denen im Uhrzeigersinn 24 Beschriftungen enthalten sind. Diese Beschriftungen bestehen aus zwei– oder dreistelligen Zahlen, einzelnen oder zweifachen Buchstaben. [60]

Abbildung 7: Vorderseite der Zirkularscheibe mit dem Chiffren–Schlüssels Nr. 10

Die sechs Ringe der Scheibe 10 zeigen im Uhrzeigersinn folgende Eintragungen:

11,112,12,113,13,114,14,115,15,116,16,117,17,118,18,119,19,121,122,123,124,125,126,127,
A, B, C, D, E, F, G, H, J, K, L, M, N, O, P, Q, R, S, T, V, W, X, Y, Z,
31,311,32,312,33,313,34,314,35,315,36,316,37,317,38,318,39,319,321,322,323,324,325,326,

que,des,pas,jay,les,est,qui,mes,par,cru,fin,car,ces,con,dir,bon,ong,sur,dit,mat,oui, ont, jeu, ils,
41, 51, 42, 52, 43, 53, 44, 54, 45, 55, 61, 62, 46, 56, 47, 57, 63, 64, 48, 58, 49, 59, 65, 66,
le, la, je, ne, on, me, si, ce, vo, us, du, ve, ni, sa, et, il, ba, ca, en, au, or, ou, ra, de,

[59] Österreichisches Staatsarchiv/Haus-, Hof- und Staatsarchiv, Handarchiv Kaiser Franz 22, Etui aus Leder.
[60] OeStA/HHStA Handarchiv Kaiser Franz 22, Etui aus Leder

Eine beigefügte Instruktion erklärt in französischer Sprache die Anwendung der beiden Scheiben zur Chiffrierung bzw. Dechiffrierung französischer Texte, die für diese Arbeit ins Deutsche übersetzt wurde:

„Anleitung zum Dechiffrieren und Chiffrieren gemäß beigefügter Chiffre

1.

Man muss vor die Zahl 10 oder 100 setzen, um anzuzeigen welche Seite der Scheibe man anwenden will.

2.

Dann ist der Buchstabe Z als Leitfaktor des Alphabets zu betrachten, das man jeweils anwenden möchte und unter eine der Ziffern des ersten Kreises des gewählten Alphabets setzt. Will man sich der Ziffern des ersten Kreises bedienen, muss man einen Strich über die Ziffer setzen, die man Z zugeordnet hat.

3.

Setzt man einen Strich unter die Ziffer, über der sich Z befindet, bedeutet dies, dass die Ziffern des dritten Kreises das Alphabet bestimmen, das man verwendet.

4.

Man kann beliebig oft die Platzierung des Buchstabens ändern, was automatisch die Ziffernkombination und alphabetische Zuordnung ändert, aber um Verwirrung zu vermeiden muss man darauf achten, dass man Änderungen der Verschlüsselung erst nach Abschluss einer Wort- oder Textverschlüsselung vornimmt.

5.

Man muss auch darauf achten, dass man vor einer solchen Änderung des Buchstabens Z vorher ein deutliches Zeichen wie Θ Δ H # setzt und dann die Ziffer, unter die man das Z setzt, mit einem Unter- oder Oberstrich markiert, um, wie es im Artikel 2 und 3 beschrieben ist, den ersten oder dritten Kreis zu definieren, der die angewendete Chiffrierung beinhaltet.

6.

Aber wenn man nach reichlicher Anwendung einer Seite der Scheibe auf die andere wechseln möchte, um die Dechiffrierung zu erschweren, muss man darauf achten, dass ein Seitenwechsel immer mit der Zahl 10 oder 100 angezeigt wird.

7.

Will man Wörter, Silben oder Artikel verwenden, die sich auf beiden Seiten der Scheibe befinden, muss man jeweils eine der Ziffern aus dem fünften Kreis platzieren, die als Fixschlüssel für alle anderen dient.

8.

Auf der Scheibe 100 muss man ebenfalls jeweils über die Silbe ju eine der Ziffern des fünften Kreises als Schlüssel im Sinne des Artikels 7 setzen.

9.

Bezüglich Scheibe 10 ist Folgendes zu beachten. Will man Silben, Wörter oder Artikel aus dem 4. Kreis, muss man einen Strich über der verwendeten Silbe anbringen, für Silben aus dem 6. Kreis jeweils darunter. Somit kann man Elemente aus dem 4. und 6. Kreis verwenden ohne den Chiffrierschlüssel zu ändern.

10.

In analoger Weise ist auf Scheibe 100 mit der Zahl über der Silbe ju zu verfahren, die als Chiffrierschlüssel mit Unterstrich oder Überstrich Silben aus dem 4. oder 6. Kreis bezeichnet.

11.

Die Ziffer, mit der man Wörter, Silben und Artikel aus dem 4. oder 6. Kreis von einer der beiden Seiten der Scheibe chiffriert, muss immer nach jener Zahl angeführt werden, die am Beginn des verwendeten Alphabets steht.

Es steht auch frei, die Ziffer (Chiffre) des ersten Kreises zu ändern und durch eine zu ersetzen. die man früher zur Chiffrierung verwendet hat. Weil man z.B. die Scheibe 10

und die Ziffern des ersten Kreises verwenden will oder auch Wörter, Silben und Artikel aus dem 4. oder 6. Kreis. Dabei ist darauf zu achten, am Beginn des zu chiffrierenden Textes zuerst die Zahl 10 und dann die jeweilige Ziffer des ersten Kreises anzuführen, unter den man den Buchstaben Z setzt. Diese Ziffer ist mit einem Überstrich zu markieren, um anzudeuten, dass man Ziffern aus dem ersten Kreis anwendet (bis dass man eine Änderung durch irgendein Zeichen ankündigt) und man setzt unmittelbar nach der entsprechenden Ziffer des 5. Kreises, die man über die Silbe or gesetzt hat. In gleicher Weise ist zu verfahren, wenn man sich der Scheibe 100 bedienen will. Sei es vom Anfang an oder als Wechsel des Chiffriercodes.

Zur Erleichterung des Dechiffriervorgangs sei darauf hingewiesen, dass auf der Scheibe 10 jede Ziffer/Zahl des 1. Kreises mit 1, im 3. Kreis mit 3 beginnt und im 5. Kreis mit 41 beginnt und mit 66 endet.
Auf Scheibe 100 beginnen die Zahlen des ersten Kreises mit 2, jene des 3. Kreises mit 4 und 5. Der 5. Kreis enthält die Zahlen von 71 bis 96.“[61]

„Als Beispiel des Zirkular-Verfahrens, wie man Ziffern Texte chiffriert, wähle man den Code der Scheibe 10 und stelle über den Buchstaben Z die Zahl 112, die sich im ersten Kreis befindet und markiere einen Strich darüber, um anzudeuten, dass die Buchstaben des Alphabets im ersten Kreis angeführten Zahlen entsprechen. Zum Transkribieren der Wörter, Silben und Artikel, die im vierten oder sechsten Kreis enthalten sind, stelle man die Schlüsselziffer 51 über das Wort or, fixiere es und beginne so:

10·$\overline{112}$ 51·12·11·12·18·124·125·18·19·14·125·122·14·115·17·14·13· -
116·16·12·46·$\overline{43}$·56 47 118·12·125·14·112·114·16·124·

Ich tausche die erste Leitziffer durch dieses Zeichen Δ: Die Leitzahl ist 44
Δ ·121·44·321·39·321·34·37·317·34·35·325·317·
36·325·326·33·325·323·311·32·321·64 $\overline{55}$ 317·314·317·316·
313·321·317·325·319·324·325·37·

Und um den gleichen Text mit der Scheibe Nr. 100 zu chiffrieren erfolgt die Ankündigung mit dem Zeichen Θ: 71 ist über die Silbe ju zu setzen

Θ 100·$\overline{29}$ 71·21·229·25·217·
228·25·$\overline{76}$·88 223·214·212·222·213·224·21·222·212·26·228·
212·228·215·228·227·82 228·212·29·84·217·“[62]

Eine Dechiffrierung der beiden ersten Zeilen auf dieser Seite ergibt, nachdem auf Scheibe 10 der Leitbuchstabe »Z« unter die Zahl »112« und die Schlüsselziffer »51« über das Wort »or« gestellt wurde:

12·11·12·18·124·125·18·19·14·125·122·14·115·17·14·13· -
a y a n t u n p e u r e f l e c

116·16·12·46·$\overline{43}$·56 47 ·118·12·125·14·112·114·16·124·
h i a ce que vo us m a u e z d i t

[61] OeStA/HHStA, Handarchiv Kaiser Franz 22, Mêthode instructive pour écrire et lire selon le chiffre ci joint. Ins Deutsche übersetzt von Fritz Mairleitner.
[62] OeStA/HHStA Handarchiv Kaiser Franz 22, Preuve de la manière dont on opère avec le chiffre. Ins Deutsche übersetzt von Fritz Mairleitner.

In Wörter zusammengesetzt: Ayant un peu réfléchi à ce que vous m‘avez dit.
Übersetzt: Ich habe ein wenig darüber nachgedacht, was Sie mir gesagt haben.

Anstelle des mechanischen Chiffren–Schlüssels konnte, je nach Verfügbarkeit, auch eine 16 seitige Tabelle des französischen Schlüssels verwendet werden, von der die erste Seite in Abbildung 8 zu sehen ist. Im Zeilenblock 2, bestehend aus 3 Zeilen, ist auf dieser Abbildung die Anordnung mit dem Leitbuchstaben Z unter 112 enthalten, die für die beschriebene Dechiffrierung verwendet wurde.

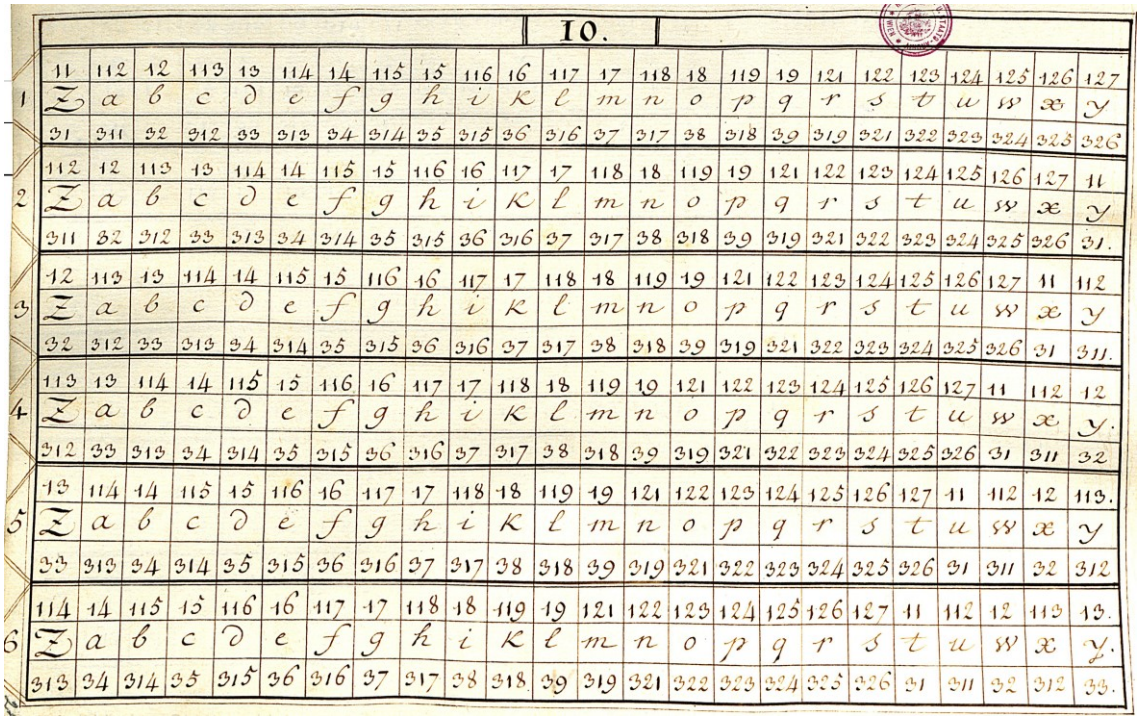


Abbildung 8: Tabelle des mechanischen Chiffren–Schlüssel 10. [63]

Auf dieser Tabellenseite 10 sind die ersten sechs Stellungen des Buchstaben Z unter den Zahlen 11, 112, 12, 113, 13 und 114 dargestellt. Mit dem Buchstabe Z als Leitfaktor des Alphabets ergeben sich 24 Kombinationen mit den Zahlen auf dem äußeren und weiter 24 Kombinationen mit den Zahlen des inneren Ringes. Im Gegensatz zur Papierform des Chiffren–Schlüssels konnte die Zirkularscheibe bequem im Reisegepäck mitgeführt werden und erlaubte eine schnellere Durchführung einer Verschlüsselung als die Benützung der Tabellen auf Papierbögen. Die Methode selbst ist mit der von Vigenère entwickelten Methode vergleichbar, weil die Chiffren beliebig oft gewechselt werden konnten, dafür aber keine

[63] OeStA/HHStA Handarchiv Kaiser Franz 22, Mappe 1-10.

Codewörter verwendeten. Zirkularscheiben ähnlicher Bauart, aber auch Linear–Schuber, sind am Beginn und während des Ersten Weltkrieges wieder in Verwendung.

Nach dem Wiener Kongress, einer Hochsaison für den geheimen Dechiffrierdienst, wurden viele Menschen misstrauisch und vorsichtiger. Diplomaten und Geschäftsleute verschlüsselten mit der Post beförderte Briefe nicht mehr mit den üblichen Chiffren, sondern benützten raffiniertere Methoden. Man schrieb die Chiffren mit sympathetischer Tinte zwischen unbedeutenden Textzeilen, verwendete verstellte Namen oder entstellte Sprachen; eine Methode, die den Beamten der Ziffernkanzlei kaum große Schwierigkeiten bereitete.[64]

2.5 Vierstellige Chiffren–Schlüssel

Ein neueres Verfahren, welches ebenfalls in französischer Sprache, aber mit vierstelligen Ziffern entwickelt wurde, wurde für die Korrespondenz des Militärs mit 10. Juni 1812 erlassen. Die Schlüsseltabelle ist in einem handlichen Format mit den Abmessungen von 34 cm Höhe und 20 cm Breite, eng beschrieben ausgeführt und durch einen Kartonumschlag geschützt. Die einzelnen Buchstaben des Alphabetes sowie Silben aus zwei oder mehreren Buchstaben und ganze Wörter wurden alle ausschließlich mit vier–stelligen Zahlen chiffriert, wobei Zahlen ab 1000 bis 8000 Verwendung fanden. Für häufiger vorkommende Buchstaben oder Bigramme wurden mehrere vier–stellige Zahlen festgelegt; wie z.B. für »a« vier Zahlen, für »e« fünf Zahlen, für »et« vier Zahlen, für »er« vier Zahlen, für »es« vier Zahlen, etc. Zwischen jeder vierstelligen Zahl wurde jeweils eine einstellige Zahl „nonvaleur“ ohne Bedeutung und fallweise eine zwei– oder drei–stellige Zahl als „insignifiant“, ebenfalls ohne Bedeutung, eingefügt. Das folgende Beispiel soll das beschriebene Verfahren näher darstellen:[65]

Klartext: „Jl faut de l’exactitude dans l’emploi de tout chiffre“
Verschlüsselter Text:
71332450120945110137886863318645682743
84686355975048142951719374738059895041 2

Auflösung: (non = nonvaleur, ins = insignifiant)
7 1332 4 5012 0 9451 1 0137 8 8686 3 3186 4 5682 7 43
non Jl faut non de non ins non ins non l’ non exactitude non dans non ins

8 4686 3 5597 5 0481 4 2951 7 1937 4 7380 5 9895 0 412
non l’ non employ non ins non de non tout non chiffre non ins non ins

[64] *Hubatschke*, Ferdinand Prantner, Buch 5, Diss., 1250.
[65] OeStA/HHStA StK Interiora 17 (alt 24), Chiffrenschlüssel, Mappe: Anonyme Schlüssel K. Franz II. (1792–1835), Chiffrant pour la Correspondance Militaire remis en 1812. fol 194.

Der verschlüsselte Text wurde in einer Reihe von Zahlen ohne Punkte dazwischen geschrieben und enthielt auffallend viele Ziffern ohne Bedeutung.[66]

Das Ziffernkabinett bildete in der Staatskanzlei einen eigenen Amtskörper und war wie eine politische Registratur, die im linken Flügel des Staatskanzleigebäudes auf dem Ballhausplatz im ersten Stock untergebracht war und mit der Geheimen Ziffernkanzlei in der Stallburg nur in loser Verbindung stand. Es hatte die von der Ziffernkanzlei entworfenen Ziffernschlüssel zu verwenden und zu verwahren. In einem angrenzenden, kleinen Zimmer wurden die Diplomaten vor ihrer Abreise in die ausländische Mission im Chiffrieren und Dechiffrieren geschult. Der Offizial der Geheimen Ziffernkanzlei, Wenzel Löschner, wurde bei der Neuorganisierung des Ziffernkabinetts 1816 als Berater herbeigezogen. Er schlug vor, Akzente und Apostrophe nicht zu chiffrieren, am Ende eines Satzes keine Erranten zu setzen sowie den Beginn und das Ende einer Depesche schwieriger zu chiffrieren.[67]

Bei dem folgenden Beispiel wird stellvertretend für mehrere dieser Art, ein deutscher Ziffernschlüssel beschrieben, der sich letztlich aus drei Tabellen mit unterschiedlichen Ziffernschlüssel zusammensetzt. Dieser befindet sich im Faszikel 20 (alt 27) des Bestandes „Chiffren–Schlüssel“ innerhalb der „Interiora“ der Staatskanzlei im Haus–, Hof– und Staatsarchiv unter anderen, ähnlich aufgebauten Chiffren–Schlüssel, die weiter im Faszikel 21 gelagert sind. Diese Tabellen bestehen aus jeweils zwei Doppelbögen mit einer Größe von ca. 75 cm Breite und 55 cm Höhe, sind ohne Datum und ohne Nummerierung und dürften in sich ständig ändernder Form bis 1835 Verwendung gefunden haben. Hervorzuheben ist, dass dieser Ziffernschlüssel durchgehend aus vierstelligen Zahlen ohne Sonderzeichen besteht, ohne Interpunktion läuft und die Erranten nicht am Ende eines Satzes eingesetzt sind. Jedes enthaltene Wort, jede Silbe und jeder Buchstabe kann neun Mal abgeändert werden und eine Zahl, die zehnte, stellt einen „Erranten“ dar, der öfters einzuschalten und ohne Bedeutung ist. Substantiva konnten höchstens drei Mal eingesetzt werden, mit veränderter Zahl jedoch öfters. Es ist anzunehmen, dass diese Chiffren–Schlüssel von der Geheimen Ziffernkanzlei entwickelt wurden.[68]

Die Beschreibung dieses Ziffern–Schlüssels mit der Anleitung über die Verwendung der ersten Tabelle wird hier eingefügt. Als Überschrift wird der Buchstabe „O“ verwendet.

[66] OeStA/HHStA StK Interiora 17 (alt 24), Chiffrenschlüssel, Mappe: Anonyme Schlüssel K. Franz II. (1792–1835), Chiffrant pour la Correspondance Militaire remis en 1812. fol 194.
[67] *Hubatschke*, Ferdinand Prantner, Buch 5, Diss., 1259f.
[68] OeStA/HHStA StK Interiora 20 (alt 27) und 21, Chiffrenschlüssel, Mappe Varia.

„O

1. Gegenwertiger Ziffer-Schlüssel lautet durchgehend auf vier Zahlen ohne Interpunktion.
2. Jedes darinnen enthaltene Wort, Silbe und Buchstaben können 9 mal abgeändert werden; nämlich hier haben jede ihre decine, davon eine Zahl einen Erranten gewidmet ist.
3. Diese Erranten müssen öfter eingeschaltet werden.
4. Auch können mit guten Vorbedacht zu Beschwerung des Ziffers die Haupt-, Nenn- und Eigen-Worte zwei bis höchstens drei Mal angesetzt werden, jedoch mit ihren veränderten Zahlen. Wie aus dem folgenden Exempel zu ersehen ist.

55056184047137387879257578909077901937092320232783953
27562754988263556351091189841897189090895727573774666
60000926583547694315

5505 6184 0471 3738 7879 2575 7890 9077 9019 3709 2320 2327 8953
err: Man hält hier da- für das die err: heuerige campagne ---- dem

2756 2754 9882 6355 6351 0911 8984 1897 1890 9089 5727 5737 7466
Kriege ---- zwischen Rußland ---- und der Pforte ---- die err: Ent- sche-

6000 0926 5835 4769 4315
id- ung err: geben wird“[69]

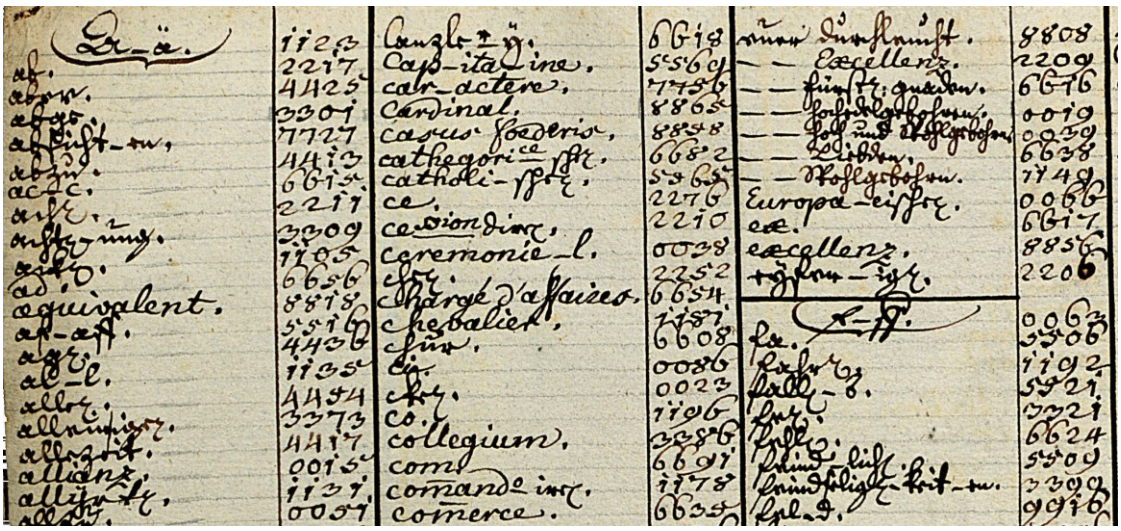


Abbildung 9: Ausschnitt aus der ersten Zifferntabelle über die ersten 20 Zeilen der ersten drei Rubriken

Zur Erschwerung einer unautorisierten Dechiffrierung wurde der ersten Zifferntabelle eine zweite und eine dritte Zifferntabelle hinzugefügt, deren gemeinsame Verwendung in einer „Weisung zum Ziffer Schlüssel“ geregelt wurde. Die Chiffrierung hatte ohne „Interpunktion“ zu erfolgen und ein Tabellenwechsel musste durch einen „indicans numerus Tabellam“ angekündigt werden. In allen drei Tabellen konnte von der vierstelligen Zahl willkürlich die zweite Zahl weggelassen werden (siehe Abbildung 9: aus 2217 für »ab« wird 217), womit sich irreführende dreistellige Zahlen ergaben, die eine Dechiffrierung ohne Chiffren–Schlüssel erschweren sollte. Für eine Dechiffrierung wurde die zweite Zahl als eine

[69] OeStA/HHStA StK Interiora 20 (alt 27), Chiffrenschlüssel, Mappe Varia, fol 10.

Wiederholung der ersten Zahl eingefügt, womit wieder die vierstellige Zahl aus der entsprechenden Chiffren–Tabelle entstand.[70]

Während der ersten Jahrzehnte des 19. Jahrhunderts wurden von der Geheimen Ziffernkanzlei nur einfache Ziffernschlüssel entwickelt, aber auch nur einfache Verschlüsselungen aufgelöst. Metternich setzte für den Entwurf neuer, technisch ausgereifter Ziffern–Schlüssel für die Korrespondenz mit den Gesandtschaften im Ausland, die absolute Sicherheit gegen fremde Auflösung bieten sollten, einen hohen Preis aus. Die beiden Subdirektoren Dollinger und Zaremba waren der Ansicht, dass diese Bedingung durch „Tabletten" mit ausgeschnittenen Räumen, in welche die Ziffer einzutragen war, erreicht werden könnte. Der Entwurf wurde von Zaremba verfasst, während die mechanische Ausarbeitung den drei Amtsdienern der Ziffernkanzlei Bix, Goetzinger und Westermayer übertragen wurde. Am 14. Jänner 1835 erreichte der Direktor Eichenfeld eine Remuneration von je 50 Gulden für die drei verlässlichen Amtsdiener, da innerhalb kurzer Zeit 16 Exemplare anzufertigen waren.[71] „Tabletten", Tabellen oder eine Beschreibung dieses Entwurfes konnten in den Archiven nicht ausfindig gemacht werden.

[70] OeStA/HHStA StK Interiora 20 (alt 27), Chiffrenschlüssel, Mappe Varia, fol 25.
[71] *Hubatschke*, Ferdinand Prantner, Buch 5, Diss., 1293.

3 Chiffrierung und Dechiffrierung im Hause Habsburg

Hinter diesem Titel verbirgt sich die über Jahrhunderte lang geübte Spionage im Staatsinteresse. So alt wie die Sitte des Briefschreibens ist auch die Klage über eine unbefugte Öffnung von Briefen, eine Verletzung des von jeher als ein Grundrecht geltenden Briefgeheimnisses. Das Recht der Unverletzlichkeit des Eigentums ist bezüglich des geschriebenen Wortes schon im Altertum offensichtlich nicht ernst genommen worden. Demgemäß hat man die Chiffrierkunst bereits im Altertum gekannt und geübt. Eine moralisch bedeutsame Dimension erlangte die Wahrung des Briefgeheimnisses mit der Einrichtung der Post im eigentlichen Sinne, weil es eine Verletzung des öffentlichen Vertrauens bedeuten musste. Trotzdem hat man aus Gründen der Staatsraison in beinahe allen Staaten die geheime Einsichtnahme in fremde Korrespondenz gehandhabt. Um hinter die Geheimnisse fremder Mächte, feindlicher, aber auch befreundeter, zu gelangen, ließ die Diplomatie Europas schon vor der Zeit der Reformation ganz allgemein Korrespondenzen abfangen und Dokumente öffnen. In den deutschen Gebieten kam es bereits im Laufe des 16. Jahrhunderts zur Bildung so genannter „Schwarzer Kabinette“, bei denen es sich um planmäßig organisierte, unter strenger Geheimhaltung funktionierender Einrichtungen handelte, die es der Staatsgewalt ermöglichte, in die der Post zur Beförderung anvertrauten verschlossenen Korrespondenzen unbefugt Einblick zu nehmen.[72]

Für die mit der Durchführung der geheimen Briefmanipulation betrauten Dienststellen kam in Frankreich schon früh der Ausdruck „Cabinet Noir“ auf, was man dann als „Schwarzes Kabinett“ übersetzt in dieser Form auch im deutschen Sprachgebiet gebrauchte. Diese Bezeichnung blieb bis Ende des 19. Jahrhunderts in Gebrauch. In Österreich verwendete man dafür häufig den Ausdruck „Loge“, die dort Bediensteten „Logisten“. Für die geheim angefertigten Briefabschriften war in der österreichischen Amtssprache die Bezeichnung „Interzepte“ üblich. Bis zu den großen europäischen Revolutionen um die Mitte des 19. Jahrhunderts traten diese Institute nie aus dem Halbdunkel heraus. Erst gegen Ende des 19. Jahrhunderts gewann die historische Forschung Zugang zu jener Gattung von Archivalien, deren Existenz man bis dahin streng geheim gehalten hatte.[73]

[72] Harald *Hubatschke*, Zur historischen und juristischen Problematik der „Schwarzen Kabinette“. In: Mitteilungen des Instituts für Österreichische Geschichtsforschung, Band 83, Heft 3 (1975) 355–364, hier 355.
[73] *Hubatschke*, Zur Problematik der „Schwarzen Kabinette“. MIÖG, Bd. 83, H.3, 356f.

In der Verfeinerung der Methoden des „Interzipierens“ hatte zunächst Frankreich deutlich die Spitze gehalten. Bereits seit 1464 besaß Frankreich eine „politische“ Postanstalt, und seither hat man die Briefspionage geradezu zur Spezialität entwickelt. Die Staatspost mit ihrer zentralistischen Leitung eignete sich für die geheime Briefüberwachung wesentlich besser als die Lehenspost Mitteleuropas. Zur Bewältigung der außerordentlichen Zunahme der französischen Briefspionage im Spanischen Erbfolgekrieg organisierte Frankreich in Spanien, in den Niederlanden und in Norditalien ein Netz von „Schwarzen Kabinetten“. Die Auswirkungen dieser Aktivitäten blieben Prinz Eugen und Karl VI. nicht verborgen, die den Wert einer solchen Einrichtung kennen lernten und ihrerseits begannen, eine Briefüberwachung im Umfang nach französischem Muster in Österreich einzurichten. Die seit Ludwig XIV. in bester Tradition bewährte Einrichtung der Briefüberwachung wurde von Napoleon I. weiter ausgestaltet und verwendet.[74]

3.1 Die Wiener Briefüberwachung

Die österreichische geheime Briefüberwachung reicht in ihren Anfängen zumindest bis zum Beginn des 16. Jahrhunderts zurück. Schon Maximilian I. soll sie angewendet haben, um von den Übergriffen der Flamen und Mailänder Kenntnis zu erlangen. Karl V. erfuhr durch die Briefüberwachung sehr oft von Verabredungen protestantischer Stände und Philipp, Landgraf von Hessen, der nichts davon ahnte, hatte seinen Briefwechsel mit den Reichsständen, worin er den Kaiser beschimpfte, schwer zu büßen. General Lazarus Schwendi, der am Hof Rudolf II. in großer Gunst stand, beklagte sich, dass der Postmeister seine Briefe behielt und aufbrach.[75]

Im Dreißigjährigen Krieg wurde die geheime Briefüberwachung allmählich zum Selbstzweck der Post. Die Erklärung des Postwesens zum Reichsregal und die Übertragung des Amts des Generalpostmeisters im Jahre 1615 zum „Erbmannslehen“ an die Taxis war ein Vorgang von großer politischer Tragweite. Die Familie der Taxis war Betreiber der Kaiserlichen Reichspost, wurde mit kaiserlicher Genehmigung 1650 in *Thurn und Taxis* umbenannt und stellte bis zur Auflösung der Heiligen Römischen Reiches den Generalpostmeister. Die habsburgischen Kaiser hatten in den österreichischen Ländern ihre eigene Post eingerichtet und hätten keinen Grund gehabt, die „Postgerechtsame“ der deutschen Fürsten zu beschneiden. Die Überwachung des Briefverkehrs durch „Schwarze Kabinette“ war aber in

[74] *Hubatschke*, Zur Problematik der „Schwarzen Kabinette“. MIÖG, Bd. 83, H.3, 357.
[75] *Stix*, Organisation der Wiener Geheimen Ziffernkanzlei. MIÖG, Bd. 51, 131.

den außerösterreichischen Gebieten nur durch die Schaffung einer Reichspost und die entsprechende Bereitwilligkeit der Taxis möglich. Auch Leopold I. hatte die Postüberwachung bereits in ähnlich systematischer und wirkungsvoller Weise benützt wie sein Rivale Ludwig XIV.[76]

Die Einbeziehung der Reichspost in das Kontrollsystem Karls VI. war eine absolute Notwendigkeit für die Politik des Kaisers. Etwaige moralische Bedenken traten zugunsten der absolutistischen Staatsraison völlig in den Hintergrund. Der führende Postpolitiker des 18. Jahrhunderts, Michael Florence von Lilien (1696–1776), hatte die Reichspost und die Taxis nach einigen Rückschlägen endgültig mit den Habsburgern verbunden und den geheimen Briefdienst zu einer der wichtigsten Stützen österreichischer Hausmachtspolitik ausgebaut. Die Zentralisierung der österreichischen Post hatte nach dem Regierungsantritt Maria Theresias vor allem den Zweck der Neuorganisation des geheimen Dienstes. Dank der organisatorischen Tätigkeit Liliens konnte der Briefwechsel des Königs von Preußen mit seinem Wiener Gesandten ebenso wie die Depeschen des sächsischen Gesandten in München, Mannheim und Paris, sogar die Berichte der venezianischen Gesandten aus London Maria Theresia vorgelegt werden. Die von Lilien geknüpften Beziehungen Österreichs zur Reichspost erwiesen sich so haltbar, dass sie der Niedergang des Heiligen Römischen Reiches nicht aufzulösen imstande war. Erst der Bruderkrieg von 1866 hat ihnen ein Ende bereitet.[77]

Die Korrespondenzen, die ihren Weg nicht über Wien nahmen, wurden mit Hilfe von Postlogen in anderen Städten kopiert und an die Zentralanstalt in Wien geliefert. Ihre Einrichtung, Organisation und Arbeitsweise wurde von Wien aus gesteuert. Auch die Auswahl und Ausbildung der Logisten lag in der Zuständigkeit des Direktors des Wiener Instituts, in dessen Anwesenheit deren Amtseid abzulegen war. An Kongressorten und bei wichtigen Reisen wurden Beamte der Ziffernkanzlei eingesetzt und in gleicher Weise wie die Logisten als Mitglieder des Gefolges ausgegeben.[78]

3.1.1 Die geheime Ziffernkanzlei bis 1848

Mit der Wende zum 17. Jahrhundert wurde der Bedarf an Entschlüsselungen geheimer Botschaften, der Kryptoanalyse, immer größer, sodass der Dienst von Kryptoanalytikern in Gruppen organisiert wurde, um die Lösung komplexer monoalphabethischer

[76] *Hubatschke*, Zur Problematik der „Schwarzen Kabinette". MIÖG, Bd. 83, H.3, 358.
[77] *Hubatschke*, Zur Problematik der „Schwarzen Kabinette". MIÖG, Bd. 83, H.3, 359.
[78] Harald *Hubatschke*, Die Wiener Geheime Ziffernkanzlei (1716-1848). In: Mitteilungen des Instituts für Österreichische Geschichtsforschung, Band 83, Heft 3 (1975) 364-390, hier 380.

Verschlüsselungen zu ermöglichen. Alle europäischen Mächte hatten ihre so genannten „Schwarzen Kammern", Zentren, in denen fremde Botschaften entschlüsselt und Informationen zusammen getragen wurden. „Die berühmteste, disziplinierteste und schlagkräftigste Schwarze Kammer war die Geheime Kabinettskanzlei in Wien." [79]

Über die Anfänge der Wiener Geheimen Ziffernkanzlei ist kein Dokument erhalten. Cobelli, der seit 1822 als Offizial in der Kanzlei gedient hatte, berichtete, dass auch ältere Beamte aus seinem Bekanntenkreis, worunter einige mehrere Generationen hindurch ununterbrochen in der Kanzlei gedient hatten und unter denen besonders Hofrat von Eichenfeld, der im Jahre 1773 angestellt worden war, so manches aus der Zeit Karls VI. und der Maria Theresia zu erzählen wussten, keine Kenntnis von einer Errichtungsurkunde hatten.[80] Das Institut hatte bis 1750 verschiedene Namen wie „das geheime „Zyffer Weeßen", „Zyffer Secretariat", „Kabinets-Secretariat" oder „Visitations– und Interceptions–Geschäft". Nach einer amtlichen Urkunde erteilte Maria Theresia im Jahre 1763 die Instruktion, dieses Institut „Geheime Kabinettskanzlei" zu nennen und Joseph II. verordnete 1787 die Bezeichnung „Kaiserlich–Königliche Geheime Cabinettskanzlei". Erst im 19. Jahrhundert wurden die Bezeichnungen „Geheimes Ziffernkabinett" oder „Geheime Ziffernkanzlei" allgemein üblich.[81]

Es wurde nach einem strengen Terminplan gearbeitet, denn die Tätigkeit der Geheimen Ziffernkanzlei durfte den Postbetrieb keinesfalls verzögern. Die Briefe für die Botschaften in Wien wurden zur „Schwarzen Kammer" umgeleitet, wo sie um sieben Uhr morgens eintrafen. Die Sekretäre schmolzen die Siegel und eine Gruppe von Stenographen fertigten Abschriften der Briefe an. Für Dokumente in Fremdsprachen wurden zur Anfertigung der Abschriften Sprachspezialisten herangezogen. Innerhalb von drei Stunden wurden die Briefe wieder in ihre Umschläge gesteckt, versiegelt und ins Hauptpostamt zurück gebracht, von wo aus sie den Bestimmungsadressen zugestellt wurden. Briefe auf dem Transitweg durch Wien kamen um zehn Uhr morgens an, die fürs Ausland bestimmte Korrespondenz aus den Botschaften in Wien um vier Uhr nachmittags. Auch diese Briefe wurden abgeschrieben, bevor sie ihre Reise antreten durften. Es waren im Durchschnitt hundert Briefe, die täglich durch die „Schwarze Kammer" gingen. Die Abschriften wurden an die Kryptoanalytiker weiter gegeben, die in kleinen Kammern saßen und den Sinn aus den Botschaften herausarbeiteten.[82]

[79] *Singh*, Geheime Botschaften, 81.
[80] *Stix*, Organisation der Wiener Geheimen Ziffernkanzlei. MIÖG, Bd. 51, 132.
[81] *Stix*, Organisation der Wiener Geheimen Ziffernkanzlei. MIÖG, Bd. 51, 133.
[82] *Singh*, Geheime Botschaften, 82.

Bereits interzipierte Briefe wurden mit unauffälligen Zeichen, meist mit Strichen an einer Ecke, versehen, um eine weitere Öffnung durch eine Logen in einer anderen Stadt zu vermeiden. Für die Behandlung aller Briefe, die über das Postamt in Wien befördert wurden, waren ausschließlich die Geheime Ziffernkanzlei und das Obersthof–Postamt kompetent, für alle anderen Briefe die jeweils nächstliegenden Postlogen. Die Hauptaufgabe der Geheimen Ziffernkanzlei bestand anschließend in der Auflösung fremder Chiffren–Schlüssel.[83]

Die Geheime Ziffernkanzlei arbeitete so perfekt, wodurch deren Ruf so groß wurde, dass die diplomatischen Vertreter der fremden Staaten ununterbrochen ihre Chiffren–Schlüssel änderten. Auch wenn die Schlüssel immer schwieriger wurden, konnte sie die Ziffernkanzlei lösen. Der Erfolg der Arbeit der Geheimen Ziffernkanzlei hing auch von der Qualität und Menge der Interzepte ab, die die Postlogen einsandten. Nach der Übernahme der Leitung der Kanzlei am 15. Jänner 1777 unterbreitete Kornfeld dem Kaiser Verbesserungsvorschläge, die sich nicht nur auf die Erweiterung der Geheimen Ziffernkanzlei sondern auch auf die Anzahl der Postlogen erstreckte. Er erreichte, dass die Polizeidirektion in Wien den Auftrag erhielt, von Zeit zu Zeit die Namen jener Personen mitzuteilen, die staatsfeindlicher oder krimineller Handlungen verdächtigt oder überführt wurden, um die Postlogen zur Überwachung des Briefverkehrs auch dieser Personen zu veranlassen. Weiter setzte er durch, dass die Zahl der Postlogen im Ausland erhöht und der Dienst in allen Logen verbessert wurde.[84]

Nach dem Tod Josephs II. geriet die Geheime Ziffernkanzlei in Verfall. Man beschränkte sich hauptsächlich auf das Entziffern der Berichte der auswärtigen Gesandten. Der Weg der geheimen Korrespondenzen wurde nicht weiter verfolgt, die umso häufiger wurde, als die Französische Revolution manche der früher üblichen geheimen Mittel durch Publizität unbrauchbar gemacht hatte. Ebenso vernachlässigte man auch ganz die Leitung der im In– und Ausland bestehenden Postlogen.[85] Als Metternich in die Staatskanzlei einzog, galt seine ganze Aufmerksamkeit einer Reorganisation der Geheimen Ziffernkanzlei und einer möglichen Vereinigung mit der Staatskanzlei, wie dies unter Kronenfels der Fall war. Es wurden zwar größere Missstände beseitigt, aber zu einer Generalreform kam es nicht. Eine große Erweiterung erreichten die Tätigkeiten der Geheimen Ziffernkanzlei in den Wintermonaten von 1814 auf 1815, als in Wien der große europäische Kongress tagte. Von dieser Zeit an gewann auch die *Polizeihofstelle* einen immer größeren Einfluss auf die

[83] *Stix*, Organisation der Wiener Geheimen Ziffernkanzlei. MIÖG, Bd. 51, 131f.
[84] *Stix*, Organisation der Wiener Geheimen Ziffernkanzlei. MIÖG, Bd. 51, 134f.
[85] *Stix*, Organisation der Wiener Geheimen Ziffernkanzlei. MIÖG, Bd. 51, 135f.

Angelegenheiten der Geheimen Ziffernkanzlei. Der Polizei musste jetzt Einsicht in alle Elaborate der Kanzlei eingeräumt werden, während sie vorher nur Interzepte erhielt, die das Polizeiliche betrafen. Von dieser Zeit an erschien täglich ein Hofrat der Polizeihofstelle in der Geheimen Ziffernkanzlei, um alle Interzepte abzuholen. Dem Präsidenten der Polizeihofstelle waren gemäß kaiserlicher Entschließung vom 3. März 1815 alle Interzepte vorzulegen, die sowohl der diplomatischen als auch der geheimen Polizei zugeordnet waren.[86]

Mit dem Ausbruch der Revolutionen im März 1848 wurde die Arbeit in der Geheimen Ziffernkanzlei sofort eingestellt. Da die Angriffe der Presse immer heftiger wurden, machte die Mehrheit des Personals den Leiter der Anstalt auf die Gefahren und auf die Verlegenheit aufmerksam, die man damit der Regierung und dem Kaiser selber bereiten würde. Daraufhin wurde der Dienst endgültig eingestellt. Die vorhandenen Interzepte wurden größtenteils verbrannt. Aus dem Ziffernarchiv wurden alle Ziffernschlüssel vernichtet, die länger schon nicht mehr verwendet worden waren.[87]

Am 4. April 1848, dem Tag der durch kaiserliche Entschließung offiziellen Auflösung der Geheimen Ziffernkanzlei, bestand deren Personal aus 22 Beamten und Dienern: einem Direktor, drei Subdirektoren, zwei Offizial–Majoren, neun Offizialen, vier Kanzleidienern, einem Kanzleidiener–Adjunkten und zwei Hausknechten. Nach Ablauf eines so genannten „Begünstigungsjahres“ wurden mit 8. Juni 1849 die Älteren in den Ruhestand versetzt, die anderen wurden dem Haus–, Hof– und Staatsarchiv zugeteilt.[88]

Wie bereits erwähnt, war die Geheime Ziffernkanzlei bei der Auflösung fremder Chiffren-Schlüssel so erfolgreich, dass sich in dieser Beziehung keine ähnliche Anstalt im Ausland mit Wien auch nur annähernd vergleichen konnte. Über die Anzahl der in der Wiener Ziffernkanzlei aufgelösten Chiffren gibt es keine Angaben. Zwei Aufzeichnungen beweisen aber, dass die Zahl der entschlüsselten Chiffren sehr hoch gewesen sein muss. Eine Niederschrift dokumentiert, dass in der Zeit vom 1. März 1780 bis 31. März 1781 fünfzehn höchst wichtige fremde Schlüssel aufgelöst wurden, wofür Remunerationen im Gesamtbetrag von 3.730 Gulden ausbezahlt wurden. In einer weiteren Aufzeichnung verweist 1823 Ziffernkanzleidirektor Eichenfeld darauf, dass er beachtliche 85 fremde Ziffernschlüssel in verschiedenen Sprachen und von schwerer Methode allein aufgelöst hatte. 1833 wurde der

[86] *Stix*, Organisation der Wiener Geheimen Ziffernkanzlei. MIÖG, Bd. 51, 136.
[87] *Stix*, Organisation der Wiener Geheimen Ziffernkanzlei. MIÖG, Bd. 51, hier 136f.
[88] Harald *Hubatschke*, Die Wiener Geheime Ziffernkanzlei (1716-1848). In: Mitteilungen des Instituts für Österreichische Geschichtsforschung, Band 83, Heft 3 (1975) 364-390, hier 388f.

Ziffern–Schlüssel des französischen Gesandten in Florenz entziffert. Den toskanischen Schlüssel hat Löschner 1815 in Paris aufgelöst.[89]

3.1.2 Geheime Ziffernsektion unter Kaiser Franz Joseph

Wie der ehemalige Offizial der Geheimen Ziffernkanzlei Ferdinand Prantner in einer Broschüre berichtete, bedurfte es bei der Wiedereinführung des „geheimen Dienstes“ nach einer kurzen Unterbrechung infolge der Ereignisse von 1848 der ganzen Überredungskunst des Freiherrn Karl Friedrich von Kübeck (1780–1855), um gegen das Rechtsgefühl des jungen Franz Joseph „dem Gedanken der Briefkontrolle Eingang zu verschaffen“. Freiherr von Kübeck hatte dem jungen Monarchen die Korrespondenzkontrolle als ein „Majestätsrecht“ definiert wobei ihm die Argumente des Fürsten Schwarzenberg (1800–1852) zur Seite gestanden seien. Der junge Kaiser Franz Joseph I. musste, wie früher Kaiser Franz II./I. erst an diesen Gedanken gewöhnt werden. So wie Kaiser Franz hatte sich auch Franz Joseph von Ratgebern in dieser Hinsicht überreden lassen. Die Errichtung der Obersten Polizeibehörde kann als Symbol für den Willen des Neoabsolutismus gelten, von Anfang an alle dem Kaiser zur Verfügung stehenden polizeilichen Mittel zur Regierungsführung auszunützen.[90]

Unter Berufung auf die allerhöchste Entschließung seiner k. k. Majestät vom 8. Juni 1849 zur Genehmigung der Errichtung einer eigenen „Abteilung für das Ziffernwesen und der translatorischen Arbeiten im Ministerium des Äußern und des kaiserlichen Hauses“ wurden mittels Dekret vom 14. Juni 1849 folgende Beamte in Anerkennung ihrer früheren guten Dienstleistungen in der neu geschaffenen Abteilung unter Beibehaltung der früheren Gehälter angestellt: Kaiserlicher Rath Anton v. Schweiger–Dürnstein als Vorstand oder Direktor, Kaiserlicher Rath Aloys v. Cobelli als Adjunkt oder Subdirektor, und die ehemaligen Offiziale Joseph Schneid, Johann Matscheko, Johann Urrisk, Joseph Eisl, Ferdinand Prantner und Friedrich Genotte. Die Gehälter blieben in der Reihenfolge der Namen bei 2500, 1800, 1400, 1300, 1200, 1100, 1000 und 900 Gulden zuzüglich eines jährlichen Quartierguldens von 400 Gulden. Diese Zusagen blieben jedoch bis zu einer definitiven Organisierung der besagten Abteilung dem Ministerium des Äußern vorbehalten.[91] Die Dienstleistungen der geheimen Ziffernkanzlei waren durch die Revolution zu Ende gegangen, sind aber in die neue

[89] *Stix*, Organisation der Wiener Geheimen Ziffernkanzlei. MIÖG, Bd. 51, 142.
[90] *Hubatschke*, Ferdinand Prantner, Buch 6, Diss., 1346–1348.
[91] OeStA/HHStA Sammlung 3, Chiffrenwesen, Mappe: Akten im Betreff der Organisierung der Section für Ziffernwesen und translatorischen Arbeiten, 3. Mai 1848–1870, fol 35 und 50.

„Sektion für Chiffrewesen und translatorischen Arbeiten“, mit der Kurzbezeichnung „Ziffernsektion“, im Ministerium des Äußern übergegangen. Nach einer Neuorganisierung konnten die Agenden der geheimen Briefüberwachung wieder aufgenommen werden.

Als 1850 die Gendarmerie des Öfteren zu Personalauskünften verschiedenster Art herangezogen wurde, geriet sie mit der geheimen Briefüberwachung in Kontakt, womit nicht einmal mehr die Korrespondenz des Innenministers Bach (1813–1893) mit den auswärtigen Polizeiagenten vor ihrem Zugriff sicher war. Im März 1850 äußerte Erzherzog Albrecht (1817–1895) den Wunsch, dass die Gendarmerie die Administration überwachen möge, wodurch der Gendarmerie–Inspektor zum Polizeiminister werde. Das Generalinspektorat der Gendarmerie hat Kempen (1793–1863) den Weg zum Chef der Obersten Polizeibehörde geebnet und er ist in Richtung der Installierung der Polizei als wirksamstes Mittel zur Wiederbefestigung des Staates tätig gewesen. Neben Kempen leistete der Generaladjudant des Kaisers, Graf Grünne (1808–1884), dieser Entwicklung der Behörden kräftig Vorschub. Gendarmerie–Inspektorat und Oberleitung der Polizei wollte er in einer Hand vereinigt wissen.[92]

Vor allem lag es Kübeck am Herzen, das Polizeiressort dem Minister des Inneren, Alexander von Bach abzunehmen, was Fürst Schwarzenberg zu verhindern wusste. Als nach dem Tod Schwarzenbergs die „Wiener Zeitung“ die kaiserliche Entschließung vom 25. April 1852 verlautbarte, die Polizeiverwaltung vom Ministerium des Innern abzutrennen und eine „Oberste Polizeibehörde“ mit Kempen als Chef zu organisieren, ging das Einvernehmen zwischen Bach und Kempen in Brüche. Die unmittelbare Unterordnung der neuen Behörde unter die Person des Kaisers verlieh Kempens Polizeibehörde den Rang eines Ministeriums.[93]

Mit der Einführung Kempens Oberster Polizeibehörde erblühten von neuem alle Methoden polizeilicher Durchdringung. Neben Kübeck und Grünne hieß der dritte große Mentor der Briefkontrolle nunmehr Freiherr von Kempen. Nach Übernahme seiner Behörde brachte Kempen durch einen Vortrag am 15. Juni 1852 über die „Notwendigkeit der Wiedereinführung des geheimen Postdienstes“ den Stein ins Rollen. Die Beaufsichtigung des Briefverkehres sei jetzt, wo Eisenbahnen, Dampfschiffe und Telegraphen die Entfernungen schwinden ließen und so Verbindungen zwischen den revolutionären Zentral–Komitees im Ausland und ihrem Anhang in den kaiserlichen Staaten in hohem Grad erleichtern würden,

[92] *Hubatschke*, Ferdinand Prantner, Buch 6, Diss., 1348f.
[93] *Hubatschke*, Ferdinand Prantner, Buch 6, Diss., 1349.

von großer Wichtigkeit. Entgegen dem Wunsche Kempens, der den Briefdienst an sich ziehen wollte, blieb die Leitung des reorganisierten Postlogendienstes in der Hand des Chefs der Wiener Zentralanstalt, der „Ziffernsektion“. Die Zentralanstalt wurde beim Ministerium des Äußern belassen. Der Kaiser begann sich für den Briefdienst zu interessieren und beauftragte Hofrat Schweiger mit der Ausarbeitung von Statuten für den gesamten Logendienst.[94]

3.2 Postlogen und ihre Bedeutung

Die am 3. April 1853 erlassene „Geheime Instruktion für die Ausübung des Postlogen-dienstes“ reorganisierte den geheimen Postdienst in der ganzen Monarchie, wobei man personell und institutionell an Einrichtung der geheimen „Ziffernkanzlei“ im Vormärz anknüpfen konnte. Von den ganzen Organisations–Dokumenten Schweigers und Cobellis für den Vortrag Carl Grafen von Buol Schauensteins (1797–1865) vom 27. Mai 1853 ist nur ein kleiner Teil in den „Akten im Betreff der Organisierung der Section für Ziffernwesen und translatorischen Arbeiten“ in der HHStA Sammlung 3–1, Chiffrenwesen, erhalten geblieben. Eines der drei wichtigen Dokumente ist neben dem „Organisations-Statutes für die Vollziehung des geheimen Dienstes durch die im Ministerium des Äußern bestehende Sektion für Ziffernwesen und translatorischen Arbeiten“ die „Geheime Instruktion für die Ausübung des Postlogendienstes“, deren Text hier eingefügt wird. Ein drittes Dokument behandelt den „Personal-Status“ der Beamten der Sektion für Chiffrewesen. Diese drei Dokumente beinhalten die Statuten, die in den folgenden 15 Jahren die Grundlage der Organisation des geheimen Briefdienstes bildeten.[95]

„Geheime Instruktion für die Ausübung des Postlogen Dienstes

Der Zweck der Anstalt des geheimen Dienstes ist, zur genauen Kenntnis dessen zu gelangen, was sowohl der äußeren als auch der inneren öffentlichen Sicherheit des Staates und seiner Wohlfahrt überhaupt nachtheilig werden könnte, um jeder etwa drohenden Gefahr auf die schnellste Art zu begegnen und das Übel wo möglich in seinem Entstehen zu ersticken.

Sämtliche Logenbeamte sind in geheimdienstlicher Beziehung unter den Director der Anstalt in Wien gestellt, welcher von allem, was die Verhältnisse des geheimen Dienstes betrifft, regelmäßig in genaue Kenntniß zu setzen ist.

Die Ausübung des geheimen Dienstes darf überall und zu jeder Zeit, nur infolge einer von dem Director der Anstalt in Vollziehung höherer Befehle, ausgehenden Ermächtigung statt finden.

[94] Harald *Hubatschke*, Der geheime Briefdienst nach 1848. In: Mitteilungen des Instituts für Österreichische Geschichtsforschung, Band 83, Heft 3 (1975) 390-398, hier 391.
[95] OeStA/HHStA Sammlung 3, Chiffrenwesen, Mappe: Akten im Betreff der Organisierung der Section für Ziffernwesen und translatorischen Arbeiten, 3. Mai 1848–1870, fol 113-114.

Es dürfen nur jene Korrespondenzen in den Logen eröffnet und abschriftlich vorgelegt werden, deren Überwachung von dem Director der Anstalt in Wien im Vorhinein genehmigt worden ist.

Andere Eröffnungen sind strengstens untersagt, und Ausnahmen nur in sehr dringenden Fällen, mit gleichzeitiger Anzeige und Begründung an den Director der Anstalt gestattet.

Die zu überwachenden Korrespondenzen werden den Logen von dem Director theils nach Kategorien, theils namentlich bezeichnet.

Ueber die der Loge von Seite des Directors zur Überwachung bezeichneten Korrespondenzen hat der Vorstand ein eigenes Protokoll zu führen, in welchem die Namen nebst dem Datum, unter welchem die Eröffnung angeordnet oder gutgeheißen worden ist, stets evident zu halten ist.

Sollten sich aus der Perlustrierung weitere, der Loge noch nicht bezeichnete Namen ergeben, deren Ueberwachung angemessen erscheint, so sind dieselben dem Director mitzuteilen, um von diesem die Ermächtigung zu erlangen, den geheimen Dienst auch auf sie ausdehnen zu dürfen.

Alle Interzepte sind unmittelbar und ohne Aufschub an den Director der Anstalt in Wien einzusenden.

Die Vorstände der Postlogen sind berechtigt, solche Interzepte, welche nach ihrer Ansicht, zumal für die Verwaltung des betreffenden Kronlandes, von dringendem Interesse sind, dem Statthalter in demselben gegen Rückstellung mitzuteilen; sie sind jedoch verpflichtet, gleichzeitig eine Abschrift davon, mit Angabe der geschehenen Mittheilung an den Director einzuschicken, an welchen auch die von dem bezüglichen Statthalter dem Vorstand der Loge zurück gestellten Piécen seiner Zeit zu leiten sind.

Als die erste Pflicht des mit der Ausübung des geheimen Dienstes innerhalb der von nun an festgesetzten Grenzen Beauftragten, ergibt sich die gewissenhafteste Beobachtung der beschworenen Verschwiegenheit, und kluge Entfernung jeder Veranlassung zur Vermuthung, dass die der Postanstalt anvertrauten Gedanken enthüllt werden.

Es wird daher den Logenbeamten die äußerste Sorgfalt in der Behandlung der Briefe und Paquete zur Pflicht gemacht; sowie zur Beseitigung jedes Verdachtes, auch jede Hemmung eines Korrespondenzstückes in seinem normalen Lauf zu vermeiden ist.

Die äußerste Vorsicht im Benehmen gegen Fremde sowohl, als gegen die in das Geheimniß nicht eingeweihten Postbeamten, ein gesetztes, bescheidenes, ruhiges und in jeder Beziehung unbescholtenes Betragen, Eifer und Fleiß im Dienste, und, erforderlichen Falls gegenseitige collegialische Unterstützung sind im Allgemeinen die Anforderungen, durch deren gewissenhafte Erfüllung der Logenbeamte seinem wichtigen Auftrage zu entsprechen vermag, und welche daher nebst der genauesten Befolgung der oben angeführten Weisungen, als die Hauptpunkte seiner besonderen Dienstpflichten bezeichnet werden.

Wien, am 3ten April 1853“[96]

[96] OeStA/HHStA Sammlung 3, Chiffrenwesen, Mappe: Akten im Betreff der Organisierung der Section für Ziffernwesen und translatorischen Arbeiten, 3. Mai 1848–1870, fol 113-114.

Es durften die Korrespondenzen nur von jenen Personen interzipiert werden, deren Über–wachung vom Direktor der Wiener Anstalt zuvor angeordnet worden war. Die Interzepte wurden unverzüglich nach Wien gesandt. Die Logisten hatten die geschworene Verschwiegenheit gewissenhaft einzuhalten, hatten sich großer Vorsicht gegenüber den nicht eingeweihten Postbeamten zu befleißigen, auf einen ruhigen unbescholtenen Lebenswandel zu achten und sich gegenseitige kollegiale Unterstützung angedeihen zu lassen. [97]

Die Auswahl und Ausbildung der Logisten lag im Ermessen und in der Verantwortung des Direktors der Ziffernkanzlei, in dessen Gegenwart auch der Eid zu absolutem Schweigen abzulegen war. Eine Verletzung des Eides konnte aus verständlichen Gründen nur in einem Sonderdisziplinarverfahren, niemals vor Gericht, bestraft werden.[98] Im Unterschied zu den Logisten war den Beamten, vor allem den höheren Beamten, ein Universitätsstudium zur Aufnahme in den Staatsdienst vorgeschrieben. Für die Regierungsspitze führte der Weg zu einem modernen Staat nur über ein Beamtentum, das mit modernen Kenntnissen ausgestattet war. Diese konnten im Studiensystem anfangs des 19. Jahrhunderts nur an der Universität vermittelt werden.[99] 1801 wurde die Vorschrift eingeführt, dass jeder Beamte vor Ablegung des Diensteides den Eid schwören musste, keiner geheimen Gesellschaft anzugehören.[100] In Anlehnung an ein Rundschreiben Alexander von Bachs vom 15. August 1849 entstand ein „Leitfaden“ für das Verhalten des idealen Beamten, in dem an oberster Stelle der erwarteten Eigenschaften „Anhänglichkeit an das monarchische Prinzip und an das Allerhöchste Regentenhaus“ standen. Weiter folgten im Tugendkatalog die wichtigsten Eigenschaften des Beamten, wie: „Ehrenhaftigkeit“, „Unbescholtenheit“, „Subordination und Gehorsam“, „Verschwiegenheit“ und schließlich die typischen bürgerlichen Pflichten.[101]

Um die Mitte des Jahres 1853 nahm der österreichische Neoabsolutismus die geheime Briefüberwachung voll auf.[102] Im Juni desselben Jahres wurden die Logen aus den Jahren des Vormärz übernommen, reorganisiert und wiederbelebt. Die Postlogen der Sektion in Wien ließen sich in drei Kategorien schematisieren: Die „Reichslogen“, die „österreichischen

[97] Harald *Hubatschke*, Der geheime Briefdienst nach 1848. In: Mitteilungen des Instituts für Österreichische Geschichtsforschung, Band 83, Heft 3 (1975) 390-398, hier 392.
[98] Harald *Hubatschke*, Die Wiener Geheime Ziffernkanzlei (1716-1848). In: Mitteilungen des Instituts für Österreichische Geschichtsforschung, Band 83, Heft 3 (1975) 364-390, hier 380.
[99] Waltraud *Heindl*, Gehorsame Rebellen. Bürokratie und Beamte in Österreich. Bd. 1: 1780 bis 1848 (2. durchgesehene Auflage, Wien/Köln/Graz 2013) 111.
[100] *Heindl*, Gehorsame Rebellen, 50.
[101] Waltraud *Heindl*, Josephinische Mandarine. Bürokratie und Beamte in Österreich. Band 2: 1848 bis 1914 (Wien/Köln/Graz 2013) 57.
[102] *Hubatschke*, Der geheime Briefdienst nach 1848, 392.

Postlogen“ und die „toskanischen Postlogen“. Zu den „Reichslogen“ zählten die Institute in Frankfurt, Nürnberg, Augsburg, Regensburg, Hildesheim, Hamburg sowie in Innsbruck, Bregenz, Konstanz und Brüssel. Im eigentlichen Sinne „österreichische“ Postlogen bestanden in Temesvar, Semlin, Kostajnica, Spalato, Triest, Venedig, Zara, Udine, Padua, Vicenza, Verona, Badia del Polesine, Mantua, Mailand, Bregenz, Innsbruck, Salzburg, Linz, Prag, Marienbad, Karlsbad, Peterswalde, Brünn, Teschen, Podgorze, Lemberg, Brody, Wien, Graz, Kaschau, Ofen–Pest, Debreczin, Esseg, Hermannstadt, Klausenburg, Laibach und Troppau. Im Süden der Monarchie kam den toskanischen Postlogen in Florenz und Livorno große Bedeutung zu.[103]

Zur gleichen Zeit wurden die Logen im Lombardisch–Venezianischen Königreich neu organisiert und die dortigen Logenchefs durch ihre Vorgesetzten eingewiesen. Radetzky (1766–1858) drängte auf eine stärkere Integrierung seiner Person in die Leitung des geheimen Postdienstes im Süden der Monarchie. In diesem, wie in den meisten ähnlichen Fällen, bildete der allgewaltige Generaladjudant des Kaisers Graf Grünne den Vermittler zwischen dem Monarchen und Hofrat Anton von Schweiger. Das Militär– und Zivilgouvernement beantragte mit Erfolg die Errichtung von Logen in Raab und Fünfkirchen. Das Fehlen von Logen in Kroatien und Slowenien empfand man angesichts der angespannten politischen Lage als sehr schmerzlich. Im Einvernehmen mit Joseph Jellačić (1801–1859), Ban des Königreiches Kroatien und Slawonien, beschloss man die Errichtung einer Loge in Agram.[104]

Im Allgemeinen erstellte Kempen die Liste der zu überwachenden Personen, übergab sie Hofrat Schweiger und dieser erwirkte mit Hilfe des Generaladjudant Grünnes die Sanktionierung des Kaisers. Die zum Teil umfangreichen Listen gaben einen Einblick in den neoabsolutistischen Begriff von politischer Vorsicht. Der Krakauer Loge fiel die Überwachung politisch bedenklicher Korrespondenzen von Emigranten und politischen Flüchtlingen zu, welche auf Grund ihrer Vertrautheit mit den Verhältnissen vom Krakauer Logenchef namhaft gemacht worden waren. Kempen ist es durch die Hilfe der Ziffernsektion gelungen, die von Lajos Kossuth (1802–1894) vergrabene ungarische Krone wiederzufinden. Im Mai 1853 ersuchte er Direktor Schweiger um Dechiffrierung jener Notizen, die die Anleitungen zur Auffindung der ungarischen Krone für Varga enthielten.[105]

[103] *Hubatschke*, Die Wiener Geheime Ziffernkanzlei (1716-1848), 381.
[104] Harald *Hubatschke*, Der geheime Briefdienst nach 1848. In: Mitteilungen des Instituts für Österreichische Geschichtsforschung, Band 83, Heft 3 (1975) 390-398, hier 393.
[105] *Hubatschke*, Ferdinand Prantner, Buch 6, Diss., 1363.

Die hohen Ausgaben zur Finanzierung der Außenpolitik führten zu einer unbefriedigenden innenpolitischen Lage. Die Monarchie unterlag dem verbündeten Königreichen Piemont–Sardinien und Frankreich in der Schlacht bei Manageta am 4. Juni 1859 und musste Mailand räumen. Am 24. Juni 1859 erlitt das österreichische Heer bei Solferino eine verheerende Niederlage. In dem am 8. Juli 1859 geschlossenen Waffenstillstand von Villafranca zwischen Franz Joseph I. und Napoleon III., dem der formelle Frieden von Zürich am 10. November folgte, musste Österreich die Lombardei an Napoleon III. abtreten, der sie an Piemont–Sardinien weitergab.[106]

Im Oktober 1859 übernahm das Finanzministerium die oberste Leitung des Postwesens, womit dem Chef dieses Ressorts nähere Details über den geheimen Briefdienst mitzuteilen waren. Zu diesem Zweck gab man ihm einen Auszug aus dem Erlass über den geheimen Postdienst vom 3. April 1853. Mit dem Zweck der Abgrenzung dieses Dienstes setzte sich auch der Direktor der Ziffernsektion Schweiger mit Finanzminister Karl Ludwig von Bruck (1796–1860) ins vertrauliche Einvernehmen. Im Zusammenhang mit den politischen Verhältnissen trat gegen Ende des Jahres 1859 eine sehr starke Zunahme des Arbeitsvolumens für den geheimen Postdienst auf. Es wurde eine neue Loge beim Postamt Feldkirch eingerichtet, worüber der Statthalter in Tirol, Erzherzog Karl Ludwig (1833–1896), mit einem kaiserlichen Handschreiben mit einem Auszug aus dem Statut unterrichtet wurde. Das Jahr 1859 war ein sehr ereignisreiches Jahr für den geheimen Postdienst, nicht nur was den unglücklichen Feldzug und den Wechsel in allen führenden Positionen in der Generaladjutantur betraf. Die Mitteilung der Interzepte wurde von nun an etwas weniger streng gehandhabt, wobei mit Ausnahme der wenigen Stücke mit der Aufschrift „Einzige Abschrift für Seine Majestät“ alle Interzepte gemäß ihrem jeweiligen Inhalt entweder dem Ministerium des Äußern oder dem Polizeichef zugänglich gemacht wurden.[107]

Das Logenpersonal dürfte auch in den 1860er Jahren zur vollen Zufriedenheit der Wiener Zentralstelle gearbeitet haben. Der Direktor der Ziffernsektion konnte am Schluss des Semesters für die um den geheimen Dienst besonders verdienten Postbeamten und Diener eine außerordentliche Remuneration beantragen. Nach dem Jahre 1864 werden die Quellen über die geheime Briefüberwachung in den Postlogen immer weniger. Es ist noch ein letztes Mal von der Kontrolle der Korrespondenz der ungarischen Parteiführer die Rede, die unter Verwendung einer Deckadresse abgewickelt worden sein dürfte. Dass dieses Aktenstück das

[106] Stephan *Vajda*, Felix Austria, Eine Geschichte Österreichs (Wien/Heidelberg 1980) 514.
[107] *Hubatschke*, Ferdinand Prantner, Buch 6, Diss., 1372f.

letzte ist, liegt an den Verlusten im Aktenbestand des „Gendarmerie–Departements“. Der Dienst dürfte aber noch drei weitere Jahre ausgeübt worden sein. Seine guten Ergebnisse verdankte er nicht zuletzt der umsichtigen Leitung, die er von der übergeordneten Wiener Zentrale, der „Sektion für Chiffrewesen und translatorische Arbeiten“ im Ministerium des Äußern erhalten hatte.[108]

Das Ende der Briefüberwachung in den Postlogen wurde letztlich dadurch verursacht, dass die Politik nach 1867 immer stärker vom Volk mitgetragen und von ihrem Charakter her immer demokratischer wurde.[109] Die Demokratisierung wurde mit der Billigung der „Dezemberverfassung“ durch den Kaiser am 21. Dezember 1867 eingeleitet, mit der sieben Gesetze in Kraft traten, die auf Regierungsvorlagen und auf den Verfassungsausschuss des Reichsrates zurückgingen. Die Staatsgrundgesetze, darunter das Staatsgrundgesetz über die allgemeinen Rechte der Staatsbürger für die im Reichsrat vertretenen Königreiche und Länder, galten als selbständige Initiative des Parlaments.[110] Die letzten Reste der „Schwarzen Kabinette“ fielen dem Liberalismus zum Opfer. Der Artikel 10 im Staatsgrundgesetz über die allgemeinen Rechte der Staatsbürger verbot die Verletzung des Briefgeheimnisses mit Ausnahme eines Richterbefehles und des Kriegsfalles. Zu diesem Grundrecht erging am 6. April 1870 das Gesetz zum Schutze des Brief– und Schriftengeheimnisses, welches als Ausführungsgesetz zu diesem Artikel des Staatsgrundgesetzes anzusehen ist.[111]

3.2.1 Dienstverrichtung in den Postlogen

Von den Offizialen sowohl in den Postlogen als auch in der Wiener Ziffernsektion wurde eine extrem schnelle Handschrift verlangt, fallweise auch Kurzschrift. Um den Vorgang bei längeren Schriftstücken zu rationalisieren, diktierten zwei oder auch vier Offiziale gleichzeitig aus einem Bogen gleich vielen Schnellschreibern, wodurch jeder Bogen in wenigen Minuten auf die geschickteste Art kopiert werden konnte. Nicht weniger Fleiß, Schnelligkeit und Geschicklichkeit als die kopierenden Offiziale benötigten die Kanzleidiener und Offiziale, die die Öffnungsmanipulationen der Briefe durchführten. Es bedurfte neben einer ungeheuren manuellen Geschicklichkeit und einem besonderen Fingerspitzengefühl für eine unsichtbare „geheime Behandlung“ der Briefe auch eines beträchtlichen Umfanges an geeigneten

[108] *Hubatschke*, Ferdinand Prantner, Buch 6, Diss., 1380f.
[109] Pieter M. *Judson*, Habsburg. Geschichte eines Imperiums 1740–1918 (München 2017) 351.
[110] Wilhelm *Brauneder*, Die Verfassungsentwicklung in Österreich 1848 bis 1918. In: Helmut Rumpler, Peter Urbanitsch (Hg.), Die Habsburgermonarchie 1848–1918, Bd. 7: Verfassung und Parlamentarismus, 1. Teilband: Verfassungsrecht, Verfassungswirklichkeit, zentrale Repräsentativkörperschaften (Wien 2000) 69–237, hier 176.
[111] *Hubatschke*, Zur Problematik der „Schwarzen Kabinette“. MIÖG, Bd. 83, H.3, 361.

Werkzeugen. Die Siegelabdrücke wurden vom Kanzleidiener mit Silberamalgam abgenommen und von dem abwechselnd zur Manipulation bestimmten Offizial behandelt. Das abgenommene Siegel wurde auf einem Zettel mit dem Namen des Adressaten bereitgelegt und der Brief sodann über einer Kerze geöffnet. Der Manipulant musste sich die Anordnung der im Kuvert befindlichen Stücke merken und sie dann dem Subdirektor zur Auswahl übergeben. Das einfachste Werkzeug, die Grundausrüstung jedes Manipulanten, bestand aus einer Paste, einer „Reibschale samt Stößel", einem „Leuchter samt Hütel", einem stumpfen Messer aus Metall und einem aus Knochen („Beinl" genannt) zur Öffnung der Briefe mit Oblaten. Rauchlose, mit dünnem Docht hergestellte „Kerzeln" vervollständigten die nötigsten „Brieföffnungs–Requisiten".[112]

Adresse und Verschluss befand sich auf den Briefen entweder auf der Vorder– oder Rückseite des zusammengefalteten Briefpapiers, oder auf einem besonderen Umschlag, den man bis zur Mitte des 19. Jahrhunderts nach eigenen Vorstellungen faltete. Die heute übliche Form des Briefumschlages wurde 1820 von einem Buchhändler namens Brever in England erfunden. Zum Verschluss der Briefe hat man früher Siegel aus Bienenwachs verwendet, seit dem beginnenden 17. Jahrhundert jedoch zunehmend Oblaten und vor allem Siegellacke, das so genannte „spanische Wachs". Die selten verwendeten Oblaten öffnete man mit Hilfe eines beinernen Messers. Häufiger verwendet wurden Siegel, deren Gebrauch in Österreich mit der Briefpostordnung von 1838 üblich wurde. Ihnen rückte man in den Logen mit einer Silberamalgampaste zu Leibe, die, zähflüssig in einem Ring eingegossen, an einer Flamme rasch erhärtete und einen scharfen Abdruck ergab. Den Siegellack brauchte man dann nur über den rauchlosen kleinen Kerzen „mit unruhiger Hand" zu erwärmen und auseinander zu ziehen. Nach dem Lesen wurde der Siegellack wieder erwärmt und auf dem neuerlich zusammengefalteten Brief der Abdruck des hergestellten Siegelstempels aufgebracht. Die Manipulation hinterließ bei richtiger Durchführung keinerlei Spuren. Die nachgemachten Siegelstempel hielten mehrere Wochen.[113]

Nicht nur die Logisten, sondern auch die Diplomaten beherrschten derlei Praktiken. In Wien hatte man 1802 die Kunst entwickelt, Briefe, die mit sympathetischer Tinte und zusätzlich in Chiffren verfasst waren, lesbar zu machen und zu entziffern, ohne das Original zu beschädigen. Hofrat Gentz konnte Siegeln in Lehm und Ton abdrucken und auf einem

[112] *Hubatschke*, Ferdinand Prantner, Buch 5, Diss., 1276.
[113] *Hubatschke*, Ferdinand Prantner, Buch 5, Diss., 1277.

Kohleofen zu Petschaften trocknen lassen. Dieses Verfahren wurde auch in der Linzer Postloge angewendet. Ein spanischer Legationssekretär verwendete auf dem Wiener Kongress beim Lösen des Siegels eine Platte mit einer runden Öffnung, um beim Erwärmen des Siegellacks das Briefpapier nicht zu beschädigen. Künstliche Siegel stellte er aus erhärtetem Wachs her. Ein walachischer Agent namens Bellio, bediente sich in Wien zur Herstellung von Siegelabdrücken einer erwärmten weißen Wachsmasse, die in kaltes Wasser getaucht, erhärtete. Für Siegel, die häufig vorkamen, wurden eigene Metallsiegelstempel nachgestochen, was den Logisten die Arbeit sehr erleichterte. Diese Siegelkopien wurden nach Nationen geordnet und in der geheimen Ziffernkanzlei in einem besonderen Schrank aufbewahrt. Wien dürfte über Kopien aller sardinischen Siegelstempel verfügt haben, deren Abdrücke von echten nicht zu unterscheiden waren. Der erwähnte Bellio, der Gentz‘ Berichte an den Hospodar der Walachei interzipierte, hatte dazu einen nachgestochenen Stempel von dessen Siegel verwendet.[114]

Sowohl in den Postlogen als auch in anderen Ländern wurden die Methoden weiter entwickelt. Graveure in Hannover hatten von jedem angefertigten Siegelstempel ein Pflichtexemplar abzuliefern; in Frankreich stach man Metallsiegelstempel auf Vorrat und in Kursachsen unterhielt der geheime Postdienst einen besonders begabten und talentierten Kalligraphen, der, falls der Originalumschlag durch die Manipulation beschädigt wurde, neue Umschläge völlig schriftgleich beschrieb und bei Bedarf auch das Datum der Absendung etc. unkenntlich veränderte. Ähnliches ist von den österreichischen Logen oder der Geheimen Ziffernkanzlei nicht bekannt, aber auch hier sind, wie überall, manchmal unter Zeitdruck peinliche Pannen passiert. Die geforderte Schnelligkeit ging manchmal auf Kosten der Genauigkeit: Verwechslungen des Siegels und andere Versehen waren als Berufsrisiko einkalkuliert. Solche Missgeschicke sind jedoch sehr selten vorgefallen.[115]

Der bedeutendste Unfall dieser Art wurde durch das ähnliche Aussehen der Siegel von Parma und Modena veranlasst, und der Herzog von Modena konnte bei Übersendung des Briefumschlages nach Parma hinzufügen: „Nicht allein ich, sondern auch Sie!“ Erzherzog Max führte deswegen beim Grafen Josef von Sedlnitzky (1778–1855) Beschwerde und man grollte der Polizeihofstelle trotz der Versicherung, dass diese mit diesem Zweig, dessen Ort der Beschwerdeführer nicht eruiert hatte, nichts zu tun habe.[116]

[114] *Hubatschke*, Ferdinand Prantner, Buch 5, Diss., 1278.
[115] *Hubatschke*, Ferdinand Prantner, Buch 5, Diss., 1279.
[116] *Stix*, Organisation der Wiener Geheimen Ziffernkanzlei. MIÖG, Bd. 51, 141.

Die Werkzeugausrüstung der Logen wurde von der Geheimen Ziffernkanzlei ausgewählt und in eigenen Kassetten zusammengestellt. Leider ist keine dieser Kassetten erhalten geblieben, allerdings sind im Wiener Haus–, Hof– und Staatsarchiv einige geöffnete und nicht mehr weitergeleitete Briefe überliefert, anhand der die Methoden der Öffnung erkennbar werden. Es lag selbstverständlich im Interesse der Ziffernkanzlei, dass keine der Eröffnungsmethoden einem breiteren Publikum zugänglich gemacht wurde. Zur Vermeidung gesundheitlicher Schäden durch giftige Quecksilberoxid–Dämpfe, die bei der Erwärmung des Siegellackes und der Paste entstanden, wurde in der Geheimen Ziffernkanzlei höchst wahrscheinlich ein Dunstabzug zur Absorbierung der Giftstoffe verwendet.[117]

3.3 Organisation der „Sektion“ für Chiffrenwesen

Die Postlogen verkehrten sowohl untereinander als auch mit der Ziffernkanzlei bzw. Ziffernsektion schriftlich nur in Chiffren, die man des Öfteren auswechselte. Nicht chiffrierte Begleitschreiben waren streng verboten. Die Umschläge der täglichen Interzept–Sendungen waren in besonderer Art versiegelt und fallweise mit Deckadressen versehen, so etwa mit der Adresse fingierter Personen oder den Geschäften in Wien. Oft war es für die Postämter nicht leicht, derart getarnte Sendungen verlässlich an die Ziffernkanzlei zu leiten. Wie die Beamten in den Postlogen hatten die Beamten in der Ziffernkanzlei intelligent, eifrig, sprachkundig und absolut zuverlässig zu sein, weil, wie bei allen Geheimdiensten, oft Wohl und Wehe von Menschen in ihrer Hand lag und eine Auswahl der Interzepte oder deren Verfälschung über Schicksale entscheiden konnten. Ein gegenüber dem Direktor der Geheimen Ziffernkanzlei abgelegter Eid verpflichtete sie zu absolutem Stillschweigen.[118]

Neben der Aufgabe der Öffnung aller in Wien zu überwachenden Briefe, die ihr das Obersthof–Postmeisteramt zuspielte, war die Ziffernkanzlei mit der Leitung der Provinzlogen befasst. Ihre Hauptaufgabe bestand aber darin, sämtliche Interzepte, sowohl die selbst gewonnenen als auch die von den Postlogen zugeleiteten, zu dechiffrieren. Einerseits galt es, Übersetzungsdienste zu leisten und fremdsprachige Ziffern aufzulösen, andererseits auch für den eigenen diplomatischen Gebrauch selbst Ziffernschlüssel zu entwerfen, die dann dem Ziffernkabinett der Staatskanzlei zur Verfügung gestellt wurden. Von den Ziffernschlüsseln, die die Geheime Ziffernkanzlei für den eigenen Gebrauch zur Korrespondenz mit dem

[117] *Hubatschke*, Ferdinand Prantner, Buch 5, Diss., 1280.
[118] *Hubatschke*, Ferdinand Prantner, Buch 5, Diss., 1281.

diplomatischen Vertretungsbehörden im Ausland entwarf, sind nur wenige erhalten. Sie dürften immer dann vernichtet worden zu sein, wenn die Gefahr eines Krieges bestand. [119]

Die genannten Aufgaben der Beamten der neuen Sektion für Ziffernwesen sowie die Rückkehr von Bitermann und Ottenfeld in die neue Ziffernsektion sind im bereits erwähnten „Personal Status" enthalten, aus dem hier der Text des §1 eingefügt wird.

> „Personal Status
> und Behandlung der gegenwärtigen und zukünftigen, mit der Vollziehung des geheimen Dienstes beauftragten Beamten der Sektion : „für Ziffernwesen und translatorische Arbeiten" im Ministerium des Äußern.
> §1
> Da diese Abtheilung auch fernerhin die im Ministerium des Äußern benöthigten translatorischen Arbeiten, die Verfertigung von Ziffer-Schlüsseln für die allerhöchsten Missionen, so wie überhaupt alle jene Dienstleistungen zu besorgen haben wird, welche ihr bisher zugewiesen waren, so ergibt sich schon aus diesem Grunde, und abgesehen von der wünschenswerten Verjüngung des dermaligen Beamtenstandes, die Notwendigkeit der Verstärkung des gegenwärtigen aus sieben Beamten und zwei Dienern bestehenden Personals, welches zuvörderst durch Einberufung der dermalen im Haus-, Hof- und Staatsarchive verwendeten vormaligen Kabinettsoffiziale Rath Bitermann und Ritter v. Ottenfeld, dann des dortigen Diener Joseph Bacher zu vervollständigen ist. […]" [120]

Hervorzuheben ist die in diesem Personal Status festgeschriebene „Aufgabe der Verfertigung von Ziffer–Schlüssel für die allerhöchsten Missionen", wovon die Verschlüsselungsmethoden für höhere Aufgaben im Gegensatz zu einfachen Schlüssel für untergeordnete Aufgaben abzuleiten ist, für die die Ziffernsektion nicht zuständig war.

Die mit dem 8. Juni 1849 in die Ziffernsektion aufgenommenen Offiziale Schneid und Prantner wurden bereits am 16. Juni den Departements A, B, C und D im Ministerium des Äußern für die ungarischen Angelegenheiten als translatorische Hilfskräfte zugewiesen. 1852 kehrten nicht nur Prantner und Schneid sondern auch Bitermann und Ottenfeld in die Sektion zurück. Zusammen mit dem Logenstatut wurde am 3. April 1853 auch das noch wichtigere „Organisations-Statut für die Vollziehung des geheimen Dienstes durch die im Ministerium des Äußern bestehende Sektion für Zifferwesen und translatorische Arbeiten" erlassen und regelte den geheimen Postdienst der gesamten Logenpolitik der nächsten 15 Jahre.[121]

Das von Schweiger und Cobelli ausgearbeitete Organisations-Statut hatte vor allem die Kooperation der Postlogen mit der Wiener Zentralanstalt, der „Sektion", zum Inhalt. Da es

[119] *Hubatschke*, Ferdinand Prantner, Buch 5, Diss., 1289.
[120] OeStA/HHStA Sammlung 3, Chiffrenwesen, Mappe: Akten im Betreff der Organisierung der Section für Ziffernwesen und translatorischen Arbeiten, 3. Mai 1848–1870, fol 107-108.
[121] *Hubatschke*, Ferdinand Prantner, Buch 6, Diss., 1383–1385.

sich um eines der wenigen, noch vorhandenen Dokumente in diesem Zusammenhang handelt, werden hier die ersten sieben Paragraphen von insgesamt 28 wiedergegeben:

„Organisations Statut
Für die Vollziehung des geheimen Dienstes durch die im Ministerium des Äußern bestehende „Section für Zifferwesen und translatorische Arbeiten“

§ 1: Die bei dem Ministerium des Äußern bestehende, mittelst Allerhöchster Entschließung vom 8ten Juni 1849 aus den dienstfähigen Beamten der vormaligen geheimen Kabinettskanzlei gebildete Sektion „für Zifferwesen und translatorische Arbeiten“ ist unter Beibehaltung dieser Benennung und ihrer damaligen Dienstverrichtungen, sowie eines besonderen, von den übrigen Departements gehörig getrennten Amtslokales im Gebäude des Ministeriums künftighin auch mit der Vollziehung des geheimen Dienstes beauftragt, und als eine besondere, in sich abgeschlossene Anstalt unter die Überwachung des Ministers des kaiserlichen Hauses und des Äußern gestellt.

§ 2: Seine k.k. apostolische Majestät behalten Sich die unmittelbare, jedesmalige Ernennung des Direktors vor.

§ 3: Uiber die Besetzung aller übrigen Stellen der Beamten und Diener ohne Ausnahme, so wie über deren Pensionierung, Quieszirung oder Entfernung beschließen Seine Majestät über Vorschlag des Direktors und Begutachtung Seitens des Ministers des Hauses und des Äußern.

§ 4: Der einzige Zweck des geheimen Dienstes ist die Wahrung der höchsten Interessen des Thrones und des Staates; es sollen daher auf diesem Wege keineswegs andere Zwecke verfolgt werden.

§ 5: Die Ausübung dieses Dienstes darf überall und zu jeder Zeit nur in Folge einer von dem Direktor der Anstalt in Vollziehung des allerhöchsten Willens ausgehender Ermächtigung stattfinden.

§ 6: Es dürfen nur jene Korrespondenzen in Wien und den Kronländern eröffnet und abschriftlich vorgelegt werden, deren Uiberwachung im Vorhinein von Seiner Majestät gutgeheißen worden ist.

§ 7: In Folge dessen hat der Chef der obersten Polizeibehörde, und nach Umständen der Minister des Äußern auf kurzem Wege Verzeichnisse der Personen mit begründeten Schlagwörtern vorzulegen, welche mit der allerhöchsten Genehmigung versehen, unmittelbar an den Direktor der Anstalt geleitet werden, dem das Geeignete zu veranlassen obliegen wird.

[§ 8 bis § 28 sind hier nicht wiedergegeben]. Wien, am 3ten April 1853“ [122]

Der Direktor der „Section für Chifferwesen und translatorische Arbeiten“ beim Ministerium des Äußern und des Hauses hatte einen Eid zu Gott dem Allmächtigen zu schwören und bei seiner Ehre und Treue Seiner Majestät, Kaiser Franz Joseph dem Ersten, zu geloben, unverbrüchlich treu und gehorsam zu sein. Nachdem Seine apostolische Majestät ihn zum

[122] OeStA/HHStA Sammlung 3, Chiffrenwesen, Mappe: Akten im Betreff der Organisierung der Section für Ziffernwesen und translatorischen Arbeiten, 3. Mai 1848–1870, fol 95-100.

„Hofrathe und Direktor der Sektion“ zu ernennen geruht hatte, musste er schwören, die ihm in seinem Amte obliegenden Pflichten gewissenhaft zu erfüllen und das von Seiner Majestät dem Kaiser allerhöchst genehmigte Organisations–Statut der Abteilung, der er vorsteht, genau zu befolgen. Dieser Eid wurde von Anton v. Schweiger–Dürnstein am 2. Mai 1853 in Gegenwart des Ministers des Äußern und des Hauses Graf von Buol Schauenstein abgelegt. Aloys v. Cobelli legte den gleichen Eid am 21. April 1862 in Gegenwart des Ministers des kaiserlichen Hauses und des Äußern Graf von Rechberg (1806–1899) ab.[123]

Als Zweck des geheimen Dienstes wurde vom Statut „die Wahrung der höchsten Interessen des Thrones und des Staates sowie die Abwendung von Nachteil und Gefahr“ verlangt. Die Vorschläge für die zu kontrollierenden Korrespondenzen gingen vom Chef der Obersten Polizeibehörde und vom Minister des Äußern aus. Der Direktor der Sektion leitete sie über den Generaladjutanten zur Genehmigung an den Kaiser. Auf allerhöchsten Befehl und im Hinblick auf § 9 des Organisations-Statuts enthielt das genehmigte „Categorien–Verzeichnis“ die Korrespondenzen der in Wien akkreditierten Gesandtschaften sowie sämtlicher fremder Konsulate im Reiche.[124] Die Interzepte mussten je nach Inhalt dem Minister des Äußern oder dem Chef der Obersten Polizeibehörde mitgeteilt werden. Die Zusendung erfolgte in der Regel einmal täglich. Der Direktor der Ziffernsektion hatte im Besonderen die Pflicht, in ausnahmsweise wichtigen Angelegenheiten eine Abschrift des Interzepts sofort dem Kaiser vorzulegen (§15). Das Ziffernwesen an sich, das Chiffrieren und Dechiffrieren, unterstand ausschließlich dem Minister des Äußern (§19). Dem Chef der Obersten Polizeibehörde wurden nur die Entzifferungselaborate von polizeilichem Interesse schriftlich mitgeteilt (§20).

In einer Neuauflage des „kaiserlichen Hof– und Staatshandbuches für das österreichische Kaiserthum“, das vom Ministerium des Inneren im Herbst 1855 herausgegeben wurde, erschienen entsprechend dem Punkt 4 der „Allerhöchsten Entschließung vom 27. April 1853“ auch die Namen und einige Daten der Beamten und Diener der Ziffernsektion unter jenen des Ministerium des Äußern als „Beamte des außerordentlichen Dienstes“. Dies stellte einen sichtbareren Beweis der „legalisierten“ Position der Ziffernbeamten dar, die bis 1867 und darüber hinaus, ihre Tätigkeit im Geheimen ausgeübt hatten. [125]

[123] OeStA/HHStA Sammlung 3, Chiffrenwesen, Mappe: Akten im Betreff der Organisierung der Section für Ziffernwesen und translatorischen Arbeiten, 3. Mai 1848–1870, Eidformel, fol 196–199.
[124] OeStA/HHStA Sammlung 3, Chiffrenwesen, Mappe: Akten im Betreff der Organisierung der Section für Ziffernwesen und translatorischen Arbeiten, 3. Mai 1848–1870, Schreiben von Grünne an Schweiger vom 12. Juni 1853, fol 150–151.
[125] OeStA/HHStA Sammlung 3, Chiffrenwesen, Mappe: Akten im Betreff der Organisierung der Section für Ziffernwesen und translatorischen Arbeiten, 3. Mai 1848–1870, Vortrag vom 15. Oktober 1855, fol 182–195.

Einen Einblick in die Qualifikation eines Beamten in der Ziffernsektion, seine Einstellung und seine Tätigkeit gibt der Text des „Unterthänigsten Promemoria“, den Johann Urrisk am 4. November 1863 verfasste und mit einer Kurzbiographie wie folgt beginnt:

> „Ergebenst Gefertigter, absolvierter Jurist, befähigter Richter in Civili, Criminali und in politicis, mehrerer Sprachen kundig, gewesener Referent beim hiesigen Kriminalgerichte, wurde im Jahre 1835 mittelst Dekret zum Offizial der k.k. geheimen Chiffren Cabinett Kanzlei mit dem Range eines Hofsekretärs ernannt und wird bald 37 Jahre seiner Dienstzeit zählen. Gleich am Beginn meiner neuen ämtlichen Thätigkeit habe ich mit besonderer Vorliebe mich dem Chiffren Wesen gewidmet, und da das Interesse dafür sich immer mehr steigerte, so ward mir dieser höchst wichtige Zweig bald zum Bedürfniß – ja zur Leidenschaft geworden. […] Johann Urrisk, k. Rath“[126]

Im weiteren Text verweist Urrisk auf seine Erfolge in der Auflösung „Neapolitanischer Chiffre–Correspondenzen zur verhängnisvollen Zeit des italienischen Krieges“. Mit dem vollständig ausgearbeiteten italienischen Schlüssel konnte er über 2000 Piècen dechiffrieren, darunter sehr viele von hoher Wichtigkeit, auch im Zusammenhang mit „der Katastrophe der Neapolitanischen Königs–Familie, der Entthronung des König Ottos, der darauffolgenden Candidaturen und der Wahl des neuen griechischen Königs, endlich des weltberühmten Fürsten–Congreßes in Frankfurt, etc.“[127] In den wenigen Tagen der Einladung zu diesem hochwichtigen Congreß, in denen sich Otto von Bismarck (1815–1898) vom 3. bis 15. August 1863 in Gastein aufhielt, konnte Urrisk von der Correspondenz des Herren Otto von Bismarck mit dem königlich preußischen Außenministerium in Berlin 82 Piècen dechiffrieren, die seiner Majestät dem Kaiser und seiner Excellenz dem Herrn Grafen von Rechberg vorgelegt wurden. Zu seinen Leistungen zählten besonders die Auflösung und Verfassung des neuen Schlüssels in französischer, italienischer und deutscher Sprache.[128]

Die sprachlichen Anforderungen an die Kandidaten im Aufnahmeverfahren sind einem Bericht vom 25. Juli 1869 an Hofrat Prantner zu entnehmen, in dem die Elaborate der Sprach-Prüfungen von Hauptmann Matscheko vorgelegt wurden. Matscheko hatte vom 12. bis 14. Juli 1869 vier Zeitungsartikel zu übersetzen und zwar, vom Böhmischen ins Englische, vom Polnischen ins Italienische, vom Kroatischen ins Deutsche und vom Englischen ins Französische. Matschenko hatte auch den zweiten Teil der Prüfung, die Auflösung eines einfachen Chiffren–Schlüssels, bestanden.[129]

[126] OeStA/HHStA Sammlung 3, Chiffrenwesen, Mappe: Personalia, Unterthänigstes Promemoria, fol 20–21.
[127] OeStA/HHStA Sammlung 3, Chiffrenwesen, Mappe: Personalia, Unterthänigstes Promemoria, fol 21–22.
[128] OeStA/HHStA Sammlung 3, Chiffrenwesen, Mappe: Personalia, Unterthänigstes Promemoria, fol 33–36.
[129] OeStA/HHStA Sammlung 3, Chiffrenwesen, Mappe: Personalia, Sprachenprüfung, fol 420.

Im Zusammenhang mit dem Krieg 1866 berichtete Cabelli an den Minister des k.k. Hauses und des Äußern, Alexander Graf Mensdorff–Pouilly (1813–1871) in einem Schreiben vom 15. Juli 1866, dass er bereits vor Ausbruch des gegenwärtigen Krieges den Traditionen des Institutes entsprechend, die Vorstände der Filialanstalten angewiesen hatte, beim mindesten Anschein einer Gefahr sämtliche von ihm ausgegangenen Korrespondenz–Stücke und Namenslisten sofort zu vertilgen und die Utensilien in sicheren Gewahrsam zu bringen. Außerdem habe er selbst sämtliche im Institut seit längerem aufbewahrten Interzepte und entbehrliche Papiere verbrannt und vor einigen Tagen den geheimen Dienst, bis auf einen provisorischen Dienst in Wien, gänzlich eingestellt. Einen großen Teil der Akten des Institutes hatte Cobelli mit den Akten des Ministeriums zur Abfahrt nach Ofen verschifft. Sollte die Übersiedelung des Ministeriums des Hauses und des Äußern nach Ofen wirklich stattfinden, so steht in Pest eine geeignete Anstalt mit diplomatischem Schutz zur Verfügung. Die zur Fortsetzung des provisorischen Dienstes unentbehrlichen Akten und Requisiten würde Cobelli in seinen persönlichen sicheren Gewahrsam nach Klosterneuburg nehmen.[130]

Die „Sektion“ (seit 1870 „Departement“) „für Chiffrewesen und translatorische Arbeiten im Ministerium des Äußern“ als Nachfolgeinstitut der „Geheimen Ziffernkanzlei und Zentrale des diplomatischen Zifferndienstes“ hatte schon bei ihrer Einrichtung mit Allerhöchster Entschließung vom 8. Juni 1849 innerhalb des Ministeriums des Äußern eine Sonderstellung eingenommen. Sie war nicht voll in diese Zentralstelle integriert, sondern unterstand dem Ministerium in gleicher Weise wie sämtliche Gesandtschaften und Konsulate im Ausland. Bis 1853 waren der Sektion zunächst folgende Aufgaben zugeteilt: Die Konstruktion der Ziffernschlüssel für die eigene Korrespondenz mit den auswärtigen diplomatischen Vertretungen, das Chiffrieren und Dechiffrieren der Depeschen und Berichte, sowie die Übersetzung von Dienststücken in oder aus den weniger geläufigen Sprachen, wie etwa dem Griechischen, Spanischen, Wallachischen, Schwedischen etc. Das heißt, dass der Aufgabenbereich der Ziffernsektion der gleiche war wie derjenige der alten Ziffernkanzlei, allerdings um die Agenden des ehemaligen Ziffernkabinetts der Staatskanzlei vermehrt und zunächst um die Agenden der geheimen Briefmanipulation vermindert.[131]

[130] OeStA/HHStA Sammlung 3, Chiffrenwesen, Mappe: Akten im Betreff der Organisierung der Section für Ziffernwesen und translatorischen Arbeiten, 3. Mai 1848–1870, Schreiben vom 15. Juli 1866, fol 256-257.
[131] *Hubatschke*, Ferdinand Prantner, Buch 6, Diss., 1383f.

Die Referatseinteilung des Ministeriums des Äußern erfuhr seit 1849 nicht weniger als fünf Änderungen. Anlässlich der fünften Änderung im Jahre 1867 wurden, nachdem die geheime Briefüberwachung eingestellt worden war, die „Angelegenheiten für Chiffre– und translatorische Arbeiten“ als achtes Ressort des Departements K installiert. Die Einteilung von 1868 sah zwei Sektionen vor, in deren zweiter neun Departements bestanden. Innerhalb des Departements 2 befanden sich die „Angelegenheiten für Chiffre- und translatorische Arbeiten“. Im Jahr 1872 wurden die Einteilung nach „Geschäftsgruppen“ vorgenommen und innerhalb der Geschäftsgruppe II, Abteilung B war das „Departement für Chiffre– und translatorische Arbeiten“ nunmehr als Departement VI eingeteilt. Nach der Einteilung von 1877 bestand das Chiffredepartement als Unterabteilung der Geschäftsgruppe I, der Präsidialsektion, und nach der Einteilung von 1882 war es an die zehn Departements für administrative Angelegenheiten angeschlossen; 1909 wurde es als Departement 13 fest installiert. Das Chiffren–Departement hatte den translatorischen Dienst nicht mehr zu versehen; dafür existierte nun ein eigenes „Übersetzungsbüro“ als Departement 14. Das Chiffredepartment blieb als Departement 13 bis 1918 bestehen.[132]

[132] *Hubatschke*, Ferdinand Prantner, Buch 6, Diss., 1393–1395.

4 Presse und Geheimdienst im Neo–Absolutismus

Kurz nach der Niederschlagung der Revolution in Wien konnte man den regierungs–unfähigen Kaiser Ferdinand (1793–1871) dazu bewegen, abzudanken. Ihm wäre nach der Thronfolge–Ordnung Franz Josephs Vater, Franz Karl (1802–1878), gefolgt, der aber zu Gunsten seines Sohnes auf die Krone verzichtete. So konnte am 2. Dezember 1848 in Olmütz/Olomouc der damals 18-jährige Franz Joseph (1830–1916) den Thron der Habsburgermonarchie besteigen. Seine Macht stützte sich zunächst auf die Armee, die die äußeren und inneren Feinde besiegt hatte. Radetzky (1766–1858) war es gelungen, den Angriff Sardinien–Piemonts zurückzuschlagen, und Windischgrätz (1787–1862) und Jellačić (1801–1859) hatten die Wiener Revolution besiegt. Die endgültige Festigung des Systems des Neoabsolutismus erfolgte allerdings erst nach der Niederschlagung der ungarischen Revolution in Világos. Am 7. März 1849 kam es zur Auflösung des Reichstages, der in der Endphase des Kampfes um Wien nach Kremsier/Kroměřiž in Mähren übersiedelt war, und zur Verhaftung von Abgeordneten. Die vom Reichstag ausgearbeitete sogenannte Kremsierer Verfassung trat nie in Kraft, doch nahm die am 7. März 1849 publizierte oktroyierte Verfassung einige Gedanken davon auf. Diese Konstitution bedeutete allerdings niemals mehr als ein formal gültiges Dokument, das bereits mit dem Silvesterpatent 1851 wieder aufgehoben wurde. Der Schwenk zum Absolutismus war damit vollzogen.[133]

Die Führung dieser neuen Politik lag in den Händen eines neuen Politiker–„Teams“, an dessen Spitze Ministerpräsident Fürst Felix Schwarzenberg (1800–1852) stand. Das Hauptproblem bildete die Situation in Ungarn, wo die Revolution am radikalsten war. Nach der Niederlage der ungarischen Revolutionäre bei Világos übte der militärische Oberbefehlshaber und General-Gouverneur Julius Jakob Freiherr von Haynau (1786–1853) Vergeltung für die Absicht der Eigenständigkeit an den Aufständischen, die im Land geblieben sind.[134]

Die geheime Überwachung und Verfolgung der ungarischen Emigranten hingegen wurde Alexander von Bach übertragen, dem unter der Schirmherrschaft Schwarzenbergs die Polizei als ein dem Innenministerium unterstelltes Organ zugeteilt wurde. Die ungarischen

[133] Karl *Vocelka*, Geschichte Österreichs: Kultur-Gesellschaft-Politik. Der Neoabsolutismus. (Graz/Wien/Köln 2000; Heyne Taschenbuch, München ^{5}2002) 206.
[134] *Vocelka*, Geschichte Österreichs, 207f.

Revolutionäre, die ins Ausland geflüchtet waren, hätte man schwerlich durch die Berufsdiplomaten überwachen lassen können.[135]

4.1 Telegraphie, Diplomatie und Pressepolitik

Nach der Liberalisierung des Pressegesetzes durch „die Erklärung der Aufhebung der Censur in allen Staaten, wo sie besteht“[136] durch Kaiser Ferdinand I. am 15. März 1848, musste die staatliche Macht der politischen Öffentlichkeit, der „öffentlichen Meinung“ Rechnung tragen. Die Presse und die öffentliche Meinung sind zu einem Faktor des politischen Kalküls geworden, und konnten die verantwortlichen Staatsmänner nach 1848 nicht mehr wie bisher von Entscheidungsprozessen ausschließen. Das spätere zweifache Anwendungsschema staatlicher Pressepolitik, diplomatisches Vorgehen nachträglich öffentlich zu rechtfertigen oder im Vorhinein die Presse zu beeinflussen, um Regierungsintensionen zu realisieren, kam noch nicht zur Geltung.[137]

Viele Zeitungen, die vor allem im Abonnement vertrieben worden waren, wurden durch die plötzliche Abschaffung der Zensur während des Revolutionsjahres auch auf der Straße verkauft. Weil die Zeitungen wesentlich mehr Menschen erreichten, übten sie auch einen bedeutend größeren Einfluss auf die öffentliche Meinung aus, als die verschiedenen Gesellschaften oder Vereine, womit sie sich einen öffentlichen Raum schufen.[138] Diesen Raum, den die Presse öffnete, konnte man zugleich auch als neue Ebene gesellschaftlicher Selbstreflexion verstehen. Die Zeitung installierte den Leser als politisch mündiges Subjekt und versuchte, ihn zunehmend für eigene Zwecke zu mobilisieren.[139] Die Blätter scheuten aber nicht davor zurück, Gerüchte zu verbreiten oder sogar schamlose Verunglimpfungen bekannter Persönlichkeiten abzudrucken. Es dauerte auch nicht lange, bis die Regierung ein Pressegesetz entwarf, um auf den Inhalt der Zeitungen einwirken zu können.[140]

Ein entsprechendes Gesetz, das Kaiserliche Patent vom 14. März 1949, das gegen den Missbrauch der Presse erlassen wurde und das Verfahren in „Preß–Übertretungsfällen“ festgesetzt hatte, lautete wie folgt:[141]

---

[135] *Frank*, Ein Diener seiner Herren, 45.
[136] Allerhöchstes Patent vom 15. März 1848. Verleihung der Constitution und Aufhebung der Censurgesetze. Online unter: <http://alex.onb.ac.at/cgi-content/alex?aid=pgs&datum=1848&page=88&size=45> (17. Oktober 2017).
[137] *Kammerhofer*, Diplomatie und Pressepolitik 1848-1918, 460.
[138] *Judson*, Habsburg, 241.
[139] *Osterhammel*, Die Verwandlung der Welt, 64.
[140] *Judson*, Habsburg, 241.
[141] OeStA/AVA Nachlässe AN Bach, Karton 28, Pressewesen, fol 00014.

„Wir Franz Josef der Erste
von Gottes Gnaden Kaiser von Oesterreich; König von Ungarn und Böhmen, König der Lombardei und Venedigs, […] etc, etc.

Haben in Erwägung, daß in Folge Unseres Patentes vom 13. März 1849 gegen den Mißbrauch der Presse auch die bestehenden Vorschriften über das Verfahren in Preßsachen einer Revision unterzogen werden mußten, nach Maßgabe des § 120 der Reichsverfassung auf den Antrag Unseres Ministerrathes zu verordnen beschlossen, und verordnen, wie folgt:

Art. 1

Vom Tage der Kundmachung dieses Patentes ist sich in allen Kronländern, für welche Unser Patent vom 13. März 1849 gegen den Mißbrauch der Presse erlassen wurde, hinsichtlich des Verfahrens in Preß-Übertretungsfällen nach der beifolgenden, von Unserem Ministerrathe am heutigen Tage vollzogenen Vorschrift zu benehmen.

Art. 2

Von demselben Zeitpunkte an tritt die provisorische Verordnung vom 18. Mai 1848 über das Verfahren in Preßsachen außer Wirksamkeit.

Art. 3

Unser Minister des Inneren und der Justiz sind mit dem Vollzuge dieses Patentes beauftragt.

Gegeben in unserer königlichen Hauptstadt Olmütz den vierzehnten März des Jahres Eintausend Achthundert neun und vierzig.

Franz Josef m.p.

L.S.

Schwarzenberg m.p. Stadion m.p. Krauß m.p. Bach m.p. Cordon m.p. Bruck m.p. Thinnfeld m.p. Kulmer m.p.“ [142]

Der Tradition absolutistischer Auffassungen einer „negativen“ Pressepolitik fühlten sich die amtlichen Pressestellen (Pressleitungscomitee 1852 und Pressleitungsbureau 1860) weitgehend verpflichtet. Bis zur innenpolitischen Trendwende anfangs der 60er Jahre des 19. Jahrhunderts überwogen repressive, polizeistaatliche Methoden in der Handhabung der Presse. Reglementierung, Überwachung und präventives Verbot regierungsfeindlicher politischer Öffentlichkeit ersetzten fast zur Gänze „positive“ pressepolitische Maßnahmen.[143]

Im Ausland war die Pressearbeit den Konsulaten und Botschaften zugeordnet. Autorisierte Presse–Korrespondenz wurde von Wien ausgehend in chiffrierter Form über die diplomatischen Dienste im Ausland den Redaktionen folgender Zeitungen regelmäßig zur Veröffentlichung zugeleitet: „Risorgimento“ in Turin, „Merkur“ in Altona, „Schlesische Zeitung“ in Breslau, „Postzeitung“ in Augsburg, „Breslauer Zeitung“ in Breslau, „Conservative Zeitung für Schlesien“ in Breslau, „Magdeburgische Zeitung“ in Magdeburg, „Deutsche allgemeine Zeitung“ in Leipzig, „Allgemeine Zeitung“ in Augsburg, „Oberpostamtszeitung“ in Frankfurt, „Correspondent“ in Hamburg, „Deutsche Volkshalle“ in

[142] OeStA/AVA Nachlässe AN Bach, Karton 28, Pressewesen, fol 00014.
[143] *Kammerhofer*, Diplomatie und Pressepolitik 1848-1918, 460f.

Köln, „Börsenhalle“ in Hamburg, „Correspondent“ in Nürnberg, „Schwäbischer Merkur“ in Stuttgart und „für sämtliche Berliner Blätter“ Wolff in Berlin.[144]

Die Diplomaten reagierten unterschiedlich auf die telegraphische Kommunikation, deren Depeschen im Vergleich zu Briefen kurz und vor allem schnell waren. Manche begrüßten die verstärkte Anbindung an eine zentrale Führung und andere widersetzten sich der telegraphischen Kommunikation. Die Erhöhung der zentralen Steuerung hatte eine profunde Auswirkung auf die Diplomaten. Mit dem Aufkommen der telegraphischen Übermittlung war das Zeitalter der großen Botschafter, welche notgedrungener Weise Politikmacher waren, vorbei. Früher konnten Botschafter eine Hauptrolle, vielleicht sogar eine entscheidende Rolle in internationalen Krisen spielen.[145]

Während der zweiten Hälfte des 19. Jahrhunderts wurden die Zeitungen und die Regierungen in gleicher Weise vom Kartell der vier neuen Agenturen wie *Reuters*, *Havas*, *Wolff* und der *Associated Press* abhängig, die den globalen Informationsfluss steuerten. Das Vertrauen der Agenturen in das globale Telegraphennetz beeinflusste die Art des Nachrichtenflusses und sie gestalteten damit das Grundprinzip der Verwendung des Netzwerkes. Wichtige Neuigkeiten bewegten sich entlang der Telegraphenlinien, und wo solche Linien waren, da waren auch die letzten Nachrichten verfügbar. Mit Hilfe der telegraphischen Aussendungen konnten geographische Peripherien zu Informationszentren werden und umgekehrt. Die Vereinigung der Verteilung der Informationen mit der Telegraphie leistete einen signifikanten Beitrag zur weiteren Umwandlung des globalen Raumes.[146] Reuters hatten enge Kontakte sowohl zur Britischen Regierung als auch zu führenden Kabel–Unternehmen. Reuters wurde daher zu Recht als eine „halb–offizielle Institution“ des Britischen Imperiums bezeichnet. Dementsprechend wurde der Fluss der telegraphischen Übermittlung von Nachrichten nicht nur mit der Struktur des Kabel–Netzwerkes sondern auch mit der imperialen Politik verbunden.[147]

Neben einem weitgefächerten publizistischen Instrumentarium im In– und Ausland leisteten Telegraphenagenturen, Depeschen– und Korrespondenzbüros bei der Flankierung der

[144] OeStA/AVA Nachlässe AN Bach, Karton 28, Pressewesen, fol 00008.
[145] David Paul *Nickles*, Under the Wire. How the Telegraph Changed Diplomacy. Diplomatic Autonomy and Telecommunications (Cambridge/Mass. & London/England 2003) 34.
[146] Roland *Wenzlhuemer*, Connecting the Nineteenth–Century World: The Telegraph and Globalization (Cambridge 2013) 91.
[147] *Wenzlhuemer*, Connecting the Nineteenth–Century World, 91.

österreichisch–ungarischen Außenpolitik wertvolle Dienste. Das 1860 gegründete „k. k. Telegraphen–Korrespondenz-Bureau“, das 1882 personell und administrativ dem Ministerratspräsidium unterstellt worden war, und die „Politische Korrespondenz“, die 1875 der „Österreichischen Korrespondenz“ nachfolgte, gehörte durch die leichte Lenkbarkeit und ihren großen Wirkungskreis zu den wesentlichsten und mächtigen Organen der Regierungs–Pressepolitik. Die Abhängigkeit der österreichischen Agentur, die nahezu gleichberechtigt neben den großen europäischen Agenturen Wolff, Reuters und Havas, gemeinsam mit der *Correspondance Havas* den telegraphischen Dienst für Rumänien, Bulgarien und die Türkei verrichtete, lag seit Beginn offen zutage. Dies gestattete den Wiener Zentralbehörden, das *k.k. Telegraphen-Korrespondenz-Bureau,* ohne die sonst üblichen Vorbehalte und Rücksicht–nahmen, als einzige autorisierte Informationsquelle für die auswärtige Politik der Monarchie in den Dienst ihrer Diplomatie und Propaganda zu stellen. Die Vorteile dieser Monopolstellung überwogen die Nachteile der Schwerfälligkeit der Nachrichtenübermittlung bzw. der Tatsache, dass die Meldungen offiziösen und offiziellen Charakter hatten.[148]

Nach der Gründung des Deutschen Reiches und mit der Ernennung von Gyula Graf Andrassy (1823–1890) zum Außenminister der Doppelmonarchie änderten sich in den 1870er Jahren Zielrichtung der auswärtigen Diplomatie ebenso wie Stellenwert und Arbeitsweise der Presse–Außenpolitik. Die bedingungslose Unterordnung der Regierungspresse zur Unterstützung der diplo–matischen Vorgänge blieb das Hauptanliegen Andrassys, ansonsten huldigte er gemeinsam mit dem Kaiser dem Prinzip, Diplomatie von „politischer Öffentlichkeit“ oder gar öffentlicher Kritik in Presse und Parlament so weit als möglich fernzuhalten. Andrassy betonte 1876 gegenüber dem Monarchen, „dass die Haltung der Blätter zwar nicht angenehm sei, jedenfalls aber die Freiheit unserer Entschließungen in keiner Weise beeinträchtigen kann.“[149]

4.2 Netzwerk der Agenten

Am Beginn der Regierungszeit Franz Josephs erreichte die Revolution in Ungarn ihren Höhepunkt, als sich Ungarn am 14. April 1849 beim Reichstag in Debrecen für unabhängig erklärte, das Haus Habsburg–Lothringen vom Throne Ungarns verstoßen und Kossuth zum Präsidialregenten Ungarns ausgerufen hatte. Nach diesen Erklärungen verbündete sich das konservative zaristische Russland mit Franz Joseph, und mit russischer Militärhilfe wurde

[148] *Kammerhofer*, Diplomatie und Pressepolitik 1848-1918, 464.
[149] *Kammerhofer*, Diplomatie und Pressepolitik 1848-1918, 476.

Ungarn am 13. August 1849 bei Világos (heute Şiria in Rumänien) besiegt. Die Regierung vertrat die sogenannte „Verwirkungstheorie“, das heißt die Anschauung, dass die Ungarn durch ihr Verhalten alle bisherigen Privilegien und Rechte verloren hatten. Kossuth und vielen anderen Revolutionären gelang die Flucht ins osmanische Reich.[150]

Alexander von Bach betonte die große Wichtigkeit der Beobachtung und geheimen Verfolgung der Emigranten und wollte eine internationale Organisation gegen die revolutionären Machinationen ins Leben rufen. Die politisch–ideologische sowie persönliche Zielsetzung Bachs war die entsprechende Dramatisierung des weltweiten Kampfes zwischen Ordnung und Anarchie. Die Gefahr von Seiten der „Umsturzpartei“ veranlasste Bach, seinen Geheimdienst als den einzigen Schutzwall gegen die „drohende Anarchie“ darzustellen.[151] Unmittelbar nach der Kapitulation bei Világos und der Flucht vieler tausender ungarischer Freiheitskämpfer nach Süden, in die Türkei, begann Bach sofort mit dem Ausbau seines sich über mehrere Länder erstreckenden Agentennetzes. Seine Leute nahmen gleich die Spur der Flüchtlinge auf, da Bach fürchtete, dass diese einen neuen Aufruhr anzetteln würden.[152] Seine Agenten schickten ihre Berichte meistens an Wiener Adressen und der Innenminister fertigte dann daraus für den jungen Kaiser Franz Joseph seinen politischen Wochenbericht an. In den Ministerratssitzungen unterstrich Bach fallweise die Bedeutung seiner Berichte dadurch, dass er Auszüge aus den Originaltexten der Agenten vorlas. Dem aus dem Brief von Ujházy zitierenden Bach antwortete Fürst Schwarzenberg, indem er aus den Briefen von Szemere vorlas. [153]

Der Innenminister errichtete sein internationales Kontrollsystem hauptsächlich in der Türkei. Während in den größten europäischen Zentralen zwei bis drei Konfidenten die Emigranten beobachteten, wurden in der Türkei die Flüchtlinge im Sommer der Jahres 1850 bereits von sechzehn Agenten beschattet. Das Innenministerium unterschied zwischen *direkt verwendeten* und *indirekt verwendeten* Agenten. Die Agenten der ersten Kategorie kannten das Ziel und den Charakter ihrer Beschäftigung sowie die Quelle ihres Gehaltes, während den Agenten der zweiten Kategorie die Zusammenhänge verborgen blieben und über Verbindungsleute in die Organisation einbezogen wurden.[154]

[150] *Vocelka*, Geschichte Österreichs, 204f.
[151] *Frank*, Ein Diener seiner Herren, 45.
[152] *Frank*, Ein Diener seiner Herren, 43.
[153] *Frank*, Ein Diener seiner Herren, 46.
[154] *Frank*, Ein Diener seiner Herren, 46.

Nach Einrichtung der Organisation des außerordentlichen Dienstes im Orient ergaben sich Anfang Juni 1850 folgende Agenturen:

„I.in Paris: 1º Dr. Schaefer, als Leiter einer Loge, in vielfachen Verbindungen mit der Schweiz, mit England, Belgien, Deutschland und den Départemens stehend.
2º L……. (: aus Kurhessen :), als Functionaire der Pariser Polizei-Préfecture und habitué der Flüchtlings-Foyers, besonders gut unterrichtet.
3º Der Pole Paul C….. für die polnische Emigration.
II.in London:4º Dr. Beer, für die ungarische Emigration.
5º Moor für die ungar. Emigration (: mobil :)
III.in der Schweiz: 6º Dr. Berg, für die oestliche Schweiz.
7º Dr. J. aus Dresden, dermalen in Zürich (: als mobiles Organ verwendet :)
8º Der Pole Sarma, in Genf.
IV.in Piemont: 9º Der Pole Lowski, für Turin, unter dessen Leitung ein Ungar in Genua und ein Italiener im Kanton Tessin verwendet werden.
V.in Deutschland: 10º Dr. Herrmann in Frankfurt;
11º Der Vermittler daselbst;
12º Der Turner Heller für Mannheim;
13º Der Korrespontent in Mainz;
14º J. B…ring, eben in Stuttgart (: mobil :);
15º Dr. Lorenz in Leipzig; hat Verbindungen in der Schweiz und in Amerika;
16º Dr. Wilhelm in Augsburg, steht mit der Schweiz, mit Würtemberg und vielen Punkten Deutschlands in Verbindung.
17º Arnold für Berlin, Breslau und Krakau; unterhält Verbindungen mit Brüssel.
Agenturen im Orient:
In Constantinopel: 18º Zeichner Δ (: der Leiter des Dienstes :); 19º Ali; 20º Murat;
Für Kintahia: 21º Mehmed; 22º Abdula;
Für Aleppo: 23º Der Renegat Carabet;
Für Smyrna: 24º Mohamed;
Für Syra: 25º Said;
Für Athen: 26º Kiamil;
Für Corfu: 27º Haffiz;
Für Schumla: 28º Ahmed;
Für Toultscha: 29º Suleiman;
Für Gallatz: 30º Ismael;
Für Bukarest: 31º Mustafa;
Für Belgrad: 32º Perisi; 33º Ressy (: mobil :) haben Verbindungen mit Constantinopel, Kintahia, Widdin, Turin, Paris und den k.k. Staaten.“[155]

In der Reihe der „politischen Wochenberichte“ verfertigte Minister von Bach selbst im Februar 1851 einen Bericht, in dem er die Geschichte, die Struktur, die Arbeitsprinzipien und die praktische Tätigkeit der „staatspolizeilichen Sektion“ des Innenministeriums erörterte. Er hob hervor, dass „wir einen Teil der Revolutionspartei, auch ohne dass sie es wüssten, für

[155] OeStA/AVA Nachläse, AN Bach, Karton 26, fol 169-170.

unsere Zwecke verwenden. Auch im Orient ist dieses Netz indirekt ausgedehnt; seine Zentrale ist in Wien. Wir stehen so in Verbindung mit den leitenden Gestalten der Emigration. […] Alle Berichte kommen schließlich in die Central–Section, die unter meiner Leitung steht. Die Leitung wird von hier planmäßig und einheitlich vorgenommen. Was wir geleistet haben, zeigen die Wochenberichte, die zahlreichen größeren Memoriale, die mehr als 500 Akten mit staatspolizeilichem Inhalt (abgesehen von den mehr als 4.000 Gestionen der Section), die die Behörden innerhalb und außerhalb unserer Grenzen vor den Gefahren warnen."[156]

Bach zählte die Ergebnisse der Arbeit des Agentennetzes der Reihe nach auf und zeigte sich stolz auf seine Erfolge. Dazu gehören die Verminderung der Anzahl der revolutionären Emigranten, das »Aufhalten« der ausländischen „sozialdemokratischen" Strömungen, die Vereitelung der Versuche, Kossuth in ein anderes Land zu bringen und die Kontrolle von gefährlichen Privatbriefen. Bach sprach auch von der „initiierenden und kontrollierenden Rolle", die seine Agenten beim Heimkehren von Emigranten spielen und behauptete, dass seine Leute „die Heimkehrer und Verdächtigen" unter Kontrolle halten.[157]

Aus dem Wesen des Geheimdienstes von Alexander von Bach ergab sich, dass sich die Beteiligten einander nicht kannten. Sie wussten nicht, wer außer ihnen noch Mitglied der Organisation war. Alle informierten sich über alle und erstatteten Bericht über alle, wodurch sich der Geheimdienst in erster Linie selbst beobachtete. Die Agenten informierten Bach übereinander, aber auch über die Berufsdiplomaten, und das Außenministerium bezog seine Informationen auf offiziellen Wegen über dieselben Agenten und Diplomaten. Dies fand nicht nur auf den unteren Ebenen der Organisation statt. Der Innenminister und ab 1852 der Chef der obersten Polizeibehörde, Baron Kempen, ließ selbst die Minister beobachten und erstattete notfalls dem Kaiser Bericht.[158]

Eine gegenseitige Überwachung der Agenten und Diplomaten und die verschiedenen, zum Teil gegensätzlichen Zitate aus Berichten, die Fürst Schwarzenberg bzw. Minister von Bach in Ministerratssitzungen vorbrachten, sowie die wiederholte Betonung Bachs, dass alle Berichte seiner Agenten in die „Central–Section" des Innenministeriums kommen, von wo aus auch alle Aktionen unter seiner Leitung geplant werden, lassen darauf schließen, dass diese „Central-Section" im Innenministerium über eine eigene Chiffrierabteilung verfügte,

[156] *Frank*, Ein Diener seiner Herren, 46.
[157] *Frank*, Ein Diener seiner Herren, 46f.
[158] *Frank*, Ein Diener seiner Herren, 48.

falls die Agenten chiffrierte Berichte verfertigten. Es finden sich in der „Ziffernsektion“ des Außenamtes keine Hinweise darauf, dass Berichte der Agenten des Innenministeriums dechiffriert oder Briefe aus der „Central–Section“ chiffriert abgesandt wurden.

Aus Briefen von Hofrat von Schweiger an den Generaladjudant des Kaisers, Graf Grünne vom 19. November 1857 bzw. 10. Juni 1858 geht lediglich hervor, dass die wichtigen Mitglieder der so genannten „altkonservativen Partei“ in Ungarn weiterhin einer permanenten scharfen Briefüberwachung unterworfen wurden, die Schweiger immer wieder forcierte. Als Zugehörige zu den Altkonservativen wurden eine Witwe in Wien, ein Oberbaurat der Eisenbahn, ein Buchhändler in Parma und ein Wiener Mittelschullehrer verdächtigt, weil sie Verbindungen mit verschiedenen ausländischen Journalen unterhielten.[159]

Die Beobachtung der Revolutionäre konzentrierte sich am Ende der 1850er Jahre auf die heimgekehrten Emigranten in Ungarn. Bei einem Sieg der italienischen und der ungarischen Aufständischen 1848 wäre das Habsburgerreich als Vielvölkerstaat zerfallen. Aus globaler Sicht blieb die größte europäische Revolutionsbewegung zwischen 1789 und 1917 wenig beachtet. Wichtig war die Emigration über den Atlantik. Die Vereinigten Staaten nahmen flüchtige „Achtundvierziger“ gerne auf. Lajos Kossuth gelangte letztlich über das Osmanische Reich Ende 1851 in die USA und wurde dort als Held gefeiert. Kaiser Franz Joseph begnadigte Kossuth 1867, der aber bis zu seinem Tode im italienischen Exil lebte.[160]

[159] *Hubatschke*, Ferdinand Prantner, Buch 6, Diss., 1372.
[160] *Osterhammel*, Die Verwandlung der Welt, 781.

5 Technische und organisatorische Entwicklungen im 19. Jahrhundert

Die technischen Entwicklungen des 19. Jahrhunderts haben die Welt in einer Weise verkleinert, für die kein früheres Beispiel in der Geschichte aufzuweisen ist. Der Güter– und Personenverkehr ließ Entfernungen schrumpfen und ermöglichte den Menschen intensiv miteinander zu kommunizieren. So konnten sich Netzwerke bilden, innerhalb derer der Transfer von technischen Innovationen stattfinden konnte, die an Kommunikation gebunden waren.[161] Diese Entwicklung bewirkte das Schrumpfen von Zeit und Raum infolge der Revolution im Kommunikations– und Verkehrswesen und die damit verbundene Beschleunigung der Mobilität von Menschen, Gütern und Ideen. Die Kompression von Zeit und Raum brachte immer mehr Menschen in persönlichen oder zumindest virtuellen Kontakt miteinander. Der beschleunigte Güterverkehr wirkte sich auch auf die Dauer der Übermittlung von Briefen und Depeschen aus, soweit diese nicht aus Sicherheitsgründen mit eigenen Kurieren befördert wurden.[162] In erster Linie war es die Schifffahrt, da sie für die Verbindung der durch die Meere getrennten Weltteile das einzige in Betracht kommende Mittel bildete. Als Benjamin Franklin (1706–1790) im Jahre 1775 seine erste Reise von Amerika nach Europa machte, brauchte er noch 42 Tage für die Durchquerung des Ozeans. Im Jahre 1819 benötigte die „Savannah“, das erste Dampfschiff, welches die Fluten des Ozeans durchquerte, 26 Tage für die Überfahrt. Um 1900 war ein Schnelldampfer kaum mehr als fünf Tage für die gleiche Strecke unterwegs.[163]

Noch umfangreicher und für die Zunahme des internationalen Verkehrs am Festland wichtig war die Entwicklung, die das Eisenbahnwesen eingeschlagen hatte. Die Eisenbahn–Gesellschaften, die Mitte des 19. Jahrhunderts in großer Zahl entstanden, benötigten für ihre eigene Signaltechnik schnellere Übertragungsgeschwindigkeiten, als dies eine materielle Übermittlung ermöglichte. Informationen über Abfahrtszeiten, Verspätungen und technische Defekte mussten den Zügen auf meist eingleisigen Eisenbahnlinien vorauseilen. Ohne verlässliche Kommunikation über die Bewegung und den Aufenthalt der Züge, wäre eine sichere und wirtschaftliche Benützung der eingleisigen Eisenbahnlinie in beiden Richtungen nur schwer möglich gewesen.[164]

---

[161] Jürgen *Mirow*, Weltgeschichte (München 2009) 60.
[162] Emily *Rosenberg*, Einleitung. In: Emily *Rosenberg* (Hg.), Weltmärkte und Weltkriege, 1870–1945 (München 2012) 9–32, hier 13.
[163] Alfred Hermann *Fried*, Das internationale Leben der Gegenwart (Wien/Berlin 1908) 2.
[164] *Wenzlhuemer*, Connecting the Nineteenth–Century World, 31.

5.1 Informationswege durch Post, Telegraphie und Telephon

Die Zunahme der Kommunikation der Menschen in der Entwicklung des Postwesens ist nicht nur dem Briefverkehr, sondern auch dem telegraphischen und telephonischen Verkehr zuzuschreiben. Ein großer Aufschwung des Briefverkehrs trat nach Reformen von Rowland Hill (1795–1879) um die Mitte des 19. Jahrhunderts in England ein, mit denen kostengünstige, vorauszahlbare und einheitliche Portosätze eingeführt wurden. Der General-postdirektor des Deutschen Reichs, Heinrich von Stephan (1831–1897), auf dessen Antrag für den deutschen Postverkehr einheitliche Standards unter Bismarck eingeführt wurden, bemühte sich daraufhin um die Einrichtung einer internationalen Post–Organisation. Im Jahre 1874 trafen die europäischen Nationen, die Vereinigten Staaten, Russland, die Türkei und Ägypten ein Abkommen, innerhalb einer gemeinsamen Postvereinigung zusammenzuarbeiten. Wenige Jahre später schlossen sich Japan, Brasilien, Persien und viele europäische Kolonien an, bis der Union alle Länder der Erde angehörten. Briefmarken aller Mitgliedsstaaten waren für alle internationalen Beförderungswege gültig. Die Ausbreitung des einheitlichen globalen Postsystems durch die „Universal Postal Union“ (UPU, Weltpostverein) förderte auch die Alphabetisierung und das Briefeschreiben.[165]

Das europäische Postsystem hatte bereits einen hohen Grad an Schnelligkeit und Leistungsfähigkeit erreicht. Nun zeigte aber der Telegraph seine Möglichkeit für eine noch schnellere Informationsübertragung und es stellt sich die Frage, ob der Telegraph den Entwicklungsprozess, der Dekaden vorher eingesetzt hatte, beschleunigte, oder ob die Telegraphie eine qualitative Änderung der Entwicklung auslöste.[166]

Im dritten Quartal des 19. Jahrhunderts begann mit der Verkabelung der Welt die Zeitepoche der Telegraphie, die mehrere Jahrzehnte andauerte, bis das Telephonieren über längere Strecken erschwinglich wurde. Die Welt war um die Mitte der 1880er Jahre bereits mit so vielen Kabeln durchzogen, dass jede mittlere Stadt in Europa und in Nordamerika ihr Telegraphenamt besaß. Das große Medium mit globalisierender Wirkung war im 19. Jahrhundert der Telegraph, nicht das Telephon. Das Telephon begann seine Geschichte erst drei Jahrzehnte später mit der Eröffnung erster Vermittlungszentralen in New York 1877 bis 1878 und in Paris 1879. Mit der anfänglichen Telephon–Technologie erreichte man nur eine

[165] Emily *Rosenberg*, Transnationale Strömungen in einer Welt, die zusammenrückt. In: Emily Rosenberg (Hg.), Weltmärkte und Weltkriege, 1870–1945 (München 2012) 815–998, hier 829f.
[166] *Wenzlhuemer*, Connecting the Nineteenth–Century World, 30.

begrenzte Reichweite innerhalb einer Stadt. Die Möglichkeiten der Telephon–Kommunikation verbesserten sich erst in den 1880er und 1890er Jahren und erlebten eine rasche Entwicklung nach 1900. Obwohl der Telegraph das Leben von Privatpersonen weniger revolutioniert hatte als später das Telephon, so war er doch für Geschäft, Militär und Politik von großer Bedeutung.[167]

5.2 Die Entwicklung der Konstruktion der Telegraphie–Geräte

Die Einführung der elektromagnetischen Signalübertragung wurde erst durch eine Reihe von Entdeckungen und Erfindungen technisch möglich. Bekannte Namen großer Erfinder täuschen darüber hinweg, dass der Innovationsprozess bis zur elektromagnetischen Telegraphie nicht aus einer großen Idee bestand, sondern aus vielen kleinen Schritten, die aufeinander aufbauten.[168] Nach der Entdeckung des Elektromagnetismus von Hans Christian Ørsted (1777–1851) 1819 in Kiel war eine der Voraussetzungen für die elektromagnetische Telegraphie gegeben. Der Franzose André-Marie Ampère (1775–1836) entwickelte 1820 einen elektromagnetischen Telegraphen, der nach dem Nadelprinzip arbeitete. Eine Nadel wurde durch ein elektromagnetisches Feld nach links oder rechts bewegt. Diese Methode war aber unwirtschaftlich und nicht anwendbar, da sie für eine Übertragung über die Entfernung von einem Kilometer 60 Kilometer Draht benötigte. Gemeinsam mit seinem Göttinger Physikerkollegen Wilhelm Eduard Weber (1804–1891) führte Johann Carl Friedrich Gauß (1777–1855) 1833 ein bahnbrechendes Experiment durch. Gauß und Weber verbanden die örtliche Sternwarte mit dem nahe gelegenen physikalischen Institut mit Drähten und erzeugten durch magnetische Induktionsspulen unterschiedliche Spannungspulse, die die Kompassnadeln an den beiden Enden der Drähte synchron ausrichteten. Diese Methode arbeitete nach einem ähnlichen Prinzip wie Ørsted, benötigte jedoch nur zwei Drähte. Die Leitung diente den beiden Forschern zur Kommunikation, die Idee wurde aber aus rein wissenschaftlichem Interesse nicht vermarktet. Von Gauß und Weber stammt die Idee, die Leitungen an hohen Masten oder über die Dächer der Häuser zu verlegen.[169]

---

[167] Jürgen *Osterhammel*, Die Verwandlung der Welt. Eine Geschichte des 19. Jahrhunderts (Sonderausgabe, München ^{2}2016) 1023f.
[168] Jürgen *Mirow*, Weltgeschichte. Entwicklungsdynamik durch die Entstehung von Innovationen (München 2009) 48.
[169] Magdalena *Kersting*, Sammlung und Physikalisches Museum. Der Gauß–Weber–Telegraf. Fakultät für Physik, Universität Göttingen (Göttingen 2012/13) 6. Online unter: <https://www.uni-goettingen.de/document/> (20. März 2017)

In den ersten Tagen der Telegraphie existierten verschiedene Systeme nebeneinander. Das Grundprinzip war einfach. Ein Apparat bestand aus einer galvanischen Batterie, einem Unterbrecher und einer Vorrichtung zur Anzeige oder Aufzeichnung, wenn der elektrische Kreislauf geschlossen war oder anders gesagt, es sichtbar zu machen, wenn die Energie der Batterie fließen konnte.[170]

5.2.1 Nadel–Telegraph von Cooke und Wheatstone

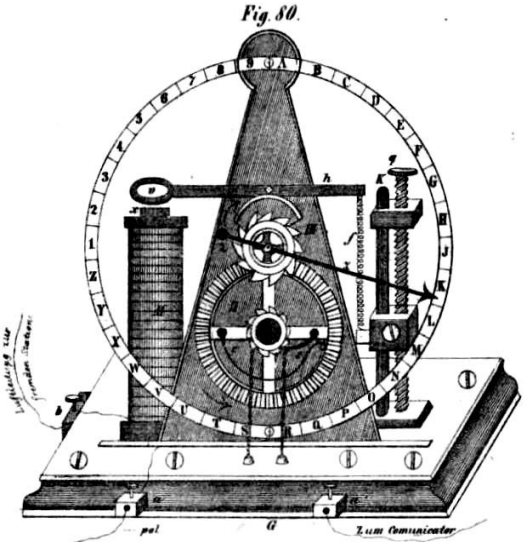
In England erfanden 1837 die beiden Physiker Charles Wheatstone (1802–1875) und William Fothergill Cooke (1806–1879) einen Nadeltelegraphen in Form einer Raute, auf der der Schnittpunkt zweier Nadeln den gewünschten Buchstaben anzeigte. Am Apparat auf der Empfangsseite waren die Nadeln auf einer horizontalen Achse nebeneinander angeordnet, die ohne Signal senkrecht standen. Zur Übertragung eines Buchstaben wurden an zwei Drähten Spannungen angelegt, die die zwei Nadeln so auslenkten, dass an deren Kreuzungspunkt der gewünschte Buchstabe des Alphabets abgelesen werden konnte. Der sogenannte Fünf–Nadel–Telegraph hatte den Vorteil, dass Nachrichten ohne Kenntnis eines Codes gesendet und empfangen werden konnten. Das System war aber unverlässlich und teuer, weil es sechs Drähte benötigte, je einen für die fünf Nadeln und einen sechsten für einen Alarm zur Signalisierung einer Übertragung. Da nur 20 verschiedene Kombinationsmöglichkeiten dargestellt werden konnten, wurden weniger oft verwendete Buchstaben wie C, J, Q, U, X und Z für eine telegraphische Übertragung ausgeschlossen.[171]

In einem weiteren Entwicklungsschritt verminderten Cooke und Wheatstone die Anzahl der Drähte und Nadeln. Sie konstruierten einen Ein–Nadel– und einen Zwei–Nadel–Telegraphen. Es mussten aber die Bedeutungen der Nadel–Auslenkungen nach links oder rechts in einem Code vereinbart werden. Der Code für den Ein–Nadel–Telegraph enthielt nun Angaben für 23 mögliche Stellungen, sodass nur drei Buchstaben, J, Q und Z ausgelassen werden mussten. Die Ein–Nadel–Ausführung war robust, verlässlich und preiswert. Diese Ausführung wurde vorzugsweise von Eisenbahnunternehmen gekauft und in Stationen eingesetzt, so auch 1843 an der Eisenbahnlinie nach Slough. Der Zwei–Nadel–Telegraph war effizienter im Einsatz und wurde hauptsächlich in kommerziellen Netzwerken installiert.[172]

---

[170] *Wenzlhuemer*, Connecting the Nineteenth–Century World, 71.
[171] *Wenzlhuemer*, Connecting the Nineteenth–Century World, 72.
[172] *Wenzlhuemer*, Connecting the Nineteenth–Century World, 72.

Cooke und Wheatstone entwickelten für die Übertragung aller 26 Buchstaben und 10 Zahlen einen Zeigertelegraphen, der eine ringförmige Skala, ähnlich wie bei einer Uhr, hatte, aber in 36 Segmentfelder unterteilt war.



Beim Drücken eines Buchstaben an der Sendestation synchronisierte sich der Zeiger auf der Empfangsstation bis zur Anzeige des gleichen Buchstaben oder der gleichen Zahl. Trotz markanter Verbesserungen war diese Ausführung mit der Synchronisation eines Zeigers früheren Modellen sehr ähnlich.[173]

Abbildung 10: Wheatstones Zeiger-Telegraph mit Echappement

5.2.2 Telegraph von Alexander Bain

Zu den Zeiger–Telegraphen und dem Morsesystem, das im Kapitel 4.2.3 auf Seite 59 ausführlich beschrieben wird, brachten auch andere Erfinder ihre Entwicklungen auf den Markt. Von diesen wird das Gerät von Alexander Bain (1811–1877), einem Uhren- und Instrumentenbauer aus Edinburgh beschrieben, weil eine modifizierte Form des Systems in Österreich eingesetzt wurde. Bain entwickelte zunächst einen elektro–chemischen Telegraphen, der zwei Innovationen beinhaltete. Im Empfangsgerät gleitete ein elektrisch leitender Stift über einen Papierstreifen, der mit einer Mischung aus Ammoniumnitrat und Kaliumferrocyanid behandelt war. Immer wenn ein Signal eintraf und am Stift eine Spannung angelegt wurde, verfärbte sich das Papier unter dem Stift blau. Die zweite Innovation betraf das Sendegerät, in dem ein Lochstreifen aus Papier, mit Löchern für Punkte und Schlitzen für Striche versehen, zum Einlesen der zu übertragenden Signale verwendet wurde.[174]

Um eine Verletzung der Patentrechte von Wheatstone und Cooke aber auch von Samuel Morse zu vermeiden, modifizierte Bain den Empfänger zu einer Art Nadeltelegraph, wobei statt einer Nadel zwei, zu einem Ring geformte Dauermagnete verwendet wurden. Durch das Anschlagen von zwei verschieden klingenden Glockenrasseln konnten die Zeichen I und V

[173] *Wenzlhuemer*, Connecting the Nineteenth–Century World, 72.
[174] *Wenzlhuemer*, Connecting the Nineteenth–Century World, 71.

gegeben werden, mit denen das Alphabet gebildet wurde. Die Konstruktion und Fertigung der Geräte erfolgte durch die Wiener Mechaniker–Werkstätte von Johann M. Ekling (1795–1876). Mit der Errichtung der Strecke von Wien nach Brünn begann im Jahre 1846 die Einführung der Telegraphie in Österreich. Als System fand die modifizierte Form des Nadeltelegraphs von Bain Verwendung. 1847 erfolgte die Erweiterung der Telegraphenlinie bis Olmütz in Mähren und auch bis Prag. Die Linien, die mit den Bain–Geräten ausgerüstet waren, funktionierten in Österreich für die Eisenbahnlinien und für den Staatstelegraphen zur vollsten Zufriedenheit. Die Übertragungsgeschwindigkeit war, wie bei allen Zeiger–Geräten, auf 100 Worte pro Stunde begrenzt. Ein weiterer Nachteil war, dass die Buchstaben nicht registriert wurden.[175]

Als Geber im Bain–System diente eine Doppeltaste, mit der die Stromstöße in polarisierter Form gegeben werden konnten, um die beiden Glockenrasseln jeweils anzusteuern.

Abbildung 11: Die Doppeltaste für die modifizierte Form des Telegraphie–Systems von Alexander Bain

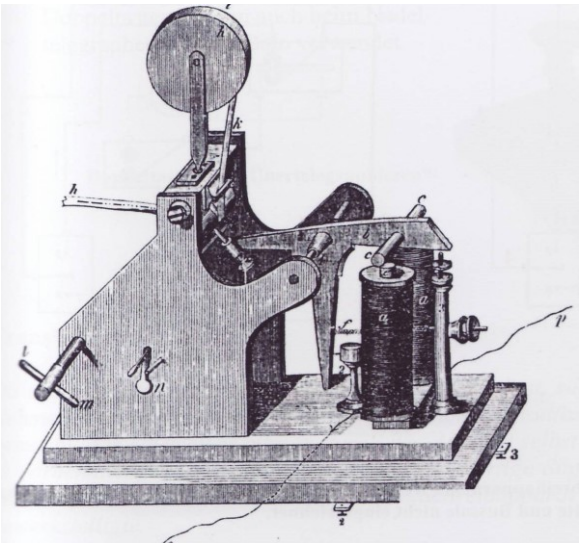
5.2.3 Druck–Telegraph von Morse

Es war das von Samuel Finley B. Morse (1791–1872) entwickelte System, das sich gegen alle anderen Apparate sowohl in den Vereinigten Staaten als auch in Europa durchsetzen konnte. Die Grundlage für die Erfindung von Morse aus dem Jahr 1837 bestand aus einem Bleistift, der eine Linie auf einem Papierstreifen aufzeichnete. Wenn ein Signal eintraf, lenkte ein Elektromagnet den Bleistift über einen Hebel auf eine Seite aus und unterbrach die Linie durch sogenannte Zacken. Die Kombination mehrerer Zacken mit unterschiedlicher Länge der Zwischenräume erlaubte die Übertragung von Zahlen und Buchstaben durch die Anwendung eines anfangs eher schwerfälligen Zahlencodes. Das System war noch nicht ausgereift. Zwei Verbesserungen von Alfred Vail (1807–1859), Assistent und späterer Mitherausgeber Morses, machten das System leistungsfähiger. Vail veränderte die Aufzeichnung so, dass der Bleistift im Ruhezustand keine Linie schrieb. Nur wenn der Stromkreis geschlossen wurde, berührte

[175] Franz *Pichler*, Die Einführung der Morse-Telegraphie in Deutschland und Österreich. In: e&i Elektrotechnik und Informationstechnik, Heft 9 (Wien 2006) 402-408, hier 406.

der Stift das Papier in Abhängigkeit von der Dauer des Signals. Alfred Vail veränderte auch den Code für die Darstellung der Zahlen und Buchstaben durch die Kombination von Punkten und Strichen in Bezug auf die Häufigkeit der zugehörigen Buchstaben in englischen Texten mit mehr oder weniger Elementen pro Buchstaben.[176]

Im Jahr 1842 stimmte der Congress der Vereinigten Staaten der versuchsweisen Installation der Morsegeräte auf der Strecke von Washington nach Baltimore zu. Zwei Jahre später ging diese Telegraphenlinie erfolgreich in Betrieb. Es war zur etwa gleichen Zeit, als Cooke die Great Western Railway Companie in England überzeugte, seine Telegraphenlinie entlang der Eisenbahnlinie nach Slough bei Windsor zu installieren.[177] Die erste deutsche „Morse–Linie" wurde von Hamburg nach Cuxhaven eingerichtet und am 15. Oktober 1848 in Betrieb genommen, wobei zum ersten Mal in Europa die sogenannten „Morsetasten" zum Einsatz kamen. Der dafür eingesetzte Telegraphen–Inspektor in Cuxhaven war Friedrich Clemens Gerke (1801–1888), der Verbesserungen entwickelte.[178]



Die ersten Telegraphenapparate hatten einen Gewichtsantrieb, der später mit einem Federantrieb, wie bei einem Uhrwerk, ersetzt wurde. Der Federantrieb war zuerst offen und wurde erst bei späteren Apparaten in ein Gehäuse eingebaut und so gegen Staub geschützt.[179]

Abbildung 12: Der Schreibapparat um etwa 1850

Der erste Code von Samuel Morse, beziehungsweise von Alfred Vail, hatte einige Mängel, weil die Einhaltung der unterschiedlich langen Abstände zwischen den Elementen des Morsezeichens sehr große Schwierigkeiten bereitete und Buchstaben bzw. Satzzeichen aus bis zu sieben Elementen bestanden. Der Telegrapheningenieur Friedrich Clemens Gerke hat die Struktur des Morsealphabets überarbeitet und zum Teil neue Zeichen geschaffen, die leichter zu lesen waren. Ferner hat er den Stiftschreiber zu einem Farbschreiber umgebaut, dessen

[176] *Wenzlhuemer*, Connecting the Nineteenth–Century World, 71.
[177] *Wenzlhuemer*, Connecting the Nineteenth–Century World, 71.
[178] *Pichler*, Die Einführung der Morse-Telegraphie, e&i, H. 9, 405.
[179] Johann *Prikowitsch*, Telegraph und Telephon in der k. (u.) k. Armee und Marine, Band 1 (Wien 2016) 22.

Papierstreifen leichter abzulesen war. Es entstanden dadurch klare Regeln für die verschiedenen Strich– und Punktekombinationen. Der Code besteht für Buchstaben nach Häufigkeit in Texten aus ein bis vier Elementen. Ziffern werden aus fünf und Satzzeichen (Punkt, Beistrich, Bindestrich, Schrägstrich etc.) aus sechs Elementen gebildet. Gerkes Alphabet wurde am 1. Juli 1852 vom Deutsch–Österreichischen Telegraphen–Verein eingeführt. Es setzte sich international durch und hat in wesentlichen Teilen bis heute noch seine Gültigkeit behalten.[180]

Tabelle 5: Alphabet nach Clemens Gerke, zu Ehren Samuel Morses „Morse Alphabet“ genannt.

Alphabet						Zahlen	
a	·−	i	··	r	·−·	1	·−−−−
ä	·−·−	j	·−−−	s	···	2	··−−−
b	−···	k	−·−	t	−	3	···−−
c	−·−·	l	·−··	u	··−	4	····−
ch	−−−−	m	−−	ü	··−−	5	·····
d	−··	n	−·	v	···−	6	−····
e	·	o	−−−	w	·−−	7	−−···
f	··−·	ö	−−−·	x	−··−	8	−−−··
g	−−·	p	·−−·	y	−·−−	9	−−−−·
h	····	q	−−·−	z	−−··	0	−−−−−

Die Vorzüge des Morsetelegraphen waren leicht erkennbar. Dieser entwickelte in der Hand eines geübten Telegraphisten 100 bis 120 Buchstaben in einer Minute, während in einer Minute der beste Zeiger–Telegraph kaum 20 Buchstaben übertragen konnte. Eine Depesche mit 20 Worten brauchte am Morse–Apparat eine Minute und 30 Sekunden, am Bain–Apparat 8 Minuten und am Zeiger–Telegraphen 14 Minuten.[181] Auch hier spielt die Häufigkeits–verteilung der Buchstaben des deutschen Alphabets in einem Standardtext eine Rolle (siehe Tabelle 1, Seite 15). Je öfter ein Buchstabe in einem deutschen Standardtext vorkommt, umso kürzer ist sein Morsezeichen. Der Buchstabe »e« mit einer höchsten Häufigkeit von 17,40 % unter den Buchstaben, hat das kürzeste Morsezeichen, nämlich einen Punkt.[182] Das Morseverfahren setzte sich in Europa gegen das Wheatstone–Cooke–System durch und wurde ab dem Jahr 1851 mit der europäischen Form des Morsecodes nach Gerke auf dem ganzen Kontinent und ab 1865 für den internationalen Telegraphenverkehr übernommen.[183] Der Morsecode selbst ist keine kryptographische Anwendung, denn er hat nicht den Zweck, die

[180] Friedrich Clemens *Gerke*, Der Elektro-Magnetismus als Maschinentriebkraft, Versuch einer Lösung des Problems (Hamburg 1857) 10f.
[181] Joseph *Forsach*, Handbuch der electrischen, galvanischen, magnetischen und electromagnetischen Telegraphie (Wien 1854) 109.
[182] *Singh*, Geheime Botschaften, 85.
[183] *Wenzlhuemer*, Connecting the Nineteenth–Century World, 73.

Nachrichten geheim zu halten. Der Morsecode ist im Grunde nichts weiter, als eine andere, digitale Form des Alphabets, die zur elektrischen Übertragung von Buchstaben, Zahlen und Satzzeichen eingesetzt wurde.

Vor Absendung einer Botschaft musste diese trotzdem verschlüsselt werden, bevor man sie dem Telegraphisten übergab. Die Verschlüsselung sorgte nicht nur dafür, dass der Telegraphist kein geheimes Material zu Gesicht bekam, sie verdarb auch Spionen, die womöglich die Telegraphenleitung angezapft hatten, das Geschäft.[184]

5.3 Ausbau des Telegraphie–Netzes in Europa und weltweit

Englische Eisenbahnplaner erkannten in den 1840er-Jahren die elektrische Telegraphie als einzig probates Mittel zur effektiven Koordination des Eisenbahnverkehrs. Sie begannen, entlang des Schienensystems Telegraphenlinien zu errichten. Durch diese Symbiose, aber auch durch das nun geweckte Interesse von Handel, Finanzwelt und Administration, bildeten sich im Laufe der 1840er- und 1850er–Jahre vor allem in den Ländern West– und Mitteleuropas sowie in den Vereinigten Staaten dichte Telegraphennetzwerke aus, die man Schritt für Schritt miteinander verband.[185] Im Jahr 1849 hat ein „electro–magnetischer Telegraph“ die Städte Berlin, Potsdam, Magdeburg, Oschersleben, Braunschweig, Hannover, Celle, Harburg, beziehungsweise Hamburg und Cuxhaven, Bremen, Minden, Düsseldorf, Köln, Frankfurt am Main, Weimar, Erfurt, Merseburg, Halle, Köthen, Wittenberg etc. verbunden, nachdem sich die betroffenen Staatsregierungen über die Errichtung dieses neuen Übertragungsmittels vereinbart und dessen Ausführung beschlossen hatten. Es bestand kein Zweifel darüber, dass dieses „blitzschnelle“ Korrespondenzmittel nicht nur den Regierungen und den Eisenbahnverwaltungen für dienstliche Mitteilungen, sondern auch der Bevölkerung zur Beförderung von Privat– und Handelsnachrichten, gegen Bezahlung einer nach Entfernung und Zeichenzahl bemessenen Taxe zugänglich gemacht werden sollte.[186]

Fortschritte in der Isolierung der Leitungen und der Kabelproduktion erlaubten es schließlich auch, Unterseekabel zu verlegen. Bereits im Jahr 1851 konnten London und Paris durch ein Kabel durch den Ärmelkanal in telegraphische Verbindung treten. Nur erstaunliche fünfzehn Jahre später durchquerten unter Wasser verlegte Telegraphenkabel den Atlantischen Ozean.[187]

[184] *Singh*, Geheime Botschaften, 85.
[185] *Wenzlhuemer*, Connecting the Nineteenth–Century World, 31f.
[186] *Meissner*, Die Correspondenz in Chiffern, 4.
[187] *Rosenberg*, Transnationale Strömungen, 828.

Nach diesen Erfolgen wurden ab dem dritten Quartal des 19. Jahrhunderts weltweit Unterwasserkabeln verlegt. Seit Indien (1870), China (1871), Japan (1871), Australien (1871), die Karibik (1872), alle größeren Staaten Südamerikas (bis 1875), Süd– und Ostafrika (1879) und Westafrika (1886) per Kabel erreichbar waren, entstand innerhalb weniger Jahre eine enorme kommerzielle Informationsverdichtung, auch wenn erst im Oktober 1902 das planetarische Telegraphennetz durch die Eröffnung eines Pazifikkabels geschlossen wurde.[188] Der Zeitabstand zwischen der Bekanntgabe von öffentlichen Geschäftsnachrichten, wie Börsennotierungen oder Preisnotierungen in aller Welt, betrug in den späten 1880er Jahren zwei bis drei Tage, bis sie am anderen Ende der „Leitung" in London veröffentlicht wurden. Private Botschaften erreichten den Empfänger über Kabel meist innerhalb eines Tages. Zum Vergleich zu diesen Übertragungsgeschwindigkeiten war die Meldung über Napoleons Invasion Ägyptens 62 Tage lang nach London unterwegs und 1815 hatte es zweieinhalb Tage gedauert, bis London von der Niederlage bei Waterloo erfuhr. Am 8. Jänner 1815 fanden in der Schlacht von New Orleans tausend britische und amerikanische Soldaten den Tod, weil ihren Kommandeuren nicht bekannt war, dass die Gegner am 24. Dezember in Gent bereits Frieden geschlossen hatten.[189]

Eine Analyse der Zahlen aus den Jahren 1881, 1892 und 1902 zeigen die strukturelle Entwicklung des globalen Telegraphennetzwerkes in den letzten 20 Jahren des 19. Jahrhunderts. Im Jahr 1881 bestand das Netzwerk aus 1.934 Knotenpunkten, die über 2.450 Leitungen verbunden waren. Etwa zehn Jahre später wies das Netzwerk bereits 2.949 Knotenpunkte auf, die 3.938 verschiedene Leitungen verbanden und nach Erreichung der globalen Umrundung im Jahr 1902 hatte das Telegraphennetzwerk 3.813 Knotenpunkte und 5.160 Verbindungen erreicht.[190] Die Rangliste der Städte mit den höchsten Zahlen an Telegraphen–Nachrichten, die alle drei Jahre ermittelt wurden, führten stets London, Paris und Wien an; Berlin lag an sechster Stelle. Die Schnittpunkte mit den höchsten Zahlen an telegraphischen Nachrichten lagen jedenfalls in europäischen Städten. Weitere Knotenpunkte mit hoher Kommunikationsdichte am oberen Ende der Rangliste waren die französischen Städte Marseille und Lyon, St. Louis in den Vereinigten Staaten und die Mittelmeerinsel Malta. Auf den Hauptachsen der globalen Kommunikation lag London, die damit auch die Rangliste der Hafenstädte anführte.[191] Zur Illustration der zur Jahrhundertwende im Staatstelegraph einge–

[188] *Osterhammel*, Die Verwandlung der Welt, 1025.
[189] *Osterhammel*, Die Verwandlung der Welt, 1026.
[190] *Wenzlhuemer*, Connecting the Nineteenth–Century World, 150f.
[191] *Wenzlhuemer*, Connecting the Nineteenth–Century World, 151.

setzten Schreibapparate wird hier das Modell aus dem Jahr 1892 abgebildet. Dieser Telegraphen–Apparat wurde von mehreren Firmen über Jahrzehnte lang erzeugt und war baugleich mit dem Schreibapparat (Relief–Schreiber), der beim Feldtelegraphenamt verwendet wurde.[192]

Abbildung 13: Telegraphenapparat Modell 1892, Erzeugnis J. Schäffler Wien.

5.4 Das Telephon in Österreich

Die stärkste Alltagserfahrung der Vernetzung kam mit dem Anschluss einzelner Haushalte an zentral gesteuerte Netzwerke. Hier lag auch ein Unterschied zwischen Telegraph und Telephon. Der Telegraph blieb ein Amtsgerät, das sich niemand ins Wohnzimmer stellte, das Telephon hingegen wurde nach einer gewissen Anlaufzeit zum privaten Gebrauchs– und Einrichtungsgegenstand. Ende des 19. Jahrhunderts war es nur eine kleine Minderheit der Bevölkerung, die an ein technisches System angeschlossen war.[193]

Der „Wiener Privat–Telegraphen–Gesellschaft“ wurde am 3. Juni 1881 die Konzession erteilt, ein Telephon–Netz in Wien, die erste Fernsprechanlage in Österreich, zu betreiben. Die Bewilligung galt für einen Umkreis von 15 km vom Stephansdom aus gerechnet. Für längere Strecken war die Technologie des Telephons zu diesem Zeitpunkt nicht geeignet. Die erste Fernsprechanlage in Österreich nahm am 1. Dezember 1881 den Betrieb auf. Die Zentrale befand sich in der Friedrichstrasse und es gab 154 private Teilnehmer. Das Telephonwesen wurde zunächst von privaten Unternehmen vorangetrieben.[194]

Wegen der steigenden Bedeutung des Telephonverkehrs und weil durch die Telephon–Verordnung vom 7. Oktober 1887 das Telephon zum „Staatsregal“ erklärt worden war, beschloss die Staatsverwaltung, die privaten Telephonnetze zu verstaatlichen wodurch im Jahre 1895 das letzte private Telephonnetz, das „Wiener Netz“, auch der Staat übernahm. Der Staat begann aus wirtschaftlichen und militärischen Überlegungen, von Wien aus Überlandleitungen für den Fernverkehr zu verlegen. Die erste österreichische

[192] *Prikowitsch*, Telegraph und Telephon, Bd. 1, 32.
[193] *Osterhammel*, Die Verwandlung der Welt, 1011.
[194] *Prikowitsch*, Telegraph und Telephon, Bd. 1, 140.

Städteverbindung wurde am 1. August 1886 von Wien nach Brünn eingerichtet. Drei Jahre später, am 18. September 1889 wurde die erste Fernleitung von Wien nach Prag in Betrieb genommen. Daraufhin begann der Staat, nach Prag auch weitere Städte wie Graz, Budapest und Triest an die Fernleitung anzuschließen. In dieser stürmischen Entwicklung nahmen in den angeschlossenen Städten Orts– und Fernzentralen den Betrieb auf, wodurch die Anzahl der Teilnehmer sprunghaft anstieg.[195]

Es war auch der Wunsch der Bürger, dass ihre Stadt das sein sollte, was man „modern" nannte. Ihre Stadt sollte beim Ausbau der Infrastruktur teilhaben, die man überall in Europa wahrzunehmen glaubte. Man musste unverzüglich handeln, wenn man sich den raschen Fortschritt auf dem technologischen und wirtschaftlichen Sektor zunutze machen wollte, um Märkte nicht an regionale Konkurrenten zu verlieren. So erwirkten zum Beispiel die Stadträte von Mährisch–Schönberg (Šumperk) 1891 beim Handelsministerium die Erlaubnis, ihren Ort an das Telephonnetz anzuschließen. Gegen Ende 1892 wurde das Fernsprechnetz in Šumperk eingerichtet. Kurz darauf hatte Ungarisch Brod um 1905 einunddreißig Telephonanschlüsse und alle waren mit einem größeren, überregionalen Fernsprechnetz verbunden.[196]

Bereits 1914 war Österreich und Europa mit einem dichten Telephonnetz überzogen, wodurch alle wichtigen Städte über Fernleitungen erreicht werden konnten. Gab es anfangs nur die „händische Vermittlung" zur Herstellung der gewünschten Verbindung zwischen den Teilnehmern, so standen ab 1914 halb–automatische und sogar voll–automatische Wähleinrichtungen und Netze zur Verfügung.

Abbildung 14: Pultstation für eine „händische Vermittlung" hergestellt in der Telephon-Fabrik A.G. Wien, etwa 1905.

Im Jahre 1910 war die Telephon–Anlage in Graz, die 2000 Einzel– und 1200 Gesellschaftsanschlüsse hatte, auf einen vollautomatischen Betrieb umgestellt worden. Wegen der vielen technisch unterschiedlichen Nebenstellenanlagen konnte das Wiener Netz vorerst nur als ein halb–automatisches Netz betrieben werden.[197]

[195] *Prikowitsch*, Telegraph und Telephon, Bd. 1, 140.
[196] *Judson*, Habsburg, 453.
[197] *Prikowitsch*, Telegraph und Telephon, Bd. 1, 140.

5.5 Drahtlose Telegraphie zur Jahrhundertwende

In den letzten Jahren des 19. Jahrhunderts war die Kryptographie in einem kläglichen Zustand. Seit Babbage und Kasinski die Vigenère–Verschlüsselung geknackt hatten, waren die Kryptographen auf der Suche nach neuen Verfahren. Es sollte wieder möglich werden, Nachrichten geheim zu übermitteln. Zudem erfand der italienische Physiker Guglielmo Marconi (1874–1937) um die Jahrhundertwende mit der drahtlosen Telegraphie ein viel mächtigeres Verfahren zur Telekommunikation, und die sichere Verschlüsselung war nun notwendiger denn je.[198]

Die Kommunikation mittels der elektrischen Telegraphie, so erfolgreich diese auch in der zweiten Hälfte des 19. Jahrhunderts eingesetzt wurde, war wegen der Notwendigkeit zwischen Sender und Empfänger eine elektrische Leitung zu haben (Freileitung, Kabel), auf den Nachrichtenverkehr zwischen festen Stationen beschränkt. Es fehlte nicht an Versuchen, um auch für mobile Stationen, vor allem für Schiffe, aber auch für Eisenbahnzüge, eine telegraphische Verbindung technisch zu realisieren. Mit der experimentellen Entdeckung der elektromagnetischen Wellen durch Heinrich Rudolf Hertz (1857–1894) im Jahre 1887 war jedoch eine neue physikalische Basis zur Realisierung eines technischen Systems zur Kommunikation zwischen mobilen Stationen geschaffen. Es dauerte aber noch weitere zehn Jahre, bis dies durch den jungen Italiener Guglielmo Marconi (1874–1937) geschah. Guglielmo Marconi, geboren in Bologna, war seit seiner Jugendzeit an den Gebieten Physik und Chemie sehr interessiert und führte zuhause experimentelle Versuche durch. Im Jahre 1894 brachte ihn ein Artikel von Righi, der die Hertz'schen Experimente behandelte, auf den Gedanken, diese als Grundlage zur Realisierung eines Telegraphie–Systems heranzuziehen. Dies führte ihn schließlich Ende 1895 zur Entwicklung seines bekannten Funksystems, das er Mitte 1896 in England der Postanstalt mit Erfolg vorführte.[199]

Marconis wesentliche erfinderische Leistung bei seinem Funksystem bestand in der Anwendung einer Antenne, damals als "Luftdraht" bezeichnet, als Gegenpol zur Erde. Damit verbesserte er die Reichweite gegenüber seinen Konkurrenten, die mit ähnlichen Anordnungen experimentierten, um ein Vielfaches. Die Möglichkeit einer drahtlosen Telegraphie zwischen Schiffen und Küstenstationen (Leuchttürme), wie diese durch das

[198] *Singh*, Geheime Botschaften, 129.
[199] Franz *Pichler*, Drahtlos über den Atlantik. Erste Telegraphie-Funkübertragung durch Guglielmo Marconi vor 100 Jahren. Online unter: <http://www.univie.ac.at/pluslucis/PlusLucis/021/s18_21.pdf> (21. August 2017).

Marconi–System möglich wurde, waren von großer praktischer Bedeutung. Bereits 1898 fanden vor Pola erste erfolgreiche Funkversuche zwischen den k. u. k. Schiffen S. M. S. Budapest und S. M. S. Lussin statt.[200]

Der Wunsch nach einer solchen Telegraphie zwischen Europa und den Vereinigten Staaten von Amerika war ebenfalls groß. Den international agierenden Kabelgesellschaften, allen voran die Firma Cable & Wireless, die das Weitverkehrs–Festnetz in ihrer Hand hatten, würde damit ein großer Konkurrent erwachsen. Am 12. Dezember 1901 wurde eine Antenne mittels eines Flugdrachens hochgezogen. Um 12 Uhr 30, 13 Uhr 10 und um 14 Uhr hörte Marconi, wie er im Tagebuch festhielt, die Morsezeichen für den Buchstaben »s«, also drei Punkte. Um ganz sicher zu gehen, wurde dieser Empfang auch am nächsten Tag bestätigt. Der "Transatlantik–Test" in Form einer drahtlosen telegraphischen Übertragung von Morsezeichen von Poldhu (England) nach St. John (Kanada) über eine Distanz von 2.170 Meilen (ca. 3500 km) war damit erfolgreich bestanden und leitete ein neues Zeitalter der Kommunikation mittels elektrischer Mittel ein.[201]

Die Entwicklung des Funkverkehrs und der Ausbruch des Ersten Weltkrieges führten zu einem drastisch erhöhten Bedarf an Verschlüsselung von Informationen und Befehlen. Zwischen 1914 und 1918 gab es allerdings keine großartigen Entdeckungen, sondern eine Reihe kryptographischer Fehlschläge. Es gab zwar eine Reihe neuer Chiffren, doch waren sie alle Variationen oder Kombinationen von Chiffren aus dem 19. Jahrhundert, die schon geknackt worden waren. Das Militär verwendete wieder dreistellige Chiffren, um den Zeitaufwand für die Chiffrierung und Dechiffrierung zu verkürzen, änderte die Chiffren bald aber wieder auf vierstellige und fünfstellige Ziffern.[202]

Ein Blick auf die ebenfalls nicht neue Chiffriermethode für die Einheit des braven Soldaten Schwejk, in der eingangs erwähnten Anekdote, zeigt einen einfachen Schlüssel, der mit Hilfe von zwei Seiten eines Romans zu lösen war sowie die Sorglosigkeit einer telephonischen Übermittlung an der Front in Galizien. Ein Fehlschlag der Ausführung eines verschlüsselten Befehles, der durch das Vertauschen der „Chiffren-Bücher“ nicht entschlüsselt werden konnte, war absehbar.

---

[200] MFCA, Marine Funker Club Austria. Online unter: <http://www.qth.at/mfca> (2. März 2017).
[201] Franz *Pichler*, Drahtlos über den Atlantik. Erste Telegraphie-Funkübertragung durch Guglielmo Marconi vor 100 Jahren. Online unter: <http://www.univie.ac.at/pluslucis/PlusLucis/021/s18_21.pdf> (21. August 2017).
[202] *Singh*, Geheime Botschaften, 134.

Ganz anders als die wachsamen und letztlich erfolgreichen Franzosen verhielten sich 1916 die Deutschen. Als die deutsche Armee schon in einer frühen Kriegsphase in französischem Gebiet eingedrungen war, hatte sie keinen Chiffrierdienst eingerichtet. Die Franzosen zerstörten bei ihrem Rückzug die Telegraphenlinien und zwangen die vorrückenden Deutschen, Funkgeräte für ihren Fernmeldeverkehr einzusetzen. Während die Franzosen die deutschen Funkmeldungen also ständig abhören konnten, standen die Deutschen mit leeren Händen da. Die Deutschen bauten ihren kryptoanalytischen Dienst erst nach zwei Jahren Krieg auf.[203]

Weil bekannt war, dass die Alliierten den gesamten transatlantischen Nachrichtenverkehr der Deutschen abhören konnten, mussten sie ihre Telegramme verschlüsseln. Dafür hatten die Briten mit ihrer ersten Angriffsaktion im Krieg gesorgt. Am ersten Tag des Ersten Weltkrieges hat das britische Schiff *Telconia* im Schutz der Dunkelheit vor der deutschen Küste die transatlantischen Kabel, die Deutschland mit Amerika verbanden, gekappt. Dieser Sabotageakt zwang die Deutschen auf den unsicheren Funkverkehr oder auf die Kabel anderer Länder auszuweichen.[204]

5.6 Gründung nationaler und internationaler Telegraphenvereine

Die Ausdehnung der Telegraphennetze in den verschiedenen Ländern bis an die Landesgrenzen und die immer rascher voranschreitenden technologischen Veränderungen brachten es mit sich, dass Abordnungen einzelner Staaten zusammenkamen, um Verfahren zu regulieren, die vor allem die globale Kommunikation und das Transportwesen betrafen.[205] Der Telegraph wurde in der zweiten Hälfte des 19. Jahrhunderts zum sichtbaren Symbol einer zusammenrückenden und miteinander verbundenen Welt. Durch die Telegraphie wurde es leicht, über große Entfernungen hinweg wirtschaftliche oder strategische Informationen auszutauschen. So wurden in diesem Bereich schon früh internationale Normen und Verfahren festgelegt und aufeinander abgestimmt.[206] Nach einer Kooperation Österreichs mit den deutschen Ländern und der Gründung des „Deutsch–Österreichischen Telegraphen–Vereins“ 1850 wurde zur Verbesserung der Internationalen Kommunikation 1865 in Paris der „Internationale Telegraphenverein“ gegründet, womit der Typus einer internationalen Verwaltungsunion mit den Zielen geschaffen wurde, die globale Kommunikation zu

[203] *Singh*, Geheime Botschaften, 136.
[204] *Singh*, Geheime Botschaften, 140.
[205] *Rosenberg*, Transnationale Strömungen, 827.
[206] *Rosenberg*, Transnationale Strömungen, 828.

standardisieren und zu regulieren. Die internationalen Telegraphen hatten die verbesserte Version des Morsealphabets übernommen und machten sie zum Standard (siehe Seite 70). Die neue Organisation war nach der Einführung der drahtlosen Telegraphie für die Zuweisung der Sende– und Empfangsfrequenzen zuständig und entwickelte Verfahren für internationale Telephongespräche.[207]

5.6.1 Deutsch–Österreichischer Telegraphen–Verein

Die Telegraphennetzwerke der einzelnen Staaten wurden von den eigenen Regierungen administriert und benutzten verschiedene Technologien und Verfahren. Weil aber von Anfang an der Wunsch einer grenzüberschreitenden Telegraphenverbindung bestand, wurde von den einzelnen Staaten eine Vereinheitlichung der Systeme angestrebt. Zur Harmonisierung der Systeme zwischen den Staaten wurde daher auf der Konferenz vom 25. Juli 1850 in Dresden der Vertrag zur Gründung des „Deutsch–Österreichischen Telegraphen–Vereins“ (DÖTV) beschlossen. Um diesen Hauptvertrag über die Bildung eines Deutsch–Österreichischen Telegraphen–Vereins vom 25. Juli 1850 und die in den Nachtrags–Verträgen vom 14. Oktober 1851, 23. September 1853 und 29. Mai 1855 enthaltenen Bestimmungen zu revidieren, zu vervollständigen sowie in „Einen Vertrag“ zusammen zu fassen, haben die folgenden, in der Reihenfolge des Art. IV der deutschen Bundesakte vom 8. Juni 1815 angeführten hohen Regierungen der deutschen Bundesstaaten: Österreich, Preußen, Bayern, Sachsen, Hannover, Württemberg, Baden und Mecklenburg–Schwerin sowie das Königreich der Niederlande auf der fünften Konferenz des Deutsch–Österreichischen Telegraphen–Vereins in Stuttgart 28 Artikel vereinbart und am 16. November 1857 unterzeichnet.[208]

Im Artikel 3 wird gefordert, dass jede Depesche von der Aufgabe bis zur Adress–Station möglichst „ohne Umtelegraphierung befördert werden“ muss. Auf allen Stationen waren die vereinbarten Apparate und Schriftzeichen anzuwenden. Gemäß Artikel 5 war jede Vereins–Regierung befugt, einzelne oder sämtliche Linien für alle oder für gewisse Arten Korrespondenz (im Kriegsfall) zeitweise außer Betrieb zu setzen. Artikel 10 legte fest, dass die Uhren aller Telegraphen–Stationen einer und derselben Vereinsverwaltung nach der mittleren Zeit der „Central–Station“ gerichtet wurden. Nach Artikel 11 konnten Staats–Depeschen in beliebiger Sprache abgefasst oder chiffriert ausgeliefert werden. Bei allen

[207] *Rosenberg*, Transnationale Strömungen, 828f.
[208] OeStA/HHStA, k. und k. Ministerium des Äußern, AR F55 Karton 1, Generalia 1861-1868, Mappe: Deutsch-Österreich zwischen den Vereins Staaten geschlossene Verträge. 1. Nachtrags-Vertrag vom 16. Nov. 1857 vereinbart zu Stuttgart.

anderen Depeschen war die Fassung in deutscher oder französischer Sprache die Regel. Ausführlich wurde im Artikel 15 die Berechnung der Depeschenübertragung nach Anzahl der Wörter und Entfernung in Zonen (erste Zone 10 Meilen, zweite Zone 15 Meilen, dritte Zone 20 Meilen) beschrieben. Eine Depesche mit 20 Worten kostete für eine Entfernung von 70 bis 100 Meilen drei österreichische Gulden. Artikel 19 regelte die Aufteilung der Vereins–Gebühren unter den Vereins–Mitgliedern. Nach Artikel 27 trat dieser Vertrag mit 1. Jänner 1858 in Kraft.[209]

Dem durch den Deutsch–Österreichischen Telegraphen–Verein (DÖTV) vom 25. Juli 1850 gegebenen Beispiel folgten bald andere Staaten. Eine Anzahl von Staaten schlossen bilaterale Verträge zur Harmonisierung der telegraphischen Kommunikation mit den europäischen Staaten ab. Der Westeuropäische Telegraphen–Verein wurde 1855 durch Frankreich, Belgien, Spanien, Sardinien und der Schweiz gegründet. Beide Vereine arbeiteten ab dem Beginn eng zusammen.[210]

5.6.2 Der Internationale Telegraphen–Verein

Die Bildung des Deutsch–Österreichischen Telegraphen–Vereins und der Beginn der Verlegung von Telegraphen–Kabeln ließen auch auf internationaler Ebene eine Kooperation zwischen den Staaten sinnvoll erscheinen, um die Kommunikationsmöglichkeiten zu verbessern. Die 20 Gründungsmitglieder traten 1865 in Paris zu einem ersten internationalen Telegraphen–Kongress zusammen und gründeten den Internationalen Telegraphen–Verein (International Telegraph Union, ITU), durch welchen der internationale Telegraphenverkehr in einem für ganz Europa gültigen Vertrag seine Regelung erhielt. Bei diesem ersten Kongress wurde festgelegt, dass ausschließlich Morse–Telegraphen im internationalen Telegraphie–Verkehr verwendet werden.[211] Der zweite internationale Telegraphenkongress im Juni 1868 in Wien schuf das „Bureau international des administrations télégraphiques“ in Bern als Zentralorgan, welches die Nachrichten über die Vorgänge im europäischen Telegraphie–Verkehr zu sammeln und die Arbeit der periodischen Konferenzen vorzubereiten hatte. Ab dem Jahr 1869 veröffentlichte dieses Büro das "Journal télégraphique" das sich mit allen Angelegenheiten der internationalen Telegraphie beschäftigte. In den Ausgaben der

[209] OeStA/HHStA, k. und k. Ministerium des Äußern, AR F55 Karton 1, Generalia 1861-1868, Mappe: Deutsch-Österreich zwischen den Vereins Staaten geschlossene Verträge. 1. Nachtrags-Vertrag vom 16. Nov. 1857 vereinbart zu Stuttgart.
[210] *Wenzlhuemer*, Connecting the Nineteenth–Century World, 105.
[211] *Wenzlhuemer*, Connecting the Nineteenth–Century World, 73.

Jahre 1877, 1883, 1887, 1889, 1892, 1894, 1897, 1901 und 1903 enthielt das „Journal télégraphique“ einen Anhang mit dem Titel „Nomenclature“, in dem alle verlegten Unterwasserkabeln aufgelistet waren und Angaben über deren Länge, Zeitpunkt der Verlegung und Inbetriebnahme, Bedienungspersonal sowie der Administration durch staatliche Institutionen oder private Unternehmen enthielten.[212]

Auf dem dritten Kongress in Rom 1872 kam man überein, die großen Privat–Kabelgesellschaften zu den Kongressen zuzulassen, ohne ihnen jedoch Stimmrecht einzuräumen. Der vierte Kongress, 1875 zu St. Petersburg, teilte das internationale Vertragsinstrument in zwei Urkunden, von welchen die erstere, die sich mit unveränderlichen Rechtsverhältnissen der Verwaltungen untereinander und dem Publikum gegenüber befasste, von den diplomatischen Vertretern der Staatsregierungen unterzeichnet wurde, während der Abschluss der zweiten, welche die Reglementären Bestimmungen betraf, nur von den technischen Delegierten erfolgte. Die folgenden Kongresse haben sich nur mit Abänderung der Ausführungsbestimmungen (Reglement) zu diesem Vertrag befasst.[213]

Auf dem fünften Kongress in London 1879 vereinbarte man das in Deutschland von Heinrich von Stephan ins Leben gerufene Worttarifsystem, und auf dem sechsten Kongress, Berlin 1885, wurde von Stephan der Antrag auf Schaffung eines Einheitstarifs, wenigstens für den europäischen Verkehr, eingebracht (siehe Seite 64). Dieser Antrag fand zwar nicht allgemeine Annahme, doch beschloss der Kongress weitere Vereinfachungen des Tarifs, um die spätere Einführung eines Einheitstarifs vorzubereiten. Nach den Bestimmungen des Berliner Vertrags bildete sich der internationale Tarif aus einer Gebühr für das Wort, welche der Staat des Aufgabegebiets und der Staat des Bestimmungsgebiets (Terminaltaxen) und die etwa zwischen dem Aufgabe– und Bestimmungsgebiet liegenden Staaten (Transittaxen) jeder für sich erhob. Die Terminaltaxen und die Transittaxen wurden für jeden Staat einheitlich festgestellt. Die Terminaltaxe wurde einheitlich auf 10 Cent, die Transittaxe auf 8 Cent für jedes Wort mit der Ermäßigung auf 6½ und 4 Cent für kleinere Staaten festgesetzt.[214]

Diese konzertierten Bemühungen harmonisierten letztlich die europäische Telegraphie bereits am Beginn ihrer Geschichte. Die Maßnahmen zur Bildung internationaler Netzwerke begünstigten die entmaterialisierte Kommunikation über große Entfernungen. Im

[212] *Wenzlhuemer*, Connecting the Nineteenth–Century World, 108.
[213] Telegraphenkongresse. In: Meyers Konversationslexikon, Band 15 (Leipzig/Wien [4]1885-1892) 572.
[214] Telegraphenkongresse, 573.

europäischen Kontext konnte dies durch den Zusammenschluss existierender nationaler Netzwerke in der Nachbarschaft erreicht werden.[215]

5.7 Feldtelegraphenwesen der österreichisch–ungarischen Armee

Nach der Aufstellung des Eisenbahn– und Telegraphenregiments (ETR) im Jahre 1883 und der Gründung der Telegraphentruppenschule 1889 erfolgte die Ausbildung des Kader–personals beim ETR und an der Telegraphentruppenschule in Korneuburg. Die erforderlichen Vorschriften für die Ausbildung der Offiziere, Unteroffiziere, Chargen und Mannschaften wurden durch die Abteilung 5 des Kriegsministeriums (KM) in Zusammenarbeit mit dem ETR und der Telegraphentruppenschule herausgegeben. Die Marinevorschriften wurden durch das „k. u. k. Marine Technische Comite" erstellt und in Pola herausgegeben. Die systematisierten Telegraphenapparate waren spezielle Entwicklungen für den Militär–gebrauch, es wurden aber auch „Staatstelegraphenapparate", also zivile Telegraphenapparate eingesetzt, vor allem im Bereich des „Reservetelegraphen". Die Handhabung dieser Telegraphenapparate war auch Bestandteil der Ausbildung.[216]

Zur Erklärung der verwendeten Begriffe Staatstelegraph, Feldtelegraph und Reservetelegraph:
Der *Staatstelegraph* umfasste alle technischen Einrichtungen der Telegraphen– und Telephon–Verbindungen innerhalb des eigenen Staatsgebietes und auch jener für Verbindungen ins Ausland. Geleitet wurde der Staatstelegraph von der Staats–Telegraphenverwaltung; in den Kronländern gab es Telegraphendirektionen.
Der *Feldtelegraph* wurde von den Telegraphen– und Telephon–Formationen der Truppe gebildet, deren Personal in Truppenschulen durch die Armee ausgebildet wurde. Der Feldtelegraph erstellte und unterhielt die Verbindungen zu den Kampftruppen an der Front.
Der *Reservetelegraph* war ein Verbindungsglied zwischen dem Feldtelegraphen und dem Staatstelegraphen. Mit dem Vorrücken der Armee hatte er so rasch als möglich das stabile Staatstelegraphennetz feindwärts zu erweitern, sodass in erster Linie die operierenden Armee–kommanden in telegraphischer Verbindung mit dem Hinterland blieben.[217]

Im Unterschied zu den Apparaten des Staatstelegraphen waren gemäß Vermerk im „Feld–Telegraphen–Wesen des k. k. Heeres" von 1885 die älteren Typen mit einem liegenden

[215] *Wenzlhuemer*, Connecting the Nineteenth–Century World, 106.
[216] *Prikowitsch*, Telegraph und Telephon, Bd. 1, 26.
[217] *Prikowitsch*, Telegraph und Telephon, Bd. 1, 13.

Galvanoskop ausgerüstet.[218] Die Feldtelegraphenapparate der Type M. 1892 hatten bereits ein senkrecht montiertes Galvanometer und verfügte auch über eine stärkere Triebfeder im Laufwerk, womit eine Laufdauer des Werkes bei der größtmöglichen Geschwindigkeit auf zehn Minuten verlängert werden konnte. Durch die Wahl einer stärkeren Drahtsorte für die Multiplikations–Spulen wurde die magnetisierende Wirkung des Linienstromes beträchtlich verstärkt und daher die Empfindlichkeit des Relais erhöht. Der Feldtelegraphenapparat M.1892 wurde über Jahrzehnte erzeugt und ist als Tischapparat wesentlich größer ausgeführt als das Modell 1892, welches beim Staatstelegraph verwendet wurde.[219]

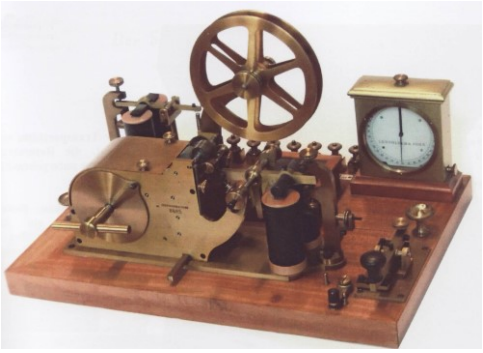


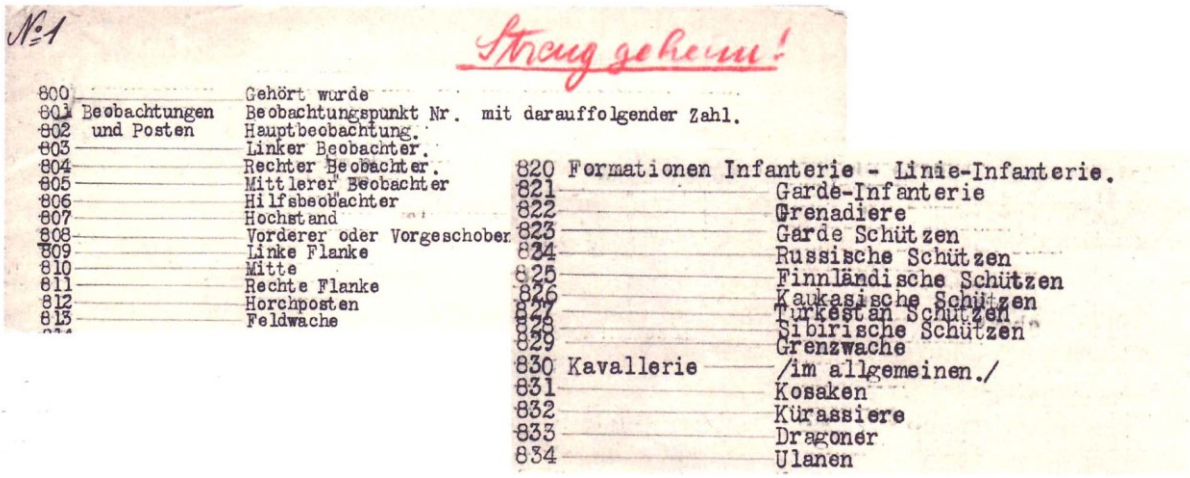
Abbildung 15: Feldtelegraphenapparat M. 1892, Erzeugnis Leopolder & Sohn.

Die rasante technische Entwicklung des Telephons und das dadurch entstandene staatliche Telephonnetz machte sich das Militär zu Nutze. Im Ersten Weltkrieg war das Staatstelephon unverzichtbarer Bestandteil des militärischen Verbindungswesens. Die Angelegenheiten des Staatstelegraph wurde in technischer und organisatorischer Hinsicht durch die Telegraphenverwaltung wahrgenommen. Das Personal des Reservetelegraphen war für die Aufrechterhaltung der vielen technischen Einrichtungen wie Telephon– und Fernschreibzentralen, Vermittlungen, Fernämter, Verstärkerämter etc. von immenser Bedeutung.[220] Auch die Erzählung im Zusammenhang mit der neuen Chiffriermethode im Militärzug auf der Reise an die Front in Galizien, in die der brave Soldat Schwejk verwickelt war (Seite 2), enthält die Beschreibung der Übertragung der verschlüsselten Depesche per Telephon vom Stab zum Bataillon und weiter telephonisch vom Bataillon zur Kompanie.

Zum Abhören feindlicher Telephon– oder Telegraphennetze wurde der *Spezialtelephondienst* eingerichtet. Die Tätigkeit der *SpeTelfStationen* beschränkte sich auf das Abhören feindlicher Gespräche mit Vermittlung der Erde, was bei Verwendung von Telephon–Einfachleitungen oder bei einer Linienführung, die eine genügende induktive Fernwirkung erzeugt, möglich war. Der Telephonabhorchdienst und der Radioabhorchdienst waren in Verbindung mit den

[218] *Prikowitsch*, Telegraph und Telephon, Bd. 1, 27.
[219] *Prikowitsch*, Telegraph und Telephon, Bd. 1, 32.
[220] *Prikowitsch*, Telegraph und Telephon, Bd. 1, 142.

Dechiffrierdiensten bei den Armeekommanden besonders im Stellungskrieg wichtige Dienste zur Nachrichtenbeschaffung.[221]


№1

Streng geheim!

800 Gehört wurde
801 Beobachtungen Beobachtungspunkt Nr. mit darauffolgender Zahl.
802 und Posten Hauptbeobachtung.
803 Linker Beobachter.
804 Rechter Beobachter.
805 Mittlerer Beobachter
806 Hilfsbeobachter
807 Hochstand
808 Vorderer oder Vorgeschober
809 Linke Flanke
810 Mitte
811 Rechte Flanke
812 Horchposten
813 Feldwache

820 Formationen Infanterie - Linie-Infanterie.
821 Garde-Infanterie
822 Grenadiere
823 Garde Schützen
824 Russische Schützen
825 Finnländische Schützen
826 Kaukasische Schützen
827 Turkestan Schützen
828 Sibirische Schützen
829 Grenzwache
830 Kavallerie /im allgemeinen./
831 Kosaken
832 Kürassiere
833 Dragoner
834 Ulanen

Abbildung 16: Der von der russischen Artillerie verwendete Ziffernkode mit Zahlen von 800 bis 988 wurde komplett entziffert.

Die lückenlose Ermittlung eines feindlichen Ziffernkodes zeigte die traditionelle Leistungs–fähigkeit österreichischer Dechiffranten in sprachlicher und kryptoanalytischer Hinsicht und erinnert an die Kryptoanalysten in der Ziffernkanzlei beziehungsweise in der Ziffernsektion.

[221] *Prikowitsch*, Telegraph und Telephon, Bd. 1, 268f.

6 Entwicklung der Chiffren–Schlüssel für die Telegraphie

Mit der Einführung der Telegraphie Ende der 1840er Jahre wurde die Übertragung von Informationen, außer den Eisenbahnunternehmen, auch den Korrespondenzbüros, offiziellen Stellen sowie der breiten Öffentlichkeit zugänglich gemacht. Die Entwicklung der Chiffren–Schlüssel für die neue Technik wird daher hier in einem eigenen Kapitel, dem Hauptkapitel dieser Arbeit, untersucht, da der Text der Nachrichten im Unterschied zu einem Brief nicht verschlossen, sondern in einer offenen Form dem Beamten an der Aufgabestation übergeben werden musste. Der Inhalt der Nachricht war nach der Übertragung zumindest den beiden Telegraphenbeamten an der Aufgabe– und an der Empfangsstation bekannt. Obwohl die Telegraphenbeamten zur Verschwiegenheit verpflichtet waren, so wollte weder ein Privatmann, noch eine Behörde oder eine Regierung, offene Briefe versenden, oder durch den Telegraphisten im Klartext schreiben lassen. Die Personen oder Institutionen, die den Telegraphen benutzten, haben daher zur Verschlüsselung der Schrift gegriffen.[222] Dies bedeutete die Entstehung und Verwendung vieler unterschiedlicher Chiffren–Schlüssel.

1849 veröffentlichte C.L. Meissner, Professor der „Ingenieur–Wissenschaft am Collegio Carolino“ und Mitglied der „Herzoglichen Eisenbahn–Commission zu Braunschweig“, eine Anleitung für die „Correspondenz in Chiffern“, um das bisher Briefe–schreibende Publikum mit der praktischen Seite zur Benutzung der telegraphischen Anstalten vertraut zu machen. Bemerkenswert ist dabei die Entwicklung einer Verschlüsselungsmethode für Braunschweig und Preußen, die aus einem grammatikalischen und lexikalischen Teil besteht und damit der Entwicklung eines Chiffren–Schlüssels für gehobene Ansprüche in Wien sehr ähnlich ist.

6.1 Chiffren–Tafeln aus Braunschweig und Preußen

Als einfachstes Chiffren–System konnte ein Geheimtextalphabet dadurch erzeugt werden, dass die Buchstaben gegenüber dem Alphabet zum Beispiel um drei Buchstaben verschoben wurden, wodurch ein Text unter Verwendung der neuen Reihenfolge der Buchstaben den Sinn verlor. Es handelte sich dabei um die bereits von Caesar benützte und nach ihm benannte Caesar–Verschiebung. Um den täglichen Gebrauch dieses monoalphabetischen Chiffren–Systems zu erleichtern, konnte an einer runden Dose, zum Beispiel einer Schnupftabakdose, sowohl die äußere Seitenwand des Deckels als auch die äußere Seitenwand des Unterteils, in

[222] *Meissner*, Die Correspondenz in Chiffern, 6.

so viele Teile geteilt werden, als der Telegraphenapparat in der Lage war, verschiedene Zeichen, Buchstaben und Zahlen, zu übertragen. In diese Felder konnte man die Buchstaben des Alphabets und die Zahlen 1, 2, 3 bis 0 schreiben. Durch Verdrehen des Deckels auf der Dose war jede mögliche Verschiebung der beiden Buchstabenreihen zueinander möglich. Zur Erinnerung der Verschiebung notierte man den Name des Korrespondenten oder die verabredete Signatur der Korrespondenz auf dem Deckel. Dieses Chiffren–System war zwar leicht anwendbar und hatte wohl in vielen Fällen genügt, brauchte aber so viele Buchstaben wie die Nachricht selbst, und da der Tarif für die telegraphische Beförderung nach Anzahl der Zeichen bemessen wurde, kam das Porto für solche Mitteilungen etwas hoch zu stehen.[223]

Geheimnisse, welche unter keinen Umständen in die Hände Unbefugter gelangen sollten, konnten keinesfalls nach diesem einfachen System übertragen werden. Es wurde daher ein System empfohlen, welches eine Entzifferung einer Depesche nur Demjenigen möglich machte, welcher im Besitze des zwischen den Korrespondenten festgesetzten Chiffren–Schlüssels war. Zugleich waren in diesem System Veränderungen möglich, obwohl die telegraphischen Geräte nur 23 verschiedene Zeichen übertragen konnten, die dem Alphabet entnommen wurden, wobei »i« mit »j« gleich gesetzt wurde und die Buchstaben »x« und »y« entfielen. Für eine vollständige Korrespondenz waren 25 Tafeln erforderlich, was 23 x 23 x 25 = 13.125 verschiedener Chiffren ermöglichte und überdies eine Einsparung in der Anzahl der übertragenen Buchstaben (Zeichen) von 12 bis 50 % ergab. Die Einrichtung der Chiffren–Tafeln beruhte darauf, dass jede Tafel gleich viele vertikale und horizontale Kolumnen enthielt, die den verschiedenen Zeichen auf der Zeichenscheibe des Telegraphen entsprachen. In den Kreuzungspunkten der Kolumnen entstehenden Feldern waren nun ein großer Teil für die deutsche Sprache erforderlichen Worte enthalten und jedes Feld bzw. Wort, welches in diesem Feld geschrieben stand, wurde mit zwei Buchstaben bezeichnet, wovon der erste im horizontalen Titelfeld und der zweite am linken Rand der Zeilen stand. Die Ziffernblätter des Königlich Preußischen und der Herzoglich Braunschweig'schen Telegraphen waren gleich und verwendeten für die telegraphischen Chiffren folgende 23 Zeichen:

a b c d e f g h i k l m n o p q r s t u v w z .

Das Chiffren–Buch war daher nur auf diese 23 Zeichen aufgebaut und jede Tafel, außer den Randkolumnen, mit 23 x 23 = 529 Feldern versehen.[224]

[223] *Meissner*, Die Correspondenz in Chiffern, 7.
[224] *Meissner*, Die Correspondenz in Chiffern, 8f.

Anlage A.

A lo	a	b	c	d	e	f	g	h	i	k	l	m	n	o	p	r	s	t	u	v	w	z	·
·	Praesens indicativi singul. I	Imperfect. indicativi sigul. I	Futurum indicativi singul. I	Perfectum indicativi singul. I	Plusquamp. indicativi singul. I	Fut. exact. indicativi singul. I	Imperfect. conjunctivi singul. I	Plusquamp. conjunctivi singul. I	1	6	Imperativ singularis	Infinitiv. praesens	a	b	c	d	e	f	ie	opponiren	sanctioniren	thätig	voran
z	Praesens indicativi singul. II	Imperfect. indicativi singul. II	Futurum indicativi singul. II	Perfectum indicativi singul. II	Plusquamp. indicativi singul. II	Fut. exact. indicativi singul. II	Imperfect. conjunctivi singul. II	Plusquamp. conjunctivi singul. II	2	7	Imperativ pluralis	Infinitiv. praeteritum	g	h	i	j	k	l	ei	Optik	sanft	Thatsache	voran sein
w	Praesens indicativi singul. III	Imperfect. indicativi singul. III	Futurum indicativi singul. III	Perfectum indicativi singul. III	Plusquamp. indicativi singul. III	Fut. exact. indicativi singul. III	Imperfect. conjunctivi singul. III	Plusquamp. conjunctivi singul. III	3	8	Imperativ „Sie"	Participium	m	n	o	p	q	r	?	Orakel	satt	thauen	voran-tragen
v	Praesens indicativi plural. I	Imperfect. indicativi plural. I	Futurum indicativi plural. I	Perfectum indicativi plural. I	Plusquamp. indicativi plural. I	Fut. exact. indicativi plural. I	Imperfect. conjunctivi plural. I	Plusquamp. conjunctivi plural. I	4	9	Passivum	Adjectivum von:	s	t	u	v	w	x	.	Orden	sauer	Thauwind	voran-ziehen
u	Praesens indicativi plural. II	Imperfect. indicativi plural. II	Futurum indicativi plural. II	Perfectum indicativi plural. II	Plusquamp. indicativi plural. II	Fut. exact. indicativi plural. II	Imperfect. conjunctivi plural. II	Plusquamp. conjunctivi plural. II	5	0	Comparativ von:	Superlativ von:	y	z	ck	ch	sch	st	Menge	ordentlich	saugen	Theater	vorar-beiten
t	Praesens indicativi plural. III	Imperfect. indicativi plural. III	Futurum indicativi plural. III	Perfectum indicativi plural. III	Plusquamp. indicativi plural. III	Fut. exact. indicativi plural. III	Imperfect. conjunctivi plural. III	Plusquamp. conjunctivi plural. III	ä	ö	Substantiv nom. singul. von:	Substant. nom. plur. von:	fs	th	pf	ph	ü	tz	Mensch	ordinair	saumselig	Thee	vorauf
s	Praesens indicativi „Sie"	Imperfect. indicativi „Sie"	Futurum indicativi „Sie"	Perfectum indicativi „Sie"	Plusquamp. indicativi „Sie"	Fut. exact. indicativi „Sie"	Imperfect. conjunctivi „Sie"	Plusquamp. conjunctivi „Sie"	erfinden	erzählen	Substantiv. genit-singul. von:	Substant. genit. plur. von:	fließen	gefangen	Gesetz	Grund	hindern	irgend	miethen	ordnen	schaden	theeren	voraus
r	ab	aufgeben	bekleiden	bilden	Concept	denn	edel	einzig	erfolgen	Erzherzog	Substantiv. dativ-singul. von:	Substant. dativ. plur. von:	fließen	geflissen	gesetzt	grüssen	hinein lassen	irren	mit	Ort	Schadhaftigkeit	theilen	voraus-laufen
p	abarbeiten	aufgeber	belieben	binden	copiren	den Vorzug haben	ehe	Eisen	erfordern	es	Substantiv. accus. sing von:	Substantiv. accus. plur. von:	flüssig	gegen	Gesinnung	gültig	hingehen	ist	mittelst	Papier	scheiden	tel	vorlesen
o	absenden	ausser	bemerken	bis	Correspondent	Depesche	ehren	electrisch	ergänzen	euer	Tafel A	Tafel B	fordern	gegen einander	Gespräch	gut	hingehen	keine	mittheilen	passen	scheinen	telegraphiren	vorschreiben
n	absender	ausser der Regel	bemühen	bis auf Weiters	correspondiren	der	ehrlich	Electricität	ergeben	ewig			formen	Gegenklage	gestalten	Gutachten	hinnehmen	kommen	mittlerweile	peinigen	schreiben	Telegraph	vorsehen
m	absetzen	Bahn	benachrichtigen	blättern	da	dergleichen	eifern	Element	ergreifen	Fach			förmlich	gegenreden	gestatten	Güte	hinschreiben	können	müde	Pfahl	sehen	telegraph. Bureau	vorziehen
l	absicht	bald	benehmen	Blatt	dabei	die ersten	Eigenschaft	empfangen	erhaben	Factor			fort	gegenwärtig	gesund	gute Groschen	hinsehen	kosten	müssen	pfeifen	sehr	tragen	wagen
k	adressat	Bank	benützen	blau	dafür	des	eilen	Empfänger	erheben	fähig			fortfahren	Gehalt	getrauen (sich)	haben	hinten	kräftigen	müssig	Pfennig	sein	trügen	wegen
i	adressiren	barmherzig	berathen	bleiben	dafür halten	deshalb	ein	empfinden	erhoben	fahren			forthelfen	geheim	gewährleisten	habhaft	hinterher	kreuzen	muthig	pflastern	setzen	üben	weggehen
h	alle	bauen	beraubcn	blenden	dagegen	deutlich	einbringen	empor	erinnern	fallen			fortkommen	geheim halten	Gewerbe	haften	hinterlassen	kühn	möglich	plätten	sichern	über	wehren
g	aller	beabsichtigen	bereden	blühen	daher	deutsch	eindringen	enden	erkennen	falsch			fortschaften	gehen	gewichtig	halb	hinter sich	kurz	nach	Polizei	sicherlich	übermässig	weit
f	allerseits	Beamter	bereiten	bohren	dahin	dicht	eine	eng	erklären	fangen			fragen	gehorchen	gewinnen	halbiren	hinwegnehmen	in kurzer Zeit	nachdem	Porto	sich rechtfertigen	übereinstimmen	wenig
e	alles	bearbeiten	bereits	borgen	damit	die	einem	entfernen	erlangen	Farbe			frankiren	gelb	gewiss	halten	hinwenden	lachen	nachdenken	pressen	sistematisch	um	wenn
d	als	Bedacht nehmen	bergab	Botenlohn	dann	dienen	einen	entheben	erlassen	fassen			Frau	Geld	Gewissensfreiheit	Hand	hinzu	laden	nachfragen	Privatnachricht	so	umkehren	wichtig
c	alsbald	bedenken	bergauf	braun	daran	diese	einer	entrichten	erlauben	fast			fréeh	gelten	gewogen	handhaben	hoch	lagern	nachlassen	putzen	sogar	um zu	wohnen
b	also	bedeuten	berühren	brechen	darauf	diesem	eines	entsagen	ermächtigen	faulen			frei	gemach	gewöhnen	handeln	hochmüthig	Land	nachreden	quälen	solche	un	wollen
a	alt	bedienen	beschlagen	Brief	darlegen	diesen	einlegen	entsetzen	ermessen	Feder			fremd	gemein	gierig	hängen	hoffen	lang	namentlich	quer	solchem	unaufschieblich	Wort

Abbildung 17: Anlage A als Beispiel aus dem 25-seitigen Chiffren-Buch.[225]

[225] *Meissner*, Die Correspondenz in Chiffern, 12.

Zur Darstellung der Methode wird aus dem Chiffren-Buch eine Tafel als Beispiel abgebildet, die die Beschriftung *Anlage A* (siehe Seite 86) trägt. Die deutsche Sprache beinhaltet sehr viele Zeitwörter, welche in allen Zeitformen, Personen- und Wortbiegungen gebraucht werden. Zur Einsparung von Zeichen, womit eine Verkürzung der Übertragungszeit angestrebt wurde, ist auf jeder Tafel eine gewisse Anzahl von Feldern zur Angabe der Zeitwörterformen bestimmt.

So bedeutet auf der als Beispiel eingefügten Tafel A:

a. das Praesens indicativi singulari 1. Person irgend eines Zeitwortes.
lo die Tafel A;
Auf der Tafel A. bedeutet: hl das Zeitwort empfangen, folglich a.hl ich empfange.
br das Zeitwort aufgeben, folglich a.br ich gebe auf, a.fd ich diene.
az bedeutet die zweite Person von dieser gegenwärtigen Zeit, also azhl du empfängst.
azch du beraubst; azen du korrespondierst.
aw die dritte Person der gegenwärtigen Zeit in der einfachen Zahl,
also awim er ergreift; awns er flieht.
av das Praesens indicativi plur. I. Person, also avss wir hindern, u. s. w.
auss ihr hindert. atss sie hindern. asss Sie hindern.
b. das Imperfectum indicat. I. Person irgend eines Zeitwortes.
kf das Zeitwort fangen, also b.kf ich fing; bzkf du fingst; bwkf er fing; bvkf wir fingen.
budi ihr bliebet; btei sie hielten dafür; bssf Sie nahmen hinweg.
c. Futurum indicat. I. Person singularis
c.br ich werde aufgeben, czhi du wirst empfinden; cwnk er wird fortfahren.
csnk sie werden geheim halten; d.nk ich habe geheim gehalten. dvnk wir haben geheim gehalten.[226]

Sollte die Zeitform in leidender Art, im Passivum, ausgedrückt werden, so wird den vier Buchstaben noch das Zeichen für „Passivum“ vorangestellt, z.B. »lvfvhe« er wird entfernt (worden) sein. Für die aktive Form ist keine besondere Bezeichnung erforderlich. Findet sich das Wort, welches chiffriert werden soll, nicht auf der ersten Tafel, so wird es auf einer anderen Tafel gesucht und gilt das Zeichen dieser Tafel, welches zugleich für alle folgenden Wörter gilt, wenn sie auf der gleichen Tafel zu finden sind.

Ein verschlüsselter Text »lo av ul mo wd lo tm«, der aus 14 Buchstaben besteht, ergibt den als Klartext aufgelösten Inhalt „Wir müssen verschweigen können“ mit 27 Buchstaben, was eine Verkürzung der Übertragungszeit von etwa 48 % ergibt.

Eine Verschlüsselung bzw. Entschlüsselung erfolgt nach folgender Vorgangsweise:
»lo« (Tafel A) »av« (Praesens indicat. Plur. I. Person) Wir »ul« müssen »mo« (Tafel B) »wd« verschweigen »lo« (Tafel A) »tm« können.

[226] *Meissner*, Die Correspondenz in Chiffern, 9.

Die meisten Zeitwörter lassen ferner die Ableitung eines Hauptwortes (Substantivum) oder auch eines Eigenschaftswortes (Adjectivum) zu, zum Beispiel: Benachrichtigung oder Nachricht von dem Zeitwort benachrichtigen, Benutzung von benutzen, Schrift von schreiben, voraussichtlich von voraussehen u. s. w.

Damit die Tafeln nicht alle von Zeitwörtern abgeleiteten Substantiva und Adjectiva aufgefüllt werden müssen, ist in jeder Tabelle die Bezeichnung *Substantivum* und zwar für alle vier Endungen der einfachen und der vielfachen Zahl, ebenso auch die die Bezeichnung *Adjectivum* enthalten, welche dem betreffenden Zeitwort vorgesetzt wird, zum Beispiel:

»ltim« die Ergreifung, »lssp« der Hingebung, »mtuo« die Mitteilungen bzw. »mvtg« kürzlich, »mvwn« schriftlich und »mvda« brieflich.
In gleicher Weise ist zur Bezeichnung der zweiten und dritten Vergleichsstufe, Comparativ und Superlativ, die nötige Vorsorge getroffen und es wird auf der Tafel A »luth« kühner, »muth« kühnsten bzw. »luuh« möglicher und »muuh« möglichsten bezeichnen.

Weil aber auf den Chiffren–Tafeln nicht alle Worte oder Namen angeführt werden können, so ist auf den meisten Tafeln, auch auf der Mustertabelle, das deutsche ABC und auch die Zahlenreihe von 1 bis 0 enthalten, um fehlende Worte oder Ziffernsätze auszudrücken. In diesen Fällen wird es zu einer Verschwendung von Buchstaben führen, da für jeden Buchstaben und jede Zahl zwei Buchstaben gegeben werden müssen. Die Worte sind auf den 25 Tabelle alphabetisch geordnet um das Nachschlagen beim Chiffrieren zu erleichtern. In leere Felder können Ausdrücke und Worte, die zwischen den beiden Korrespondenten öfter gebraucht werden, noch in beiden Exemplaren nachgetragen werden. Ankommende Depeschen, die in Chiffren geschrieben sind, werden mit Hilfe der gleichen 25 Tafeln dechiffriert.[227]

6.2 Chiffrieranleitungen und Methoden in Wien

Wie bereits im dritten Kapitel beschrieben wurde, war eine der „Sektion für Chiffrewesen und translatorische Arbeiten im Ministerium des Äußern“ ab Juni 1849 zugeteilten Aufgaben die Konstruktion der Ziffernschlüssel für die eigene Korrespondenz mit den auswärtigen diplomatischen Vertretungen. In der Zeit von der Genehmigung der Errichtung der

[227] *Meissner*, Die Correspondenz in Chiffern, 10f.

„Ziffernsektion“ im Juni 1849, bis man 1853 daranging, den geheimen Dienst in großem Stil zu reorganisieren, waren Prantner und Schneid, ehemalige Beamte der im April 1848 aufgelassenen „Ziffernkanzlei“, vorübergehend als *Translatoren für ungarische Angelegenheiten* beschäftigt. In diese Zeit fällt die Ausarbeitung eines neuen Chiffrier– und Dechiffrierbuches, zu dem die folgende Anleitung gehört. Dem Fragment einer Kopie mit der Anleitung zu diesem neuen Chiffrier- und Dechiffrierbuch vom 30. März 1850 „ad 2227“, deren Ränder Brandspuren aufweisen, wodurch einige Wörter fehlen, ist zu entnehmen, dass diese Bücher ebenfalls einen grammatikalischen und einen lexikalischen Teil enthielten.[228]

Der lesbare Teil der Beschreibung für das Chiffrier– und Dechiffrierbuch beginnt wie folgt:

„Copia ad 2227 1850
Das Chiffrier und Dechiffrierbuch besteht aus einem grammatikalischen und einem lexikalischen Theile.
Der grammatikalische Theil enthält nebst den …
1. die einsilbigen Formwörter
2. ″ mehrsilbigen Formwörter
3. ″ Abänderungsformen
4. ″ Abwandlungsformen der Hilfszeitwörter
5. ″ ″ ″ des Zeitwortes „leben …

als Muster für die übrigen dient.
Für jede dieser zur Wortfügung erforderlichen …
die entsprechenden Ausdrücke in besonderen Tabelle…
gestellt. Jede derselben ist mit der ihren Inhalt…
den Uiberschrift versehen, und enthält in de…
durch Horizontallinien getrennten Zeilen die v…
den Worte alphabetisch geordnet.
Die Tabellen für ein und mehrsilbige Formwörter haben keine Pagina „ Zahl, wogegen alle übrigen als …
eine Zahl führen, welche immer aus 3 gleichen Z…
steht, so dass man daran ein Kennzeichen für die Abän…
rungs- und Abwandlungsform – Tabellen besitzt.
In allen diesen Tabellen befinden sich neben den …
den einzelnen Zeilen enthaltenen Wörtern ebenfalls …
zifferige Zahlen, welche nebst der Zahl der Pagina zur Bezeichnung derselben dienen, so dass man nur die Zahl der Pagina und der Zeile anzugeben hat, um eine bestimmte Abänderungs oder Abwandlungsform zu bezeichnen. Will man dagegen nur einsilbige Formworte anzeigen, so genügen die danebenstehenden dreiziffrigen Zahlen, weil…
…alle dadurch charakterisieren, dass sie eine Null…
….den nachgesetzt haben. […].
Wien am 30. März 1850
W. Gintl m/p“[229]

Diese Anleitung beschreibt weiter die Bezeichnung von mehrsilbigen Formwörter, die ebenfalls durch vorangestellte dreistellige Zahlen charakterisiert werden. Im lexikalischen

[228] OeStA/AVA Inneres, MdI Präsidium A 1188, Anleitung Chiffrierbuch, Mappe 2227 1850.
[229] OeStA/AVA Inneres, MdI Präsidium A 1188, Anleitung Chiffrierbuch, Mappe 2227 1850.

Teil werden zur Bildung von Sätzen ganze Phrasen alphabetisch geordnet, die durch die Zahl der Pagina und Zeile auffindbar waren. Eine Dechiffrierung wurde im umgekehrten Verfahren der Chiffrierung durchgeführt.

Die Chiffren wurden im Gegensatz zu der Version aus Braunschweig, nicht mit zwei, vier oder sechs Buchstaben, sondern in Zahlen ausgedrückt, sind aber dem Inhalt der oben beschriebenen Methode hinsichtlich der Verwendung eines grammatikalischen und lexikalischen Teiles sonst sehr ähnlich. Der Inhalt der Anleitung gibt Aufschluss über die Entwicklung der Chiffriertechnik für die telegraphische Übertragung, die mit der Beschreibung aus Braunschweig ergänzt werden kann. Darüber hinaus fehlt in der Beschreibung aus Wien eine Einschränkung auf 23 Zeichen. Es ist bereits die Verwendung der „Morse-Taste" zu vermuten, wodurch alle Buchstaben, Ziffern und Satzzeichen übertragen werden konnten. Im Deutsch–Österreichischen Telegraphen–Verein wurde ab 1. Juli 1852 das Morsealphabet verpflichtend eingeführt.[230]

Das genannte Chiffrier– und Dechiffrierbuch, zu dem diese Beschreibung und Anleitung vom 30. März 1850 geschrieben wurde, konnte weder in Wiener Archiven noch in der Österreichischen Nationalbibliothek gefunden werden. Es muss sich aber um ein groß angelegtes Werk handeln, das aus vielen Seiten bestand, weil chiffrierte Wörter auch die Seitenzahl, die Pagina, und die Zeilenzahl enthielten. Ausländische Missionen bedienten sich diesem Chiffrier– und Dechiffrierbuches für telegraphische Depeschen, sobald eine Telegraphenleitung nach Wien zur Verfügung stand.

Die Verwendung der neuen Chiffrierbücher ist dem Telegramm 369/MJ.–85 vom 5. Jänner 1854 an Dr. Alexander Bach zu entnehmen, in dem Mamulay Imrey die Fertigstellung der Telegraphenleitung von Wien nach Agram meldet und um die Benützung des Chiffren–Schlüssels anfragte.

> „Wie Eurer Excellenz bekannt sein dürfte, wird die Telegraphen-Verbindung hier bis Agram in der kürzesten Zeit in Wirksamkeit treten. Da ich für die geheime Korrespondenz mit Eurer Excellenz mit einem Chiffrierschlüssel nicht versehen bin, und nur einer für die Korrespondenz und den Chef der löblichen Polizei-Behörde mir zu Gebote steht, so erlaube ich mir ehrerbietlichst zu erfragen, ob ich mich diesen letzten Schlüssel bedienen soll, […]."[231]

[230] *Gerke*, Der Elektro-Magnetismus, 11.
[231] OeStA/AVA Inneres, MdI Präsidium A 1188, Mappe 369/1854 M.I.

Ein weiterer Ziffernschlüssel mit der Bezeichnung „Deutscher Chiffre No 478/3“, dessen Herkunft unbekannt ist, liegt vom 12. November 1860 vor, der für Briefe aber auch für telegraphische Depeschen, für untergeordnete Zwecke, ausgearbeitet und verwendet wurde. Dieser vierstellige Chiffren–Schlüssel besteht aus insgesamt 2915 Chiffren, die auf 27 Seiten festgehalten sind. Die Zahlen von 1001 bis 3700 beinhalten 2700 Buchstaben, Silben und Wörter in alphabetischer Reihenfolge, während den Zahlen von 3701 bis 3916 geographische Bezeichnungen und spezifische Eintragungen zugeordnet waren.[232]

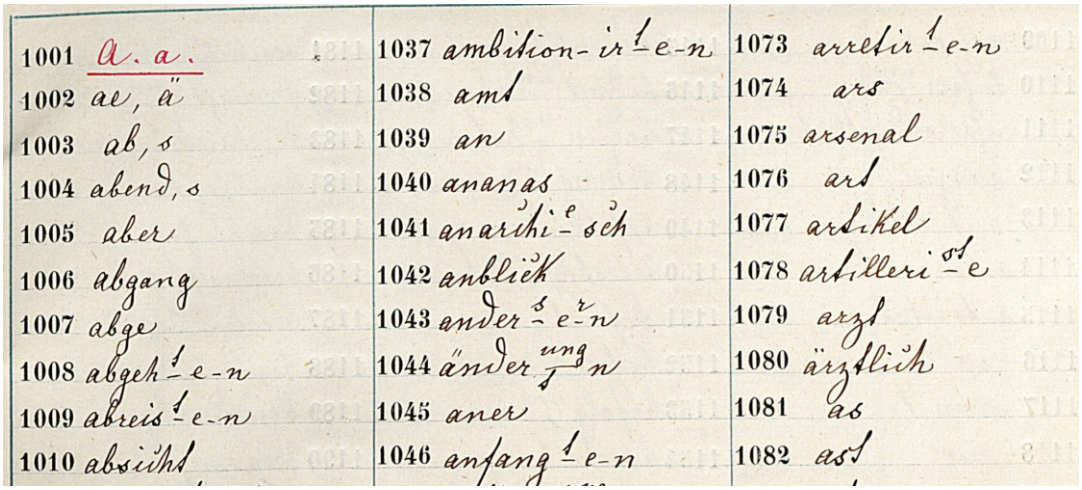

1001 a. a.
1002 ae, ä
1003 ab, s
1004 abend, s
1005 aber
1006 abgang
1007 abge
1008 abgeh ! e-n
1009 abreis ! e-n
1010 absicht
1037 ambition- ir ! e-n
1038 amt
1039 an
1040 ananas
1041 anarchi- e sch
1042 anblick
1043 ander- s e- r n
1044 änder- ung s n
1045 aner
1046 anfang ! e-n
1073 arretir ! e-n
1074 ars
1075 arsenal
1076 art
1077 artikel
1078 artilleri- st e
1079 arzt
1080 ärztlich
1081 as
1082 ast

Abbildung 18: Die ersten 10 Zeilen der Seite 1 des Ziffernheftes, das insgesamt 27 Seiten umfasst.

Dem Beginn der vierstelligen Chiffren im vorstehenden Tabellenauszug aus dem Ziffernheft ist die alphabetische Reihenfolge der Buchstaben, Silben und Wörter zu entnehmen. Viele Chiffren haben mehrere Bedeutungen, wie zum Beispiel die Zahl 1043, die für folgende vier Begriffe verwendet werden konnte: *anders, andere, anderer* und *anderen*. In diesem einfachen Diktionär ist kein grammatikalischer Teil enthalten.

Die Anleitung mit einem praktischen Beispiel lautet wie folgt:

> „Deutscher Chiffre No 478/3.
>
> Der gegenwärtige deutsche Ziffernschlüssel ist sowohl für die telegraphische als die gewöhnliche Correspondenz geeignet. Er enthält das Alphabet, die Silben, die gebräuchlichen Worte, die Wochentage, Monate, Zahlen, Unterscheidungszeichen, dann die entsprechenden Namen der Länder, Städte, Flüsse und Personen, so dass man damit alles schreiben kann, was man will.
>
> Dieses, 2700 Bedeutungen (von 1001 bis 3700) umfassende Ziffernheft dient gleicher Maßen zum Chiffrieren und Dechiffrieren der Depeschen oder Briefe, da die alphabetisch geordneten Bedeutungen und die arithmetisch geordneten Zahlen das Auffinden derselben sehr leicht machen.

[232] OeStA/HHStA StK Interiora 21 (alt ad 27), Chiffrenschlüssel, Mappe 12. November 1860.

Die Unterscheidungszeichen müssen richtig angebracht werden, um den Sinn des Geschriebenen nicht zweifelhaft zu machen. Die Zahl 3474 „Umlautzeichen“ wird benützt, wenn man bei einem Worte das a in ä, das o in ö, das u in ü oder den Doppellaut au in äu verwandeln will.

Wünscht man bei einem Worte die einfache oder die vielfache Zahl genau anzugeben, so bedient man sich im ersten Falle der Zahl 3475 und im zweiten Falle der Zahl 3470, welche die einfache und vielfache Zahl anzeigen.

Die Zahlen 3477 bis inclusive 3484, dann 3696 bis inclusive 3700 bedeuten nichts und werden ganz nach Belieben zwischen die, eine Bedeutung habenden Zahlen gesetzt, um diese letzteren besser zu verbergen.

Die noch leer gelassenen Zahlen von № 3701 bis 4024 können benützt werden, um beliebige Worte, Namen u.s.w. nachträglich hinein zu setzen.

Um einem Missverständnisse vorzubeugen, müssen jedoch die neuen Bedeutungen in beide Exemplare eingetragen werden.

Die nachfolgenden chiffrierten Zeilen mögen als Beispiel dienen, wie man diesen Chiffre anwendet. _____“[233]

„Heute so eben 2 Uhr mittags sind wir in Madeira glücklich
1955.2833.1545.3422.3063. 2338. 2826.3278.2031. 3534. 1877.

ange-kommen |.| -----
1049. 2147.3468.3482.

Die See- Reise habe ich ganz gut über-standen |.| -----
1477.2796.2663.1914.1996.1776.1908.3050. 2870.3466.3700.

Clima hier herr- lich |.| tropische Gewächse in schön-ster
1324.1959.1959.2229.3465. 3028. 1856. 2031.2776.2878.

Blüt- |:Umlautzeichen:|-he |.| Ganze su- ite gesund ----- |.|
1229. 3474. 1939.3468.1776.2909.2068.1853.3699.3468.

Brief-e |:Vielfachzeichen:|aus Wien und Poßenhofen durch englischen
1247. 3476. 1103.3596.3076. 3562. 1533. 3510.

Consul erhalten |.|
1356. 1615. 3481.“[234]

Einfachere Ziffern–Schlüssel hatten den Zweck, den Zeitaufwand für Telegramme geringerer Wichtigkeit in der Chiffrierung und Übertragung zu verkürzen.

Ferdinand Prantner stellte 1869 fest, dass die vorhandenen französischen und deutschen Chiffren einerseits für den Gebrauch mit den eigenen Missionen bereits ungenügend wären und die Herstellung neuer Diktionärs notwendig und auch zweckmäßig schien. Mit den im Zifferndienst gewonnenen reichen Erfahrungen auf dem Gebiete der Kryptographie könnten die bisherigen Chiffriermethoden durch ein neues Verfahren ersetzt werden. Die damals verwendeten Diktionäre boten nicht ausreichende Möglichkeiten für ein sicheres und zugleich

[233] OeStA/HHStA StK Interiora 21 (alt ad 27), Chiffrenschlüssel, Mappe 12. November 1860.
[234] OeStA/HHStA StK Interiora 21 (alt ad 27), Chiffrenschlüssel, Mappe 12. November 1860.

präzises Chiffrieren. Nach Prantners Ansicht war eine Beschränkung auf die Zahlen von 1000 bis 9000 oder weniger, nicht gerechtfertigt, da die in einer Korrespondenz auftretenden gleichen Chiffren unterschiedliche Bedeutungen haben konnten (siehe Bemerkung zur Chiffre 1043, Seite 91). Für eine klare Chiffrierung hätte jede Bedeutung eine eigene Chiffre erfordert.[235]

In einem neuen Verfahren nahm Prantner sowohl die dreistelligen Zahlen von 101 bis 999 als auch die fünfstelligen Zahlen von 10.000 aufwärts in die neuen *Cahiers* auf. Das Suchen der Wörter im *Cahier Chiffrant*, also dem Verschlüsselungsbuch, wurde durch Verteilung zahlreicher, mit gesperrter Schrift gedruckter Leitbedeutungen, erleichtert, die die alphabetische Progression markierten. Auch wurden längere und kürzere Serien von Wörtern in jenen zusammengesetzten Bedeutungen, deren erster Teil sich unverändert wiederholte, durch rote Linien hervorgehoben. Schon das bisherige Verfahren hatte durch Anwendung verschiedener Methoden des so genannten „chiffre primitif", der teilweisen Maskierung, einen hohen Grad von Sicherheit. Als gänzlich geeignet ließ Prantner aber nur ein solches Verfahren gelten, durch das die vorhergegangenen und weiter folgenden chiffrierten Korrespondenzen gegen Kompromittierung vollkommen geschützt blieben, ohne dass in ein anderes Diktionär gewechselt werden müsste.[236]

Dies wurde dadurch erreicht, dass die im Diktionär enthaltenen Chiffren in andere Zahlen übersetzt wurden und diese Substituierung anderer Zahlen sich nach einem vom fremden Dechiffreur nicht zu eruierenden Gesetz in jeder Depesche erneuerte. Dieses Verfahren nannte Ferdinand Prantner „Transkription". Es entsprach den genannten Anforderungen in geeigneter Weise und seine Einführung hatte neben der Gewährleistung der absoluten Sicherheit auch zur Folge, dass bei sämtlichen Missionen ein einziges homogenes Verfahren an die Stelle der bisherigen Vielfältigkeit der Chiffren und des Chiffrierens trat.[237] Diese „Transkription", die zusätzliche Verschlüsselung, wird im späteren Kapitel 6.3.2 anhand der Chiffrier- und Dechiffriertabellen Nr. 8588 als „Transponiermethode" auf den Seiten 103 bis 105 im militärischen Bereich ausführlich beschrieben.

Wie erwähnt, wurde für eine rasche Übertragung von Telegrammen auf der technischen Seite im Artikel 3 des Vertrages des Deutsch–Österreichischen Telegraphen–Vereins gefordert,

[235] *Hubatschke*, Ferdinand Prantner, Buch 6, Diss., 1449.
[236] *Hubatschke*, Ferdinand Prantner, Buch 6, Diss., 1449f.
[237] *Hubatschke*, Ferdinand Prantner, Buch 6, Diss., 1450.

dass jede Depesche von der Aufgabe bis zur Adressstation so wenig als möglich „umtelegraphiert“ werden solle. Je nach Entfernung musste das Telegramm aus technischen Gründen jedoch wiederholt telegraphiert werden, was Zeit in Anspruch nahm und Kosten verursachte. Die Erklärung über ein am 30. Juni 1872 um 12 Stunden in Wien verspätet eingetroffenes Telegramm aus Paris gibt Auskunft über den zeitlichen Verlauf einer telegraphischen Depesche sowohl für die technische Übertragung als auch für die Dechiffrierung. Als Antwort auf eine Beschwerde wurde folgender Brief 13.080/II vom 31. August 1872 vom Handelsminister an das k.k. Ministerium des Äußern in Wien gesendet:

> „[…] Das fragliche Telegramm No. 90510 welches am 30. Juni um 9 Uhr 30 M. in Paris aufgegeben war, langte um 9 Uhr 45 Minuten Morgens in Bregenz an, wurde von da um 11 Uhr 15 Minuten Morgens nach Wien abtelegraphiert und dortselbst um 11 Uhr 40 Minuten Vormittags dem Depeschenträger zur Zustellung übergeben. Die Zustellung erfolgte am 30. Juni um 12 Uhr 10 Minuten Mittags an das Chiffern Department gegen den beiliegenden vom Amtsdiener Med gefertigten Empfangschein, welcher seinerzeit rückgemittelt worden wolle. […]“.[238]

Die technische Übertragung des Telegramms von Paris bis Bregenz dauerte 15 Minuten und von Bregenz nach Wien 25 Minuten, wobei die Unterbrechung bis zur neuerlichen Absendung in Bregenz 1 ½ Stunden betrug. Insgesamt ergab das eine Übertragungszeit von der Aufgabe in Paris mit einer „Umtelegraphierung“ bis zur Zustelladresse zwei Stunden und 10 Minuten. Die Zustellung an das Chiffren Departement, die Dechiffrierung selbst und die Überbringung an den Adressaten nahm neun Stunden und 20 Minuten in Anspruch. Aus diesem Vorgang ist ersichtlich, dass die Beförderung und Dechiffrierung eine längere Zeit als die Übertragung selbst benötigte, obwohl die Beamten im „Department VI“ im Ministerium des Äußern (siehe Seite 53) in ständiger Bereitschaft waren und ohne Verzögerung arbeiteten.

Außer dem mächtigen Ziffernschlüssel, der in der Ziffernsektion mit einem vielseitigen und daher umfangreichen Diktionär für die diplomatischen Dienste im Ausland entwickelt wurde, waren bei Behörden, Gendarmerie, Polizei und Militär Chiffren mit einfachen Chiffren–Tabellen oder kleinen Chiffren–Büchern mit den für den jeweiligen Bereich spezifischen Begriffen und Worten in Verwendung. Wegen der geringen Anzahl der Exemplare wurden diese handschriftlich verfasst und galten meist für einen bestimmten regionalen Bereich. Aus dieser Vielfältigkeit der Chiffriermethoden werden einige Beispiele gezeigt, die von Dienststellen in begrenzter Zahl und nur in bestimmten Ländern verwendet wurden.

[238] OeStA/HHStA AR F6-34 Karton 1, Mappe Telegraphie, Vide 4, Telegramme Brief 13.080/II vom 31. August 1872.

Chiffren–Schlüssel Kärnten:

Ein Chiffren–Schlüssel für Kärnten wurde 1898 „zum geheimschriftlichen Verkehr zwischen dem k.k. Landes-Präsidium in Klagenfurt, den k.k. Bezirkshauptmannschaften in Kärnten und dem Grenz–Polizei–Commissariat in Pontafel“[239] herausgegeben. Je ein Exemplar des Chiffren–Schlüssels wurde an das k.k. Landespräsidium in Klagenfurt, die k.k. Bezirkshauptmannschaften Hermagor, Klagenfurt, Spittal, St. Veit, Villach, Völkermarkt und Wolfsberg, das k.k. Grenzpolizei Commissariat in Pontafel und den k.k. Polizei Präsident in Wien verteilt sowie dem hohen k.k. Ministerium des Innern vorgelegt.[240]

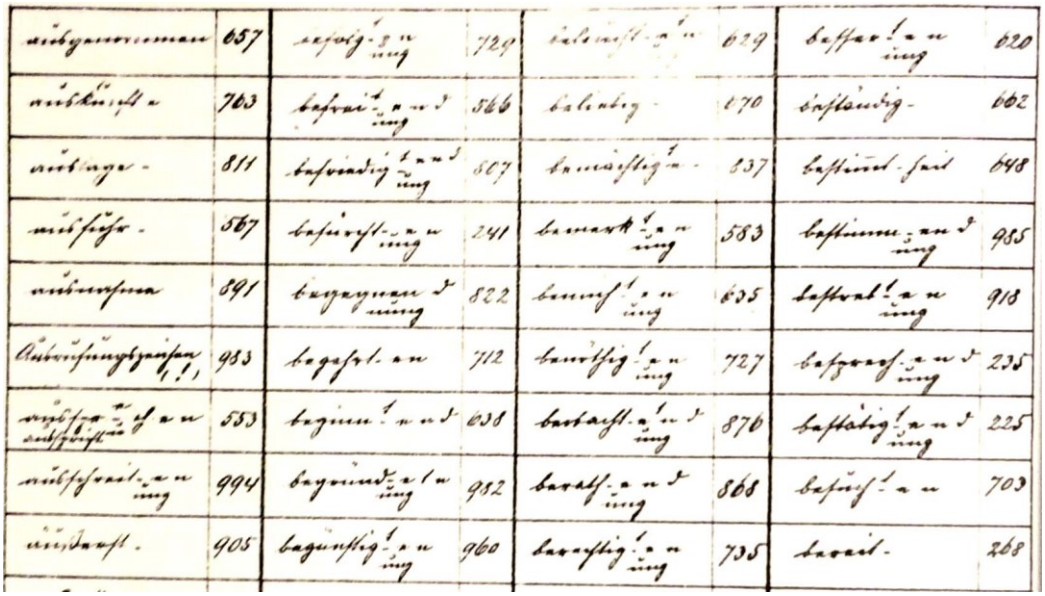


Abbildung 19: Ausschnitt aus der Chiffren–Tabelle mit Begriffen und Zahlen von 001 bis 999.

Als Beispiel wird ein Telegramm des Grenzpolizei–Commissariat Pontafel mit dem dreistelligen Chiffren–Schlüssel für Kärnten teil–chiffriert gezeigt:

> Klartext: Signalisierter Anarchist soll mit größerer Menge Dynamit Montag mit Eisenbahn von Italien dort eintreffen. Derselbe ist sogleich zu verhaften und hiesigem Landesgerichte einzuliefern. Landespräsidium.

Chiffrierter Text: 290 216 *soll mit* 588 *Menge* 526 502
(*signalisierter*) (*Anarchist*) (*größerer*) (*Dynamit*) (*Montag*)
706 318 835 243 846 *eintreffen* 251 829 184 458
(*mit*) (*Eisenbahn*) (*von*) (*Italien*) (*dort*) (Punkt) (*Derselbe*) (*ist*) (*sogleich*)
177 142 218 671 *und hiesigem* 772 218 116
(*zu*) (*ver*) (Bindezeichen) (*haften*) (*Landes*) (Bindezeichen) (*Gerichte*)
790 *einzuliefern Landespräsidium*
[gilt nur erste Bedeutung] [241]

[239] *Prikowisch*, Drahtlose Telegraphie, Bd. 2, 389.
[240] *Prikowisch,* Drahtlose Telegraphie, Bd. 2, 389.
[241] *Prikowisch,* Drahtlose Telegraphie, Bd. 2, 390.

Durch die Teil–Chiffrierung einer Nachricht war die Möglichkeit einer Kompromittierung eher gegeben als bei einer Voll–Chiffrierung.

Chiffren–Schlüssel Niederösterreich:
Der Chiffren–Schlüssel für Niederösterreich gemäß Chiffren–Buch (Praes. 2 483 XIV–13, Min. f. L.V.) bestand aus dreistelligen Zahlen für Buchstaben, Silben und kurzen Worten. Lange Begriffe wurden aus Silben und Buchstaben zusammengesetzt.

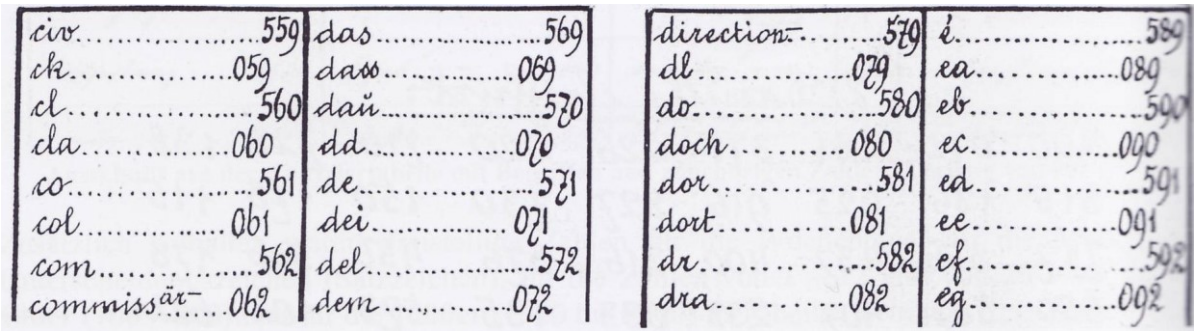

civ 559 | ck 059 | cl 560 | cla 060 | co 561 | col 061 | com 562 | commissär 062
das 569 | dass 069 | daß 570 | dd 070 | de 571 | dei 071 | del 572 | dem 072
direction 579 | dl 079 | do 580 | doch 080 | dor 581 | dort 081 | dr 582 | dra 082
e 589 | ea 089 | eb 590 | ec 090 | ed 591 | ee 091 | ef 592 | eg 092

Abbildung 20: Ausschnitt aus den Chiffren–Tabellen 4 und 5, die in Niederösterreich verwendet wurden.

Gemäß der Chiffrierinstruktion wurden die dreistelligen Chiffren für die telegraphische Übertragung in fünfstellige Zifferngruppen umgewandelt und vor der Dechiffrierung wieder in „Dreier-Gruppen“ zurückgesetzt, was dem folgenden Beispiel gut zu entnehmen ist. [242]

Klartext: Über Demonstrationen anlässlich gestriger Wahlversammlung Hainfeld, sowie über laut Zeitungen in Hainfeld und Nachbargemeinden erfolgte Verhaftungen chiffriert sofort telegraphieren. Dortiger Bericht vom 27. Oktober, Zl 325g eben erhalten.

Chiffren–Text: 400 072 281 371 026 020 716 722 138 815 136 925 916 827 730
150 178 115 717 856 437 400 216 876 456 506 178 650 507 407
253 033 135 573 101 622 916 152 907 636 508 555 182 856 123
881 181 008 505 081 173 537 420 983 995 454 971 989 470 488
986 974 590 098 101 153

Chiffren–Text in fünf Stellen abgeteilt:
40007 22813 71026 02071 67221 38815 13692 59168 27730
15017 81157 17856 43740 02168 76456 50617 86505 07407
25303 31355 73101 62291 61529 07636 50855 51828 56123
88118 10085 05081 17353 74209 83995 45497 19894 70488
98697 45900 98101 15352 [243]

[242] *Prikowisch,* Drahtlose Telegraphie, Bd. 2, 391f.
[243] *Prikowisch,* Drahtlose Telegraphie, Bd. 2, 391.

Dechiffrement:

400/07 2/281/3 71/026 020/71 6/722/1 38/815 136/92 5/916/8 27/730
über dem- on- str- ation^{en} an- lass- lich gest- ri- ger wahl-ver-sam- lung

150/17 8/115/7 17/856 437/40 0/216/8 76/456 506/17 8/650/5 07/407
ha- in- fe- ld so- wie über lau- t zeitung^{s}(pl) in h Θ und

253/ 03 3/135/ 5 73/101 622/91 6/152/9 07/636 508/55 5/182/8 56/123
nach-bar^{e}-gemein^{e}-den er-folg$^{e\text{-}n}$ ver- haft- un- gen → chiffr^{e}-irt so- fort

881/ 18 1/008/5 05/081 173/53 7/ 420/9 83/995 454/97 1/989/4 70/488
telegraf-irer ← (a/l) dort- ige bericht^{e} von 27 October Zahl 3 1000 2 100

986/97 4/590/0 98/101 153/ 52
50 9 eb- en er- halt$^{e\text{-}n}$ ~ [244]

Die Umwandlung von dreistellige in fünfstellige Chiffren ist in diesem Fall nicht mit einer zweiten Chiffrierung zu vergleichen oder zu verwechseln und obwohl die Übertragung in „Fünfergruppen" erfolgte, ist die textliche Vielfalt doch auf eine dreistellige Chiffrierung des Klartextes eingeschränkt.

Chiffren–Schlüssel Bosnien–Herzegowina:
Von der k.k. Hof– und Staatsdruckerei in Wien wurde ein Chiffren–Schlüssel mit vier Ziffern für die Bosnisch–Herzegowinische Verwaltung (Zl. 1 005 res. Ex 1887) gedruckt.[245]

gna(ä)d-ig e	2563	gre	1857
gne	2990	greif-lich t e-n	2887
gni	2878	grenz-'e-n-d	2562
gno	1855	grenzbewachung	1849
gnu, gnü	4622	grenzcordon	2884
go, gö	1426	grenzposten	1858
Gödöllö	1484	grenzregulirung	6622
gold-"en	6112	grenzsperre	4115
golja	8280	grenzstation	2984
Gomjonica	4100	grenzstreit-igkeit	2993
go(ö)nn-'e-n	4112	grenzverkehr	4625
gora	1137	grenzwache	6111
Gorazda	1465	gri-e	6107
gornj-'a-e	1461	Griech-isch e-n	6114
gornji Vakuf	8285	Griechenland	6480
gos-s	8274	griff-en	6478
go(ö) tt-lich	6110	gro	7761
gottesdienst	1427	gross	7764
gr	8288	grosses Aufsehen verursach-'e-n-d	7762
gra	6108		
grab-en	8286	grossen Einfluss besitz-'end	6759
Gračanica	7744, 7763		
grad	4118	grösser	7439
Gradačač	6474, 6501	grossgrundbesitz-er	7436
Gradiška (bosnisch)	1459	grossma(ä)cht-e	6758
graf (gräf-)	1440	grösste-r n — m — s	6751
Grahovo	1131, 1522	grösste Beschleunigung	2897
grau	1482	grösste Sorgfalt	3186
grausam-keit	1850	gru	6490
Graz	4101	grub-e-n	6489

Chiffrant

4532	4561 lik
4533 ohne ih-ren n	4562 log-en
4534 oder aber	4563 lossag-t ung en
4535	4564 lieb-'e-n
4536 officiös	4565 lig-e — m — n — r — s
4537 ok	4566 kreisbehörde in Tuzla berichtet (dass)
4538 officierstellvertreter	4567
4539 niederle(a)ge-n	4568 1903
4540 nöthig-'e-n	4569 kriech-'en-d
4541 noch mehr	4570 ks
4542 Nil	4571 ku(ü)h-e
4543 notific-ation ir-'en	4572 kop
4544 Enuntiation -en	4573 knu
4545 nuil	4574 klimm-'en
4546 nachdru(ü)ck-lich	4575 knüpft-t ung en
4547	4576 kleid-ung er
4548 nachmittag	4577 kof-f
4549 namentlich	4578 kob
4550 marschbereit-schaft	4579
4551 mehr als	4580 just-iz
4552 mässigung	4581 jung
4553	4582 kanzl-er ei
4554 massregeln (zu) ergreifen	4583 kad
4555 mappe	4584 kann er
4556	4585 spontan -e-m-n-r
4557	4586
4558	4587 kais. u. kön.
4559 lof	4588 Juni
4560 lös-t ung en	4589 kan-n

Dechiffrant

Abbildung 21: Auszug aus der Tabelle des vierstelligen Chiffren-Schlüssels, der eine Auswahl von maximal 9.999 Begriffen umfasste.

[244] *Prikowitsch,* Drahtlose Telegraphie, Bd. 2, 392.
[245] *Prikowitsch,* Drahtlose Telegraphie, Bd. 2, 393.

Dieser Schlüssel mit vierstelligen Ziffern wurde mit Ergänzungen von 1887 bis 1912 verwendet. In Friedenszeiten erfolgten Ergänzungen und Änderungen des Chiffren–Schlüssels nur in Jahresabständen. Alle Chiffren-Schlüssel enthielten auch ein Verzeichnis aller Stellen, die über den gleichen Schlüssel mit Gebrauchsanleitung verfügten.[246]

Außer den vielen unterschiedlichen Chiffren–Schlüsseln, die in den Kronländern und im Ausland angewendet wurden, zeigt das folgende Beispiel, dass es darüber hinaus für besondere Vorkommnisse zusätzliche Codierungen gab, die von allerhöchster Stelle genehmigt werden mussten, bevor sie Anwendung fanden. Es kann davon ausgegangen werden, dass die angeführten Decknamen chiffriert nach Berlin übertragen wurden.

B. Frischauer schrieb am 14. März 1888 folgenden Brief an Kronprinz Rudolf:

> „Wien, 14. März 888. Eure Kaiserliche Hoheit! Ich erlaube mir Eurer Kaiserlichen Hoheit Erlaubnis zu erbitten, über die Auslieferung und eventuellen Verhaftung des Abg. Schönerer eine Chiffren-Depesche nach Berlin senden zu dürfen, damit Eure Kaiserliche Hoheit noch Freitag in Kenntnis der interessanten Vorgänge gelangen, denen wir hier entgegengehen. Die Depesche wird an den Kammerdiener adressiert sein. Ich erlaube mir einen Schlüssel beizulegen, welcher die Depesche für alle nicht eingeweihten Personen unverständlich macht. Mit diesem Schlüssel werden Eure Kaiserliche Hoheit die Depesche leicht dechiffrieren können. Genehmigen Eure Kaiserliche Hoheit die Versicherung treuester Verehrung und Dankbarkeit. Ergebenster B. Frischauer.“[247]

> „Schlüssel für Depeschen
> Reichsrat heisst in der Depesche Getreidemarkt
> Rechte . . . . . Provinzkäufer
> Linke . . . . . Arrangeure
> Deutschnationale . . . . . Beistaende
> Regierung . . . . . Schiedsgericht der Börse
> Schoenerer . . . . . Steffens
> Polizey . . . . . Notar
> Detectivs . . . . . Schreiber
> Krawall . . . . . Tafel
> Großer Krawall . . . . . große Tafel
> Erzherzog . . . . . Josef
> Verhaftung . . . . . Verheirathung
> Auslieferung . . . . . Verlobung
> Kronprinz Rudolf . . . . . General
> Kaiser . . . . . Führer
> Richterstand . . . . . Agenten
> Beschimpfungen . . . . . Komplimente“[248]

[246] *Prikowitsch,* Drahtlose Telegraphie, Bd. 2, 393.
[247] OeStA/HHStA HausA Nl. Schlager Eckartsau, Konvolut 1, Kronprinz Rudolf, Folge 36.
[248] OeStA/HHStA HausA Nl. Schlager Eckartsau, Konvolut 1, Kronprinz Rudolf, Folge 37.

6.3 Verschlüsselung für das Militär

Aus der Sichtweise des Militärs wurde die Gefahr einer Abhörung und Entschlüsselung einer Depesche einer staatlichen Stelle als geringer eingestuft als dies auf eine telegraphische Nachricht im militärischen Bereich zutraf. Eine Korrespondenz fand weniger oft statt und die Benützer des Chiffren–Schlüssels waren Beamte der eigenen Verwaltung. Eine Durchgabe mittels Telegraph oder Telephon fand unter Aufsicht statt. Beim Militär war die Situation anders. Auch im Frieden achtete man besonders auf hohe Sicherheit und Geheimhaltung des Chiffren–Schlüssels. Man ging davon aus, dass die militärische Korrespondenz abgehört und vom Gegner mit professionellem Aufwand und Können entziffert werden konnte. Alle Chiffrierunterlagen wurden nach einer gewissen Zeit der Anwendung protokollarisch durch Verbrennen vernichtet. Durch die Größe der Armee und der damit verbundenen großen Anzahl von Unterlagen war die Überwachung der verschiedenen Chiffrierverfahren nur schwer durchführbar. In Österreich–Ungarn wurde das Chiffrierwesen schon vor dem Ersten Weltkrieg im Evidenzbüro im Kriegsministerium durchgeführt. 1907 übernahm der damalige Hauptmann des Generalstabes Max Ronge die „Kundschaftsgruppe“, deren eine der Untergruppen die Chiffriergruppe war. Dieser Chiffriergruppe gehörte ab 1911 auch Hauptmann Andreas Figl an.[249]

6.3.1 Militärschlüssel für untergeordnete Zwecke

Der folgende Schlüssel zeigt den alten österreichischen Militärchiffre, der für untergeordnete militärische Zwecke in Österreich–Ungarn bis in die 1890er Jahre im Gebrauch stand.[250]

*	a	b	c	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z	*
B	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31	32	33	34	35	36	11	B
e	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31	32	33	34	35	36	11	12	13	14	e
n	24	25	26	27	28	29	30	31	32	33	34	35	36	11	12	13	14	15	16	17	18	19	20	21	22	23	n
k	21	22	23	24	25	26	27	28	29	30	31	32	33	34	35	36	11	12	13	14	15	16	17	18	19	20	k
o	25	26	27	28	29	30	31	32	33	34	35	36	11	12	13	14	15	16	17	18	19	20	21	22	23	24	o
v	32	33	34	35	36	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31	v
a	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31	32	33	34	35	36	a
c	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31	32	33	34	35	36	11	12	c

Abbindung 22: Schlüsseltafel des österreichischen Militärs für untergeordnete Zwecke.

[249] *Prikowitsch,* Drahtlose Telegraphie, Bd. 2, 394.
[250] Johann *Prikowitsch,* Drahtlose Telegraphie in der k. (u.) k. Armee und Marine, Band 2 (Wien 2016) 395. Dazu wird als Quelle angegeben: Andreas *Figl*, Systeme des Chiffrierens (Graz 1926).

Die Anordnung erinnert an das Vigenère–Quadrat, hat aber im Gegensatz dazu nicht 26 sondern nur acht horizontale Linien für das Schlüsselwort „Benkovac“ und chiffriert die Buchstaben mit zweistelligen Zahlen und nicht mit Buchstaben wie bei Vigenère. Die Kopfzeile enthielt das Alphabet mit 26 Buchstaben und links und rechts des Zahlenfeldes wurde das Schlüsselwort „Benkovac“ senkrecht eingetragen. Das Zahlenfeld bestand somit aus acht Zeilen, in denen die Zahlen 11 bis 36 in beliebiger Reihenfolge eingetragen waren. Die verschlüsselten Zahlen wurden in „Fünfergruppen“ niedergeschrieben und telephonisch durchgegeben oder mit Morsezeichen telegraphiert.[251]

Zur Verschlüsselung wurde als nächster Schritt das Schlüsselwort „Benkovac“ unter den Klartext wiederholt bis an das Ende des Klartextes geschrieben, sodass jedem Buchstaben des Klartextes ein Buchstabe des Schlüsselwortes zugeordnet werden konnte:

S M S c h i f S a i d a l a e u f t m o r g e n s i e b e n U h r f r u e h e i n
B e n k o v a c b e n k o v a c b e n k o v a c b e n k o v a c b e n k o v a c b

Verschlüsselung: 30 27 16 23 32 14 16 31 12 23 27 21 36 32 15 33 17 34 36 35 16
12 15 26 30 23 28 22 29 19 31 20 29 20 15 15 29 13 15 21 25

Für die telegraphische Übertragung wurden nun aus den zweistelligen Zahlen fünfstellige Zahlen gebildet:

30271 62332 14163 11223 27213 63215 33173 43635 16121
52630 23282 22919 31202 92015 15291 31521 25765

Entschlüsselung: 30 27 16 23 32 14 16 31 12 23 27 21 36

b e n k o v a c b e n k o usw.
s m s c h i f s a i d a l S. M. Schiff Saida l… usw.

Dieser hier beschriebene Schlüssel mit zweistelligen Zahlen wurde durch den dreistelligen Friedensschlüssel ersetzt. Der Nachteil der zweistelligen Zahlen lag in diesem Falle darin, dass einzelne Buchstaben durch eine zweistellige Zahl verschlüsselt waren, was die Übertragungszeit des Geheimtextes verlängerte. Im militärischen Bereich wurde aber grundsätzlich eine rasche Übertragung gefordert. Der umfangreichere „dreistellige Chiffren–Schlüssel“ war für den Gebrauch von allen Kommandos, Behörden, Truppen und Truppenteilen, welche unter dem Kommando eines Offiziers standen, bestimmt und wurde in drei Sprachen ausgegeben. Telegramme und schriftliche Korrespondenz waren mit Ausnahme

[251] *Prikowitsch,* Drahtlose Telegraphie, Bd. 2, 395f.

der Adresse zu chiffrieren. Zu Beginn des Telegramms war die Sprache durch die folgenden Buchstaben, die ebenfalls zu chiffrieren waren, zu kennzeichnen: d = deutsch, m = ungarisch, h = kroatisch.[252]

Die Chiffren–Tabellen waren in drei Sprachen ausgeführt:

Verzeichnis der Sigel.

A.

Abend (abends)	852	allgemein	488
Ablösung	214	angeordnet	110
Abschnitt	990	Anstalt	658
Abteilung	615	April	997
achter	326	Armee	999
achtzehnter	621	Arrest	380
achtundzwanzigster	409	Artillerie	243
Admiral	916	Assistenz	313
aktiv	306	Attaché	694
Alarm	334	Attentat	437
Alarmierung	785	August	977
Alarmierungstag	806	Ausnahmsverfügungen	287
Albanien	410	Automobil	662
albanesisch	675	Aviso	120
Allerhöchst	770		

B.

Banus	983	Bezirkshauptmannschaft	295
Baracke	507	Bezirkswachtmeister	908
Barrikade	710	Blockhaus	729
Bataillon	139	Boot	834
Batterie	145	Bosnien	370
Befehl	346	bosnisch	998
Befestigung	666	Brigade	285
Behörde	788	Brücke	557
Bereitschaft	359	Bürgermeister	864

A jelények mutatója.

A.

adag	956	állomás parancsnok	345
ágyu	639	alosztály	966
akna	905	altábornagy	482
alakulás (alakzat)	118	általános	488
albán (albánul)	675	altiszt	965
Albánia	410	április	997
alezredes	532	átirat	761
alispán	730	attaché	694
állomány	735	augusztus	977
állományfelemelés	738	Ausztria	131
állomás	538	azonnal	992

B.

bán	983	bizalmas	940
barak	507	bizalmi egyén	744
bebizonyitás	892	biztos	835
behivás	714	biztositás	964
behivójegy	739	bosnyák (bosnyákul)	998
beszállásolás	920	Bosznia	370
bíróság	818		

C.

carabiniere	743	csendörség	231, 936
cirkáló	794	csónak	834

Kazalo tajnopisnih oznaka.

A.

admiral	916	atentat	437
Albanija	410	attaché	694
albanski (a—o)	675	Austrija	131
asentovanje konja	843	automobil	662

B.

ban	983	bosanski (a—o)	998
baraka	507	Bosna	370
barikada	710	brahijum (pomočnica)	313
bataljun	139	brigada	285
bilježnik	817	brod	816
bitka	796	brodovlje	333, 719
bitnica	145	broj	893
bjegunac	562	brzojav	518
bojni brod	787	brzojavka	765
boležljivnica	867		

C.

carski lovac	169	c. i. kr. (ces. i kralj.)	613, 653, 762, 804, 854, 904
cesarsko kraljevski ministar za zemaljsku obranu	381	Crnagora	982
c. kr. (ces. kralj.)	564, 633, 667, 768, 815, 862	crnogorski	753

Č.

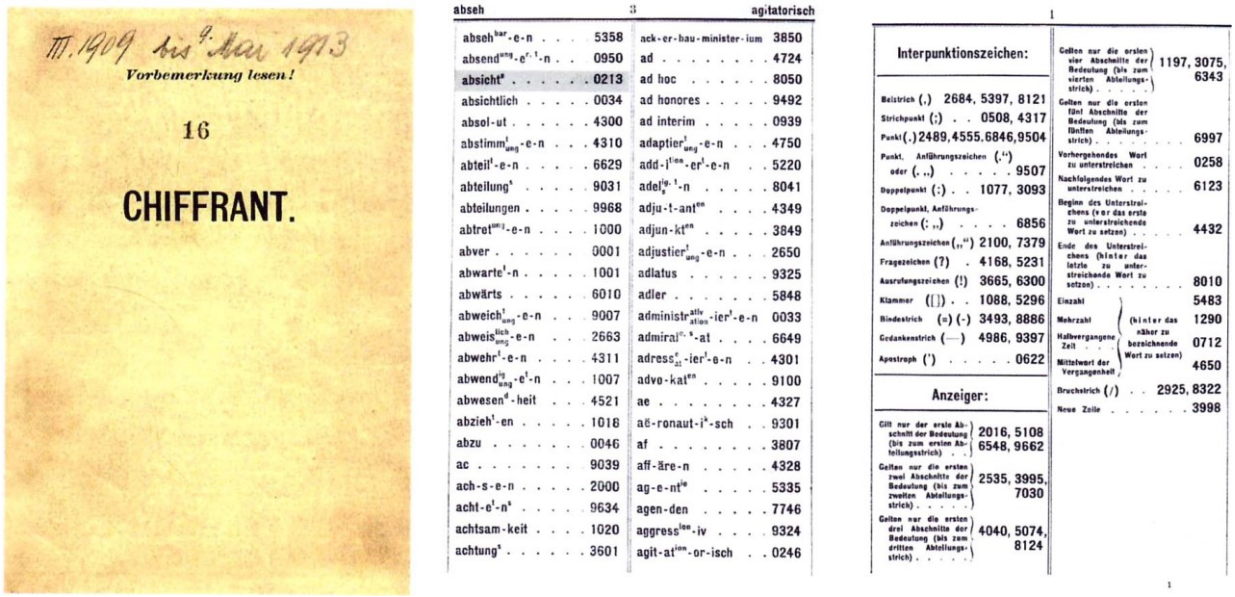
čamac	834	četna divizija	903
čardak	729	četno tielo	959

Abbildung 23: Auszug aus den dreisprachigen Chiffren–Tabellen, deutsch, ungarisch und kroatisch.

Nach einer Begutachtung des dreistelligen Friedenschiffren–Schlüssels durch den Generalstab am 1. April 1913 hatte sich dieser nicht bewährt, da er selbst im Friedensverkehr für schwerfällig gehalten wurde. Es wurde daher beantragt, den Chiffren–Schlüssel gründlich zu überarbeiten und vor allem die Anzahl der Sigel zu vermehren. Die Abteilung 5./T.B. bestätigte in einer Stellungnahme vom 7. April 1913, dass anlässlich der Balkankrise im November 1912 das wenig umfangreiche „Vocabulaire“ (999 Chiffren) nicht entsprochen habe. Es müsse daher ein vollwertiger vierstelliger Chiffren–Schlüssel hergestellt werden. Gleichzeitig wurde auf den in Kraft stehenden vierstelligen Friedenschiffren–Schlüssel aufmerksam gemacht, mit dem es zu Missverständnissen kommen könnte. Dazu erklärte am 13. August 1914 das Evidenzbüro des k.u.k. Generalstabes, dass die Absicht besteht, für die eigenen Bedürfnisse *einen* Chiffren–Schlüssel in deutscher, wenn aber durchführbar, auch für die anderen Sprachen der Monarchie zu schaffen. Das System dieser Chiffren sollte so gewählt werden, dass ein paar Chiffren–Bücher mit geringer Mühe zu einem, für jeden anderen unverständlichen Chiffren umgestaltet werden könnte.[253]

[252] *Prikowitsch,* Drahtlose Telegraphie, Bd. 2, 396f.
[253] *Prikowitsch,* Drahtlose Telegraphie, Bd. 2, 398.

Der in der Stellungnahme der Abteilung 5./T.B. vom 7. April 1914 erwähnte vierstellige Friedens-Schlüssel hatte mit 9.999 Begriffen ein wesentlich größeres Vokabular zur Verfügung als der dreistellige Friedensschlüssel mit nur 999 Begriffen. Da der dreistellige Chiffren–Schlüssel nicht entsprach und sicher auch schon längst kompromittiert worden sein dürfte, wurde dieser eingezogen. Der Friedensschlüssel Nr. 16 war vom März 1909 bis Mai 1913 in Verwendung; sein Vorgänger von 1906 bis März 1909.


III. 1909 bis 9. Mai 1913
Vorbemerkung lesen!
16
CHIFFRANT.

abseh 3 agitatorisch

absehbar-e-n	5358	ack-er-bau-minister-ium	3850
absendung-e-r-n	0950	ad	4724
absicht	0213	ad hoc	8050
absichtlich	0034	ad honores	9492
absol-ut	4300	ad interim	0939
abstimmung-e-n	4310	adaptierung-e-n	4750
abteil-e-n	6629	add-ier-er-e-n	5220
abteilung	9031	adelig-n	8041
abteilungen	9968	adju-t-ant	4349
abtretung-e-n	1000	adjun-kt	3849
abver	0001	adjustierung-e-n	2650
abwarte-n	1001	adlatus	9325
abwärts	6010	adler	5848
abweichung-e-n	9007	administrativ-ier-e-n	0033
abweisung-e-n	2663	admiral-at	6649
abwehr-e-n	4311	adress-ier-e-n	4301
abwendung-e-n	1007	advo-kat	9100
abwesen-heit	4521	ae	4327
abzieh-en	1018	aë-ronaut-isch	9301
abzu	0046	af	3807
ac	9039	aff-äre-n	4328
ach-s-e-n	2000	ag-e-nt	5335
acht-e-n	9634	agen-den	7746
achtsam-keit	1020	aggression-iv	9324
achtung	3601	agit-ation-or-isch	0246

1

Interpunktionszeichen:

Beistrich (,)	2684, 5397, 8121
Strichpunkt (;)	0508, 4317
Punkt (.)	2489, 4555, 6846, 9504
Punkt, Anführungszeichen (.“) oder (. „)	9507
Doppelpunkt (:)	1077, 3093
Doppelpunkt, Anführungszeichen (: „)	6856
Anführungszeichen („“)	2100, 7379
Fragezeichen (?)	4168, 5231
Ausrufungszeichen (!)	3665, 6300
Klammer ([])	1088, 5296
Bindestrich (=) (-)	3493, 8886
Gedankenstrich (—)	4986, 9397
Apostroph (’)	0622

Anzeiger:

Gilt nur der erste Abschnitt der Bedeutung (bis zum ersten Abteilungsstrich)	2016, 5108 6548, 9662
Gelten nur die ersten zwei Abschnitte der Bedeutung (bis zum zweiten Abteilungsstrich)	2535, 3995, 7030
Gelten nur die ersten drei Abschnitte der Bedeutung (bis zum dritten Abteilungsstrich)	4040, 5074, 8124
Gelten nur die ersten vier Abschnitte der Bedeutung (bis zum vierten Abteilungsstrich)	1197, 3075, 6343
Gelten nur die ersten fünf Abschnitte der Bedeutung (bis zum fünften Abteilungsstrich)	6997
Vorhergehendes Wort zu unterstreichen	0258
Nachfolgendes Wort zu unterstreichen	6123
Beginn des Unterstreichens (vor das erste zu unterstreichende Wort zu setzen)	4432
Ende des Unterstreichens (hinter das letzte zu unterstreichende Wort zu setzen)	8010
Einzahl	5483
Mehrzahl (hinter das näher zu bezeichnende Wort zu setzen)	1290
Halbvergangene Zeit (hinter das näher zu bezeichnende Wort zu setzen)	0712
Mittelwort der Vergangenheit (hinter das näher zu bezeichnende Wort zu setzen)	4650
Bruchstrich (/)	2925, 8322
Neue Zeile	3998

1

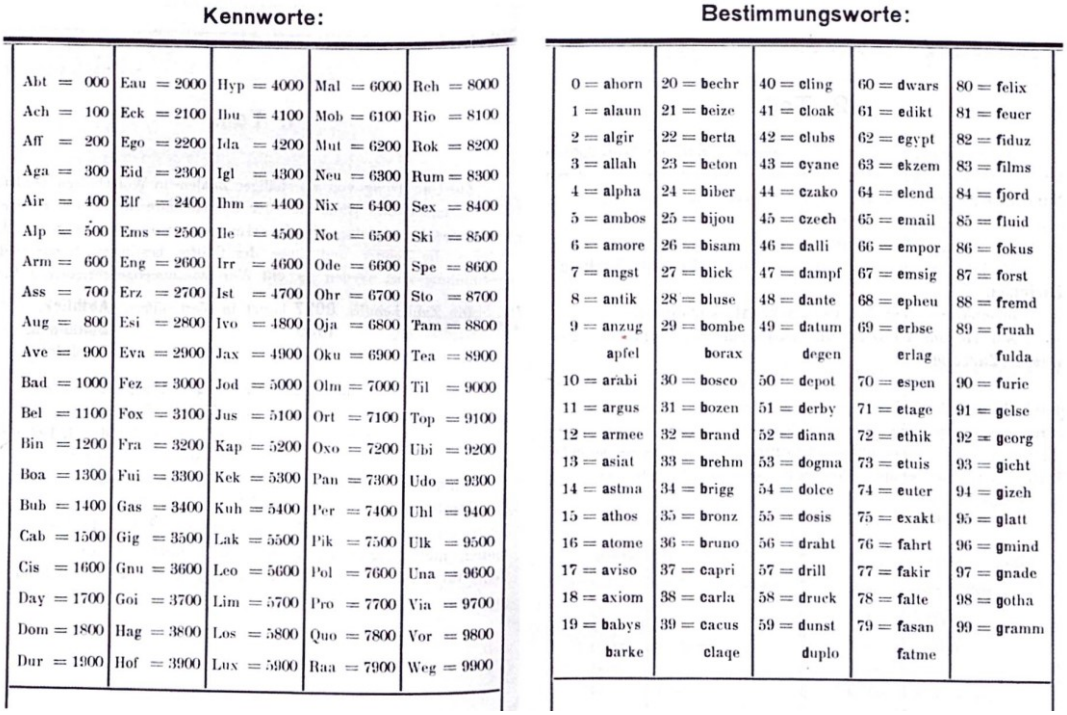
Abbildung 24: Auszug aus dem vierstelligen Friedensschlüssel Nr. 16 für den Chiffrant.

Abgelöst wurde der Friedensschlüssel 16 durch die Chiffre B, die vom August 1913 bis 25. August 1915 Verwendung fand. Während das Vokabular weitgehend unverändert blieb, wurden die Zahlen–Chiffren für die einzelnen Begriffe geändert. Ergänzt wurde der Chiffrant mit einigen Seiten für die Interpunktion, für Zahlen und geographische Begriffe. Die geographischen Begriffe, Ortsnamen und Geländebezeichnungen waren je nach Verteiler unterschiedlich.[254]

Seit dem größeren Manöver 1913 wurde empfohlen, Radiotelegramme wichtigen Inhalts grundsätzlich zu chiffrieren, weil Radiotelegramme von unberufenen Stationen mitgelesen werden konnten. Für die drahtlose Übertragung wurde zusätzlich ein Wort–Chiffrenkodex zur Umsetzung (Transponierung) von vierstelligen Zahlen in Worte ausgegeben. In Wort–Chiffren wurden die Tausender und Hunderter durch ein Kennwort ersetzt, an das ein Bestimmungswort angehängt wurde. Das Kennwort und das Bestimmungswort wurden zu einem Wort zusammengefasst. Das Umsetzen hatte bei den Radiostationen zu erfolgen. Der

[254] *Prikowitsch,* Drahtlose Telegraphie, Bd. 2, 399.

Wort–Chiffrenkodex bildete eine Ergänzung zum vierstelligen Zahlen–Chiffren–Schlüssel. Durch seine Anwendung wurde die Verstümmelung von Zahlen–Chiffren bei der radiotelegraphischen Übermittlung vermieden.[255]



Kennworte:

Abt = 000	Eau = 2000	Hyp = 4000	Mal = 6000	Reh = 8000
Ach = 100	Eck = 2100	Ibu = 4100	Mob = 6100	Rio = 8100
Aff = 200	Ego = 2200	Ida = 4200	Mut = 6200	Rok = 8200
Aga = 300	Eid = 2300	Igl = 4300	Neu = 6300	Rum = 8300
Air = 400	Elf = 2400	Ihm = 4400	Nix = 6400	Sex = 8400
Alp = 500	Ems = 2500	Ile = 4500	Not = 6500	Ski = 8500
Arm = 600	Eng = 2600	Irr = 4600	Ode = 6600	Spe = 8600
Ass = 700	Erz = 2700	Ist = 4700	Ohr = 6700	Sto = 8700
Aug = 800	Esi = 2800	Ivo = 4800	Oja = 6800	Tam = 8800
Ave = 900	Eva = 2900	Jax = 4900	Oku = 6900	Tea = 8900
Bad = 1000	Fez = 3000	Jod = 5000	Olm = 7000	Til = 9000
Bel = 1100	Fox = 3100	Jus = 5100	Ort = 7100	Top = 9100
Bin = 1200	Fra = 3200	Kap = 5200	Oxo = 7200	Ubi = 9200
Boa = 1300	Fui = 3300	Kek = 5300	Pan = 7300	Udo = 9300
Bub = 1400	Gas = 3400	Kuh = 5400	Per = 7400	Uhl = 9400
Cab = 1500	Gig = 3500	Lak = 5500	Pik = 7500	Ulk = 9500
Cis = 1600	Gnu = 3600	Leo = 5600	Pol = 7600	Una = 9600
Day = 1700	Goi = 3700	Lim = 5700	Pro = 7700	Via = 9700
Dom = 1800	Hag = 3800	Los = 5800	Quo = 7800	Vor = 9800
Dur = 1900	Hof = 3900	Lux = 5900	Raa = 7900	Weg = 9900

Bestimmungsworte:

0 = ahorn	20 = bechr	40 = cling	60 = dwars	80 = felix
1 = alaun	21 = beize	41 = cloak	61 = edikt	81 = feuer
2 = algir	22 = berta	42 = clubs	62 = egypt	82 = fiduz
3 = allah	23 = beton	43 = cyane	63 = ekzem	83 = films
4 = alpha	24 = biber	44 = czako	64 = elend	84 = fjord
5 = ambos	25 = bijou	45 = czech	65 = email	85 = fluid
6 = amore	26 = bisam	46 = dalli	66 = empor	86 = fokus
7 = angst	27 = blick	47 = dampf	67 = emsig	87 = forst
8 = antik	28 = bluse	48 = dante	68 = epheu	88 = fremd
9 = anzug	29 = bombe	49 = datum	69 = erbse	89 = fruah
apfel	borax	degen	erlag	fulda
10 = arabi	30 = bosco	50 = depot	70 = espen	90 = furie
11 = argus	31 = bozen	51 = derby	71 = etage	91 = gelse
12 = armee	32 = brand	52 = diana	72 = ethik	92 = georg
13 = asiat	33 = brehm	53 = dogma	73 = etuis	93 = gicht
14 = astma	34 = brigg	54 = dolce	74 = euter	94 = gizeh
15 = athos	35 = bronz	55 = dosis	75 = exakt	95 = glatt
16 = atome	36 = bruno	56 = draht	76 = fahrt	96 = gmind
17 = aviso	37 = capri	57 = drill	77 = fakir	97 = gnade
18 = axiom	38 = carla	58 = druck	78 = falte	98 = gotha
19 = babys	39 = cacus	59 = dunst	79 = fasan	99 = gramm
barke	claqe	duplo	fatme	

Abbildung 25: Ausschnitt aus dem 1. Teil des Wort–Chiffrenkodex mit Kenn- und Bestimmungsworte.

Durch die Umsetzung von vierstelligen Zahlen–Chiffren in Wort–Chiffren wurde aus der Zahl ein Wort gemäß folgenden Beispielen gebildet:

Der Zahlenchiffre 0027 lautet in Wort–Chiffren: Abtblick
″ ″ 1300 ″ ″ ″ Boaahorn
″ ″ 8754 ″ ″ ″ Stodolce

Eine Umsetzung von Wort–Chiffren eines eingelangten Telegrammes zurück in Zahlen–Chiffren erfolgte in einem umgekehrten Vorgang.[256] Diese Methode ist einer zweifachen Chiffrierung ähnlich, die in der folgenden Transponiermethode mit vierstelligen Zahlen beschrieben wird.

6.3.2 Die Transponiermethode

Wie bereits erwähnt, wurde mit der Einführung der Friedenschiffre „B“ im August 1913 der Friedensschlüssel 16 abgelöst. Zur Erhöhung der Sicherheit gegen Abhörung und Entschlüsselung der militärischen Korrespondenz durch den Gegner wurde für übergeordnete militärische Zwecke der Friedensschlüssel „B“ nach Kriegsausbruch durch Transponierung

[255] *Prikowitsch,* Drahtlose Telegraphie, Bd. 2, 400.
[256] *Prikowitsch,* Drahtlose Telegraphie, Bd. 2, 402.

täglich verändert, wobei durch die Transponierung eine bereits chiffrierte Depesche ein zweites Mal chiffriert wurde.[257] Die Anwendung der Transponiermethode wird in der folgenden Anleitung des k. u. k. Kriegsministeriums mit einem Beispiel erklärt:

„K. u. k. Kriegsministerium
Präs. Nr. 8588 von 1914

Transponiermethode
Zum Friedenschiffre „B".

Die Methode besteht aus einer Chiffriertabelle und einer Dechiffriertabelle.
Die Chiffriertabelle zeigt sieben den Wochentagen entsprechend bezeichnete Horizontalspalten à 2 Zeilen. Die obere Zeile jedes solchen Paares zeigt in arithmetischer Reihenfolge die Elemente, aus welchen die Chiffren zusammengesetzt sind. Die untere Zeile zeigt jene Ziffern, in welchen die Chiffreelemente am betreffenden Wochentage zu verwandeln sind.

Die Dechiffriertabelle zeigt, ebenfalls sieben Horizontalspalten à 2 Zeilen. Jedoch enthält die obere Zeile jeden Paares die Elemente der einlangenden – verwandelten – Chiffren in arithmetischer Reihenfolge und darunter jene Ziffern, in welche diese Elemente verwandelt werden müssen, um wieder die ursprünglichen Zifferngruppen zu erhalten.

Chiffrieren.

Die Depesche wird normal chiffriert. Dann wird in der Chiffriertabelle der Wochentag aufgesucht, an welchem chiffriert wird. Die aus dem Chiffranten entnommenen Zahlengruppen werden dann ziffernweise in der oberen Zeile aufgesucht und durch die unmittelbar daruntersteheden Ziffern ersetzt.

Beispiel:
Donnerstag.

Zu chiffrieren wäre: „Feindliche Kavalleriedivision im Anmarsch gegen …."

Normale Chiffren:	1843	5380	0443	7654	4514	8962
Transponiert in:	3681	7164	4881	2578	8738	6059

Letztere Gruppen sind abzutelegraphieren.

Dechiffrieren.

Die Zahlengruppen der eingelangten Depesche sind mit Hilfe der Dechiffriertabelle in die ursprünglichen Chiffren zu verwandeln, indem beim Wochentage, an welchem die Depesche chiffriert wurde, die einzelnen Ziffern der eingelangten Zahlen in der oberen Zeile aufgesucht und durch die unmittelbar darunter stehenden ersetzt werden. Sodann wird die Depesche in normaler Weise dechiffriert.

Beispiel:
Donnerstag.

Eingelangte Chiffren:	3681	7164	4881	2578	8738	6059
Rücktransponiert in:	1843	5380	0443	7654	4514	8962

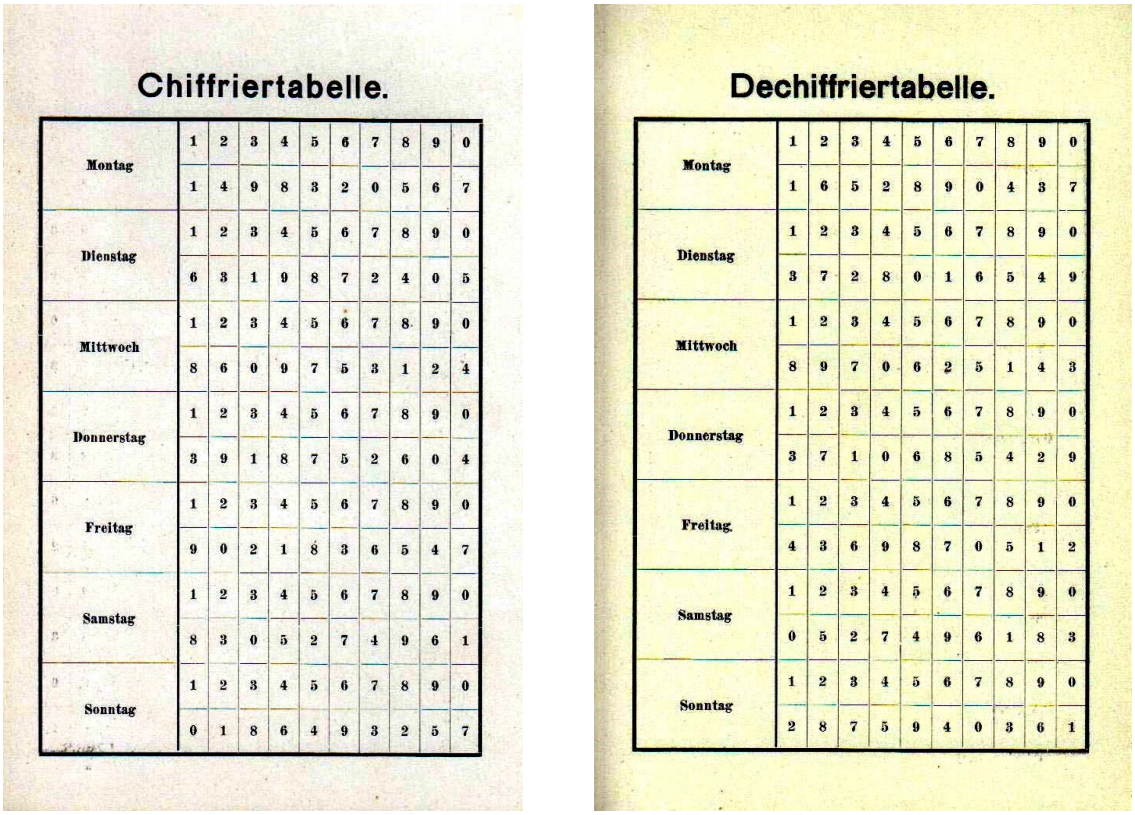
Klartext der Depesche: „Feindliche Kavalleriedivision im Anmarsch gegen …."
Neuerung.

[257] *Hubatschke*, Ferdinand Prantner, Buch 6, Diss., 1450.

Um bei längeren Depeschen und bei solchen, in welchen sich die gleichen Ausdrücke öfter wiederholen, dann bei häufigen Chiffreverkehr zweier Stellen an demselben Tage über denselben Gegenstand die Möglichkeit zu besitzen, die Transponierung auch innerhalb desselben Tages und innerhalb derselben Depesche wechseln zu können, werden Anzeiger für den Chiffrewechsel eingeführt. […]“[258]

DRUCKEREI D. K. U. K. KM. 178515

Diese Transponiermethode zum Friedensschlüssel „B“ und die Neuauflage des Verzeichnisses II (Verteiler) gelangte gemäß Erlass des K. u. k. Kriegsministeriums Präs. Nr. 8588, Wien, 13. Dezember 1914 durch Kuriere zur Ausgabe.



Chiffriertabelle.

Montag	1	2	3	4	5	6	7	8	9	0
	1	4	9	8	3	2	0	5	6	7
Dienstag	1	2	3	4	5	6	7	8	9	0
	6	3	1	9	8	7	2	4	0	5
Mittwoch	1	2	3	4	5	6	7	8	9	0
	8	6	0	9	7	5	3	1	2	4
Donnerstag	1	2	3	4	5	6	7	8	9	0
	3	9	1	8	7	5	2	6	0	4
Freitag	1	2	3	4	5	6	7	8	9	0
	9	0	2	1	8	3	6	5	4	7
Samstag	1	2	3	4	5	6	7	8	9	0
	8	3	0	5	2	7	4	9	6	1
Sonntag	1	2	3	4	5	6	7	8	9	0
	0	1	8	6	4	9	3	2	5	7

Dechiffriertabelle.

Montag	1	2	3	4	5	6	7	8	9	0
	1	6	5	2	8	9	0	4	3	7
Dienstag	1	2	3	4	5	6	7	8	9	0
	3	7	2	8	0	1	6	5	4	9
Mittwoch	1	2	3	4	5	6	7	8	9	0
	8	9	7	0	6	2	5	1	4	3
Donnerstag	1	2	3	4	5	6	7	8	9	0
	3	7	1	0	6	8	5	4	2	9
Freitag	1	2	3	4	5	6	7	8	9	0
	4	3	6	9	8	7	0	5	1	2
Samstag	1	2	3	4	5	6	7	8	9	0
	0	5	2	7	4	9	6	1	8	3
Sonntag	1	2	3	4	5	6	7	8	9	0
	2	8	7	5	9	4	0	3	6	1

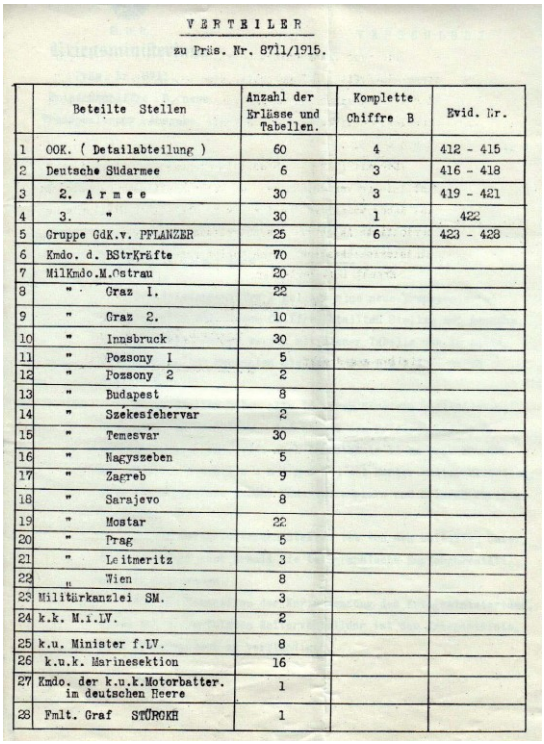
Abbildung 26: Chiffriertabelle und Dechiffriertabelle Nr. 8588 von 1914, in Postkartengröße

Die Chiffriertabelle bzw. Dechiffriertabelle 8588 traten um Mitternacht vom 23. auf 24. Dezember 1914 in Kraft und wurden bis 25. August 1915 verwendet. Gleichzeitig mit der Inkraftsetzung wurde angeordnet, das bisherige Verzeichnis II sofort nach Erhalt des neuen Verzeichnisses II kommissionell zu verbrennen. Die Übernahme der Sendung war dem Kurier auf den Kursbögen zu bestätigen und dem Kriegsministerium sogleich telegraphisch (telephonisch), nicht chiffriert, zu melden.[259]

[258] OeStA/KA NFA HHK AK 4.Armee AK 70, Chiffrentabelle 8588.
[259] OeStA/KA NFA HHK AK 4.Armee AK 70, Brief KM Präs. Nr. 8588, vom 13. Dezember 1914.

Mit Erlass des k. u. k. Kriegsministeriums, Präs. Nr. 8711 vom 9. Mai 1915 gelangten neue Transponiertabellen in ausreichender Menge direkt durch Kuriere an die Kommandostellen zur Verteilung. Die im „Verteiler“ genannten Stellen hatten alle in ihrem Bereich befindlichen, untergeordneten Stellen mit dem Friedenschiffre „B“ schleunigst ebenfalls mit Kurier zu beliefern.

> „Von dem Eintreffen der Kuriersendung des Kriegsministeriums, sowie von der erfolgten Weiterverteilung ist das Kriegsministerium telegraphisch zu verständigen. Die neue Transponierung tritt am 13. Mai 1915, 6 Uhr vorm. in Kraft; 2 Tage später sind die alten T a b e l l e n kommissionell zu verbrennen; alle anderen Behelfe zu diesem Chiffre bleiben in Kraft – so auch die M e t h o d e.“[260]



V E R T E I L E R

zu Präs. Nr. 8711/1915.

	Beteilte Stellen	Anzahl der Erlässe und Tabellen.	Komplette Chiffre B	Evid. Nr.
1	OOK. (Detailabteilung)	60	4	412 - 415
2	Deutsche Südarmee	6	3	416 - 418
3	2. A r m e e	30	3	419 - 421
4	3. "	30	1	422
5	Gruppe GdK.v. PFLANZER	25	6	423 - 428
6	Kmdo. d. BStrKräfte	70		
7	MilKmdo.M.Ostrau	20		
8	" Graz I.	22		
9	" Graz 2.	10		
10	" Innsbruck	30		
11	" Pozsony I	5		
12	" Pozsony 2	2		
13	" Budapest	8		
14	" Szekesfehervar	2		
15	" Temesvar	30		
16	" Nagyszeben	5		
17	" Zagreb	9		
18	" Sarajevo	8		
19	" Mostar	22		
20	" Prag	5		
21	" Leitmeritz	3		
22	" Wien	8		
23	Militärkanzlei SM.	3		
24	k.k. M.i.LV.	2		
25	k.u. Minister f.LV.	8		
26	k.u.k. Marinesektion	16		
27	Kmdo. der k.u.k.Motorbatter. im deutschen Heere	1		
28	Fmlt. Graf STÜRGKH	1		

Der mit k. u. k. Kriegsministerium Erlass Präs. Nr. 8588/1914 im Dezember 1914 ausgegebene Verteiler mit Nennung aller Stellen, war infolge von Verschiebungen zum Teil nicht mehr richtig. Vom k. u. k. Kriegsministerium wurde daher eine berichtigte Abschrift der Liste durch Kurierzustellung verlangt. Mit den neuen Chiffriertabellen und Dechiffriertabellen mussten vor der Anwendung mehr als 440 Stellen per Kurier versorgt werden.

Abbildung 27: Verteiler zu Chiffriertabellen zum Erlass, KM Präs. Nr. 8711/1915

Die Friedensschlüssel wurden nach Kriegsausbruch durch Transponierung verändert und nach und nach durch Kriegsschlüssel ersetzt. „An Stelle des bisherigen Friedenschiffre „B“ gelangt der neue Chiffre „F“ nach zuliegendem Verteiler zur Ausgabe. Er besteht aus je einem Chiffrant, einem Dechiffrant, einem Verteiler. Inkrafttreten des neuen Chiffres: 25. August 1915. Der alte Friedenschiffre „B“ tritt zum gleichen Zeitpunkte außer Kraft; er wolle samt allen Nebenbehelfen (Transponiermethode, -Tabelle, Direktiven, Verteiler, etc.) 6 Tage später kommissionell verbrannt werden.“[261]

[260] OeStA/KA NFA HHK AK 4.Armee AK 70, Brief KM Präs. Nr. 8711, vom 9. Mai 1915.
[261] OeStA/KA NFA HHK AK 4.Armee AK 70, Brief k.u.k. Kriegsministerium, Präs. Nr. 14.420, vom 9. August 1915.

Nach der Kriegserklärung an Serbien am 28. Juli 1914 wurde am 7. September 1914 beim Präsidialbüro des k. u. k. Kriegsministerium eine Chiffregruppe eingerichtet (Präs. Nr. 12.319 vom 7. September 1914). Die Gruppe unterstand dem Vorstand des Präsidialbureaus im Kriegsministerium. Leiter der Gruppe war Hauptmann Figl, sein Stellvertreter Hauptmann Ivanyszyn. Vor Chiffrierung jeder Depesche musste nach einem Verzeichnis überprüft werden, ob die Gegenstelle den Chiffren hat, mit dem man chiffrieren wollte.[262] Die bunte Vielfalt der Chiffren–Schlüssel, die zur besseren Unterscheidung meist mit färbigen Umschlägen hergestellt wurden, waren hauptsächlich vierstellige Zahlen–Chiffren. Fünfstellige Zahlen–Chiffren wurden erst ab 1. April 1916 mit dem Schlüssel „Atta" verwendet.[263] Weitere Untersuchungen zu Militär–Chiffren im Ersten Weltkrieg überschreiten den Untersuchungszeitraum dieser Arbeit.

Die Beschreibungen der Vorgänge zur Übertragung militärischer Depeschen soll abschließend noch auf Ereignisse besonderer Art eingehen. Auch bei bester Organisation, größter Vorsicht und sorgsamer Vorgangsweise kam es im Militärdienst doch auch zu Pannen, die folgende Verfügung des k. u. k. Kriegsministeriums, Präs. Nr. 5951/I ausgelöst hatte:

> „Wien, am 15. April 1915.
>
> Trotz des Verbotes des teilweisen Chiffrements häufen sich in letzter Zeit diese Fälle derart, daß sich das Kriegsministerium veranlaßt sieht, neuerlich das teilweise Chiffrieren von Depeschen auf das Strengste zu untersagen.
>
> Alle Bemühungen um die Geheimhaltung wichtiger Angelegenheiten sind illusorisch, wenn das Verständigungsmittel – der Chiffre – auf solch' leichtfertige Art kompromittiert wird, wie dies nun schon in mehreren Fällen mit dem eben erst zur Ausgabe gelangten neuen Kriegschiffre seitens einzelner Stellen der Fall war. Es wurde hiebei in der Bequemlichkeit so weit gegangen, daß in wortreichen Texten bloß einzelne eingestreute Chiffreworte gegeben wurden, so daß es jedem, der sich solche Telegrammabschriften zu beschaffen weiß, (z. B. durch Amtsdiener in den Telegraphenämtern), auf die denkbar leichteste Art in die Hand gegeben ist, sich einen Dechiffranten zu bilden.
>
> Die in ganz kurzer Zeit dem Kriegsministerium zur Kenntnis gelangten Fälle von solchen teilweisen Chiffrements lassen darauf schließen, daß dieser Vorgang größere Dimensionen angenommen hat.
>
> Das Kriegsministerium verfügt daher, daß in Hinkunft jeder Fall eines teilweisen Chiffrements von der empfangenden Stelle dem Kriegsministerium unter Beischluß der Originaldepesche zur Kenntnis zu bringen ist. […].
>
> Ergeht an alle Militärkommandos, die FTLtg. Nr. 5 in MISKOLCZ, FTLtg. Nr. 6 in DEBRECZEN, dann zur Kenntnis an das Kommando der Balkanstreitkräfte, MilKanzlei Seiner Majestät, k. k. Ministerium für Landes-verteidigung, k. u. Landes-verteidigungsminister, Gruppe R o h r, KM.-Marine-sektion, Eisenbahnlinienkommando KOLOZSVÁR und das Armeeober-kommando. Zwecks Weiterleitung liegt die entsprechende Anzahl Erlaß-abschriften bei."[264]

[262] *Prikowitsch,* Drahtlose Telegraphie, Bd. 2, 405.
[263] *Prikowitsch,* Drahtlose Telegraphie, Bd. 2, 406f.
[264] OeStA/KA NFA HHK AK 4.Armee AK 70, Brief KM Präs. Nr. 5951/I., vom 15. April 1915.

Diese Beschreibung peinlicher Ereignisse, die eine leichte Entschlüsselung von Nachrichten durch „Spione“ ermöglichten, zeigt deren Gefahr, wie schnell Gedankenlosigkeit dem Feind eine Chance geben konnte, den eigenen Erfolg zu verhindern.

Mit dieser Bemerkung lässt sich auf die eingangs erwähnte Anekdote aus „Die Abenteuer des braven Soldat Schwejk“ eine Verbindung herstellen, in der die Vertauschung des „Verschlüsselungs–Buches“ eine Entschlüsselung eines Befehles im Ernstfall unmöglich machte. Auch die Praxis zeigte, wie schnell ein unbedachter Fehler in der Kette der Übertragung einer geheimen Depesche zu einem Unglück führen konnte. Die teilweise Chiffrierung, gegen die sich das Kriegsministerium im April 1915 zu einer Verfügung veranlasst sah, fand fast zeitgleich mit der Panne des braven Soldaten Schwejks statt.

7 Zusammenfassung

Bis ins sechzehnte Jahrhundert haben die verdeckten Nachrichten und Methoden der monoalphabetischen Verschlüsselung mit Erweiterungen durch Codes und Homophone zur Übermittlung geheimer Nachrichten genügt. Ein entscheidender Wendepunkt in der evolutionären Entwicklung der Verschlüsselung bildete aber die Kryptographie, die sich ab dem Beginn des siebzehnten Jahrhunderts mit Chiffren für Buchstaben, Silben und Worten sowie der polyalphabetischen Verschlüsselung durchsetzte. Mit den Codes und Chiffren begann auch der Kampf zwischen den Verschlüsslern und Entschlüsslern, den Kryptographen und Kryptoanalysten, der Jahrhunderte lang, bis in die heutige Zeit andauern sollte. Die Kryptoanalyse wurde im Zusammenhang mit der Briefspionage zu einem wichtigen Instrumentarium, auf das die Herrscher nicht verzichten wollten oder konnten. Alle Staaten begannen ihre „Schwarzen Kammern" einzurichten, um die Absichten anderer Staaten möglichst früh zu erfahren. Die Wiederbelebung der Künste, Wissenschaften und des Gelehrtentums in der Renaissance war auch für die Kryptographie fruchtbar, während die wuchernden politischen Intrigen auch gute Gründe für die Geheimhaltung des Nachrichtenverkehrs lieferten. Die Staaten schickten ihre Botschafter an fremde Höfe und es entstand ein reges diplomatisches Leben. Die Gesandten erhielten Botschaften von ihren Monarchen, in denen Einzelheiten der Außenpolitik, die sie durchsetzen sollten, festgehalten waren. So herrschte genug Anlass, den Nachrichtenverkehr in beiden Richtungen zu verschlüsseln.[265]

Chiffren waren den ständigen Angriffen der Entschlüssler ausgesetzt und entwickelten sich zu neuen, stärkeren Chiffren, die so lange in Verwendung waren, bis die Entschlüssler die Schwachstellen ausfindig gemacht hatten. Dieser oftmalige Wechsel der Chiffriertabellen ist in den überlieferten Tabellen mit zweistelligen Buchstaben– oder Zahlen–Chiffren hin zu dreistelligen und vierstelligen Zahlen, mit und ohne Interpunktion, aus den Regierungszeiten von Maria Theresia bis Franz I. erkennbar. Es soll an dieser Stelle aber festgehalten werden, dass es sich bei den beschriebenen Entwicklungen haupsächlich um die Verschlüsselung der Nachrichten für gehobene Dienste, für die höchsten Stellen der Diplomatie mit größter Geheimhaltung handelte. Im Prinzip gibt es unendlich viele kryptographische Methoden, die je nach Verwendungszweck, angefangen von Liebesbriefen, deren Inhalte von den Eltern nicht entdeckt werden sollte, über die interne Korrespondenz adeliger Familien, für Spione,

[265] *Singh*, Geheime Botschaften, 44.

Presse, Agenten und für Geschäftsleute bis zur hohen Diplomatie und für militärische Zwecke eingesetzt werden konnten.

Es war der Erfahrung und Intelligenz der Spezialisten in den „Schwarzen Kammern“ im Allgemeinen, den Beamten in der Wiener Ziffernkanzlei bzw. in der Ziffernsektion im Besonderen vorbehalten, in ihrem Streben nach absoluter Geheimhaltung nicht nur geeignete Chiffrierverfahren zu entwickeln, sondern auch fremde Chiffren–Depeschen zu entschlüsseln, womit sie ihren Beitrag zum evolutionären Kampf zwischen Verschlüssler und Entschlüssler geleistet haben.

Mit der Einführung der telegraphischen Übertragung Mitte des 19. Jahrhunderts kann von einem zweiten Wendepunkt in der Entwicklung der Verschlüsselungsmethode gesprochen werden, die sich aus zwei Vorgängen zusammensetzt. Erstens bestand das Chiffrier– und Dechiffrierbuch nach einer ersten Beschreibung aus dem Jahr 1850 aus zwei Teilen; einem grammatikalischen und einen lexikalischen Teil. Zur Reduzierung der Chiffren–Felder wurden im lexikalischen Teil zu den angeführten Zeitwörtern keine weiteren Felder bzw. Chiffrierzahlen für deren Zeitformen, Personen– und Zahlenbiegungen verwendet. Die Einfügung von Feldern mit grammatikalischem Inhalt ermöglichte eine präzise Chiffrierung und führte darüber hinaus Entzifferer in die Irre, da diese Felder keinen gesuchten Text beinhalteten. Zweitens hat der erfolgreiche Kryptoanalytiker Ferdinand Prantner am Ende seiner Karriere 1869 mit seiner Erfahrung die Methode der „Transkription“, einer zweiten „Verwürfelung“ der Chiffrierung, die sich täglich und nach jeder Depesche änderte, einen entscheidenden Beitrag zur Verhinderung einer Entschlüsselung geleistet. Es kann ohne Übertreibung festgehalten werden, dass diese zweifache Verschlüsselung durch Substituierung der Chiffren aus dem Diktionär zu dieser Zeit zu einer äußerst hohen Sicherheit gegen eine fremde Entschlüsselung führte. Ein weiterer Vorteil der Doppel–Chiffrierung war die Beibehaltung des unveränderten Chiffren–Diktionärs. Diese „Transponiermethode“ wurde später vom Militär übernommen und am Beginn des Ersten Weltkrieges und während des Krieges angewendet.

Zu den erfolgreichen österreichischen Kryptoanalytikern aus dem militärischen Bereich zählen Maximilian Ronge, Andreas Figl und Hermann Pokorny.[266] Viele andere aus der Ziffernsektion traten nie ans Licht der Öffentlichkeit und sind bis auf wenige Ausnahmen, wie

[266] *Prikowitsch,* Drahtlose Telegraphie, Bd. 2, 343.

Ferdinand Prantner, Johann Urrisk, Anton v. Schweiger und Aloys v. Cobelli, vergessen. Die Arbeit eines professionellen Entzifferers ist undankbar; es ist ihm nicht erlaubt, seine Erfolge öffentlich oder auch nur im Kreise seiner Familie zu feiern, ja nicht einmal ihre engsten Angehörigen durften wissen, was sie taten. Die damit verbundenen Beschränkungen bestanden üblicher Weise auch nach Beendigung ihres aktiven Dienstes.[267]

Der Verschlüsselung von Nachrichten bedienten sich Institutionen, die sich in vier Bereiche zusammenfassen lassen, von denen jeder ein in sich geschlossenes System bildete und nur eingeschränkte Berührungspunkte zum anderen System unterhielt. Als diese in sich geschlossenen vier Bereiche können in der zweiten Hälfte des 19. Jahrhunderts das Ministerium des Äußern und seine diplomatischen Dienste im Ausland, die geheime Ziffernsektion mit ihren Postlogen zur Briefüberwachung, das Innenministerium mit seinem Agentennetzwerk und letztlich das Militär und die Marine genannt werden. Sie unterhielten ihre eigenen Abteilungen zur Verschlüsselung ihrer Korrespondenz.

Trotz intelligenter und komplizierter werdender Methoden der Kryptologie, die besonders in der zweiten Hälfte des 19. Jahrhunderts im Kontext mit der Telegraphie entwickelt wurden, lehrt die Geschichte der Kryptologie, dass der Entzifferer von den Fehlern des Gegners lebte. Dumme Chiffrierfehler wurden von Chiffriersekretären begangen. Taktische und strategische kryptographische Fehler unterliefen hingegen den Nachrichten–Führungsstäben bis hin zu den Generälen und Direktoren.[268] Die Aufteilung der Dienste ist auch eine Rivalität zwischen Politikern, wie im Untersuchungszeitraum zwischen Alexander von Bach, Minister des Inneren und Feldmarschall–Lieutenant Kempen, Chef der obersten Polizeibehörde. Das Militär verfügte darüber hinaus wegen seiner Größe über eine eigene Abteilung für das Chiffrierwesen und verfolgte seine eigene Strategie.

Obwohl die historische Kryptographie und ihr Gegner, die Kryptoanalyse, voll von ernster und spannender Geschichten sind, beinhalten sie auch lustige und auch anzügliche Begebenheiten. Das macht sie selbst für Laien interessant und reizvoll.

[267] *Bauer*, Entzifferte Geheimnisse, 430f.
[268] *Bauer*, Entzifferte Geheimnisse, 424.

8 Verwendete Quellen und Literatur

8.1 Quellenverzeichnis

Archivalien aus dem Österreichischen Staatsarchiv:

OeStA/AVA FA Harrach Fam. in spec 206.1 Chiffrierschlüssel, Allgemeines, Instructionen etc. 1658-1677.

OeStA/AVA Nachlässe AN Bach, Karton 28, Pressewesen, fol 00014.

OeStA/AVA Inneres, MdI Präsidium A 1188, Anleitung Chiffrierbuch, Mappe 2227 1850.

OeStA/AVA Inneres, MdI Präsidium A 1188, Mappe 369/1854 M.I.

OeStA/KA NFA HHK AK 4.Armee AK 70, Chiffriertabelle 8588.

OeStA/HHStA, k. und k. Ministerium des Äußern, Administrativer Registratur, Signaturen: AR F55-1 und AR F55-2.

OeStA/HHStA HausA Nl Schlager-Eckartsau 1-2-7.

OeStA/HHStA Handarchiv Kaiser Franz 22, Etui aus Leder.

OeStA/HHStA Sammlung 3, Chiffrenwesen, Mappe: Akten im Betreff der Organisierung der Section für Ziffernwesen und translatorischen Arbeiten, 3. Mai 1848–1870.

OeStA/HHStA Sammlung 3, Chiffrenwesen, Mappe: Personalia.

OeStA/HHStA StK Interiora 17 (alt 24), Chiffrenschlüssel, Mappe: Anonyme Schlüssel K. Franz II. (1792-1835).

OeStA/HHStA StK Interiora 20 (alt 27), Chiffrenschlüssel, Mappe Varia.

OeStA/HHStA StK Interiora 21 (alt ad 27), Chiffrenschlüssel, Mappe 12. November 1860.

8.2 Nachschlagewerk

Meyers Konversationslexikon, Band 15 (Leipzig/Wien [4]1885-1892).

8.3 Literatur

Franz *Adlgasser*, Kontinuität oder Wandel? Wahlrechtsreformen und das österreichische Parlament, 1861–1918. In: Parliaments, Estates and Representation (2005) 149–166.

Friedrich L. *Bauer*, Entzifferte Geheimnisse. Methoden und Maximen der Kryptologie (Zweite, erweiterte Auflage, Berlin/Heidelberg 1997).

Albrecht *Beutelspacher*, Geheimsprachen. Geschichte und Technik (5., aktual. Aufl. München 2012).

Albrecht *Beutelspacher*, Kryptologie. Eine Einführung in die Wissenschaft vom Verschlüsseln, Verbergen und Verheimlichen (Dritte, behutsam verbesserte Auflage, Braunschweig 1993).

Wilhelm *Brauneder*, Die Verfassungsentwicklung in Österreich 1848 bis 1918. In: Helmut Rumpler, Peter Urbanitsch (Hg.), Die Habsburgermonarchie 1848–1918, Bd. 7: Verfassung und Parlamentarismus, 1. Teilband: Verfassungsrecht, Verfassungswirklichkeit, zentrale Repräsentativkörperschaften (Wien 2000) 69–237.

Joseph *Forsach*, Handbuch der electrischen, galvanischen, magnetischen und electro-magnetischen Telegraphie. Ein theoretisch-praktischer Leitfaden zur richtigen Kenntniss der bezüglichen Apparate, Batterien und deren chemischen Prozesse, dann der Ein-schaltungsmethoden, nebst einer umfassenden Schilderung der neuesten Erfindungen und Verbesserungen im Gebiete der Telegraphie und des gesamten hierauf Bezug nehmenden Apparatewesens (Wien, 1854).

Tibor *Frank*, Ein Diener seiner Herren. Werdegang des österreichischen Geheimagenten Gustav Zerffi (1820–1892) (Wien/Köln/Weimar 2002).

Alfred Hermann *Fried*, Das internationale Leben der Gegenwart (Wien/Berlin 1908).

Friedrich Clemens *Gerke*, Der Elektro-Magnetismus als Maschinentriebkraft, Versuch einer Lösung des Problems (Hamburg 1857).

Jaroslav *Hašek*, Die Abenteuer des braven Soldaten Schwejk. Quer durch Ungarn (Berlin/ Weimar 1976).

Waltraud *Heindl*, Gehorsame Rebellen. Bürokratie und Beamte in Österreich. Band 1: 1780 bis 1848 (2. durchgesehene Auflage, Wien/Köln/Graz 2013).

Waltraud *Heindl*, Josephinische Mandarine. Bürokratie und Beamte in Österreich. Band 2: 1848 bis 1914 (Wien/Köln/Graz 2013).

Madeleine *Herren*, Internationale Organisationen im langen 19. Jahrhundert. Internationale Organisationen seit 1865: Eine Globalgeschichte der internationalen Ordnung. Kap. II (Darmstadt 2009).

Harald *Hubatschke*, Die amtliche Organisation der geheimen Briefüberwachung und des diplomatischen Chiffrendienstes in Österreich. In: Mitteilungen des Instituts für Österreichische Geschichtsforschung, Band 83, Heft 3 (1975).

Harald *Hubatschke*, Ferdinand Prantner (Pseudonym Leo Wolfram) 1817-1871. Die Anfänge des politischen Romans sowie die Geschichte der Briefspionage und des geheimen Chiffredienstes in Österreich. Buch 5 und 6 (ungedr. philosophische Diss. Wien 1975).

Pieter M. *Judson*, Habsburg. Geschichte eines Imperiums 1740–1918. Aus dem Englischen von Michael Müller (München 2017).

Leopold *Kammerhofer*, Diplomatie und Pressepolitik 1848-1918. In: Peter *Urbanitsch*, Adam *Wandruszka* (Hg.), Die Habsburgermonarchie 1848-1918, Band VI/I: Die Habsburger-monarchie im System der Internationalen Beziehungen (Wien 1989).

C. L. *Meissner*, Die Correspondenz in Chiffern für Regierungen, Ämter, Kaufleute und Privatiers, welche sich der electro–magnetischen Telegraphen zur Beförderung ihrer Mittheilungen bedienen wollen (Braunschweig 1849).

Jürgen *Mirow*, Weltgeschichte. Entwicklungsdynamik durch die Entstehung von Innovationen. (München 2009).

David Paul *Nickles*, Under the Wire. How the Telegraph Changed Diplomacy. Diplomatic Autonomy and Telecommunications (Cambridge/Mass. & London/England 2003).

Jürgen *Osterhammel*, Die Verwandlung der Welt. Eine Geschichte des 19. Jahrhunderts (Sonderausgabe, München ^{2}2016).

Franz *Pichler*, Die Einführung der Morse–Telegraphie in Deutschland und Österreich. In: e&i Elektrotechnik und Informationstechnik, Heft 9 (Wien 2006) 402–408.

Johann *Prikowitsch*, Telegraph und Telephon in der k. (u.) k. Armee und Marine, Band 1, Herausgeber: Republik Österreich, Bundesminister für Landesverteidigung und Sport (Wien 2016).

Johann *Prikowitsch*, Drahtlose Telegraphie in der k. (u.) k. Armee und Marine, Band 2, Herausgeber: Republik Österreich, Bundesminister für Landesverteidigung und Sport (Wien 2016).

Emily *Rosenberg*, Einleitung. In: Emily *Rosenberg* (Hg.), Weltmärkte und Weltkriege , 1870–1945 (München 2012) 9–32.

Emily *Rosenberg*, Transnationale Strömungen in einer Welt, die zusammenrückt. In: Emily *Rosenberg* (Hg.), Weltmärkte und Weltkriege, 1870–1945 (München 2012) 815–998.

Simon *Singh*, Geheime Botschaften. Die Kunst der Verschlüsselung von der Antike bis in die Zeiten des Internet (München/Wien 2000; Taschenbuch, München ^{4}2003).

Franz *Stix*, Zur Geschichte und Organisation der Wiener Geheimen Ziffernkanzlei (Von ihren Anfängen bis zum Jahr 1848). In: Mitteilungen des Instituts für Österreichische Geschichtsforschung, Band 51 (1937).

Stephan *Vajda*, Felix Austria, Eine Geschichte Österreichs (Wien/Heidelberg 1980).

Karl *Vocelka*, Geschichte Österreichs: Kultur-Gesellschaft-Politik. Der Neoabsolutismus (Graz/Wien/Köln 2000; Heyne Taschenbuch, München ^{5}2002).

Roland *Wenzlhuemer*, Connecting the Nineteenth–Century World: The Telegraph and Globalization (Cambridge 2013).

Roland *Wenzlhuemer*, Editorial–Telecommunication and Globalization in the Nineteenth Century. In: Global Communication: Telecommunication and Global Flows of Information in the Late 19th and Early 20th Century. (Historical Social Research, Vol. 35, 2010) 7–18.

Roland *Wenzlhuemer*, Globalization, Communication and the Concept of Space in Global History. In: Global Communication: Telecommunication and Global Flows of Information in the Late 19th and Early 20th Century. (Historical Social Research, Vol. 35, 2010) 19–47.

8.4 Internetressourcen

Allerhöchstes Patent vom 15. März 1848. Verleihung der Constitution und Aufhebung der Censurgesetze. Online unter: <http://alex.onb.ac.at/cgi-content/alex?aid=pgs&datum=1848&page=88&size=45> (17. Oktober 2017).

Wolfgang *Ertl*, Angewandte Kryptographie (München ^{4}2012) Online unter: <www.fh-weingarten.de/~ertel/kryptobuch.html> (28. September 2016).

Magdalena *Kersting*, Sammlung und Physikalisches Museum. Der Gauß–Weber–Telegraf. Fakultät für Physik, Universität Göttingen (Göttingen 2012/13). Online unter: <https://www.uni-goettingen.de/document/> (20. März 2017).

MFCA, Marine Funker Club Austria.
Online unter: <http://www.qth.at/mfca> (2. März 2017).

Josef *Nussbaumer*, Andreas *Exenberger*, Zitat nach Chronik der Technik (1993). Online unter: <http://homepage.uibk.ac.at/~c43207/die/papers/globchiff.pdf> (7. Jänner 2017).

Franz *Pichler*, Drahtlos über den Atlantik. Erste Telegraphie–Funkübertragung durch Guglielmo Marconi vor 100 Jahren. Online unter: <http://www.univie.ac.at/pluslucis/PlusLucis/021/s18_21.pdf> (21. August 2017).

9 Tabellen- und Abbildungsverzeichnis

9.1 Tabellen

Tabelle 1: Häufigkeitsverteilung der Buchstaben des deutschen Alphabets.
Quelle: Albrecht *Beutelspacher*, Kryptologie. Eine Einführung in die Wissenschaft vom Verschlüsseln, Verbergen und Verheimlichen (Dritte Auflage, Braunschweig 1993) Seite 18.

Tabelle 2: Häufigkeiten der Bigramme in der deutschen Sprache
Quelle: Albrecht *Beutelspacher*, Kryptologie. Eine Einführung in die Wissenschaft vom Verschlüsseln, Verbergen und Verheimlichen (Dritte Auflage, Braunschweig 1993) Seite 25.

Tabelle 3: Vigenère Quadrat:
Quelle: Wolfgang *Ertl*, Angewandte Kryptographie (München ^{4}2012)
Online unter: <www.fh-weingarten.de/~ertel/kryptobuch.html> (28. September 2016).

Tabelle 4: Ersetzungstabelle für eine homophone Chiffre.
Quelle: Albrecht *Beutelspacher*, Kryptologie. Eine Einführung in die Wissenschaft vom Verschlüsseln, Verbergen und Verheimlichen (Dritte Auflage, Braunschweig 1993) Seite 36.

Tabelle 5: Alphabet nach Clemens Gerke, zu Ehren Morses „Morse Alphabet“ genannt.
Quelle Internet: <http://www.treffpunkt-ostsee.de/maritimes/morsezeichen.php#maritimes> (29. Sept. 2016).

9.2 Abbildungen

Abbildung 1: Skydale (Holzstab).
Quelle: Geheime Botschaften, Die Kunst der Verschlüsselung von der Antike bis in die Zeiten des Internet, Seite 21.

Abbildung 2: Die Caesar-Verschiebung, auf einen kurzen Text angewendet.
Quelle: Simon *Singh*, Geheime Botschaften, Die Kunst der Verschlüsselung von der Antike bis in die Zeiten des Internet, Seite 25.

Abbildung 3: Geheimzeichen Karls des Großen
Quelle: Friedrich L. *Bauer*, Entzifferte Geheimnisse. Methoden und Maximen der Kryptologie (Zweite, erweiterte Auflage, Berlin/Heidelberg 1997) Seite 46.

Abbildung 4: Freimaurerchiffre
Quelle: Friedrich L. *Bauer*, Entzifferte Geheimnisse. Methoden und Maximen der Kryptologie (Zweite, erweiterte Auflage, Berlin/Heidelberg 1997) Seite 46.

Abbildung 5: Maria Stuarts Nomenklator. Geheimtextalphabet und Codewörter.
Quelle: Simon *Singh*, Geheime Botschaften, Die Kunst der Verschlüsselung von der Antike bis in die Zeiten des Internet, Seite 57.

Abbildung 6: Auszug aus dem Nomenklator mit einigen Codes mit wiederkehrenden a e i o u.
Quelle: OeStA/AVA FA Harrach Fam. in spec 206.1, Ciffren–Schlüssel, Allgemeines, Instructionen etc. 1658-1677. Archivum Domitum AB Harrach.

Abbildung 7: Vorderseite der Zirkularscheibe mit dem Chiffren–Schlüssel Nr. 10.
Quelle: OeStA/HHStA Handarchiv Kaiser Franz 22. Etui aus Leder.

Abbildung 8: Zwei- und dreistellige Tabelle für den mechanischen Chiffren-Schlüssel 10.
Quelle: OeStA/HHStA Handarchiv Kaiser Franz 22, Mappe 1-10.

Abbildung 9: Ausschnitt aus der ersten Zifferntabelle über 20 Zeilen der ersten drei Rubriken.
Quelle: OeStA/HHStA StK Interiora 20, Chiffrierschlüssel, Mappe Varia.

Abbildung 10: Wheatstones Zeiger-Telegraph mit Echappement.
Quelle: Joseph *Forsach*, Handbuch der electrischen, galvanischen, magnetischen und electromagnetischen Telegraphie (Wien, 1854) Anhang 13, Fig. 80.

Abbildung 11: Die Doppeltaste für die modifizierte Form des Telegraphie–Systems von Alexander Bain.
Quelle: Johann *Prikowitsch*, Telegraph und Telephon in der k.(u.) k. Armee und Marine, Band 1 (Wien 2016) Seite 24.

Abbildung 12: Der Schreibapparat um etwa 1850.
Quelle: Johann *Prikowitsch*, Telegraph und Telephon in der k.(u.) k. Armee und Marine, Band 1 (Wien 2016) Seite 22.

Abbildung 13: Telegraphenapparat Modell 1892, Erzeugnis J. Schäffler Wien.
Quelle: Johann *Prikowitsch*, Telegraph und Telephon in der k. (u.) k. Armee und Marine, Band 1 (Wien 2016) Seite 32.

Abbildung 14: Pultstation für eine „händische Vermittlung“ hergestellt in der Telephon-Fabrik A.G. Wien, etwa 1905.
Quelle: Johann *Prikowitsch*, Telegraph und Telephon in der k.(u.) k. Armee und Marine, Band 1 (Wien 2016) Seite 147.

Abbildung 15: Feldtelegraphenapparat M. 1892, Erzeugnis Leopolder & Sohn.
Quelle: Johann *Prikowitsch*, Telegraph und Telephon in der k.(u.) k. Armee und Marine, Band 1 (Wien 2016) Seite 30.

Abbildung 16: Der von der russischen Artillerie verwendete Ziffernkode mit Zahlen von 800 bis 988 wurde komplett entziffert.
Quelle: Johann *Prikowitsch*, Telegraph und Telephon in der k.(u.) k. Armee und Marine, Band 1 (Wien 2016) Seite 268.

Abbildung 17: Anlage A als Beispiel aus dem 25-seitigen Chiffrierbuch.
Quelle: C. L. *Meissner*, Die Correspondenz in Chiffern für Regierungen, Ämter, Kaufleute und Privatiers (Braunschweig 1849) Anlage A. Seite 12.

Abbildung 18: Die ersten 10 Zeilen der Seite 1 des Ziffernheftes, von insgesamt 27 Seiten.
Quelle: OeStA/HHStA StK Interiora 21, Chiffrenschlüssel. Mappe: 12. November 1860. Scan des Ziffernheftes.

Abbildung 19: Ausschnitt aus der Chiffriertabelle mit Begriffen und zugehörigen Zahlen (von 001 – 999).
Quelle: Johann *Prikowisch*, Drahtlose Telegraphie in der k.(u.) k. Armee und Marine, Band 2 (Wien 2016) Seite 390.

Abbildung 20: Ausschnitt aus den Chiffriertabellen 4 und 5, die in Niederösterreich verwendet wurden. Diese enthalten nur Silben und kurze Worte.
Lange Begriffe wurden aus Silben und Buchstaben zusammengesetzt.
Quelle: Johann *Prikowitsch,* Drahtlose Telegraphie in der k. (u.) k. Armee und Marine, Band 2 (Wien 2016) Seite 392.

Abbildung 21: Auszug aus der Tabelle des vierziffrigen Chiffrierschlüssels, der eine Auswahl von maximal 9 999 Begriffen umfasste.
Quelle: Johann *Prikowitsch,* Drahtlose Telegraphie in der k. (u.) k. Armee und Marine, Band 2 (Wien 2016) Seite 393.

Abbindung 22: Schlüsseltafel des österreichischen Militärs für untergeordnete Zwecke.
Quelle: Johann *Prikowitsch,* Drahtlose Telegraphie in der k. (u.) k. Armee und Marine, Band 2 (Wien 2016) Seite 395.

Abbildung 23: Auszug aus den dreisprachigen Chiffriertabellen, deutsch, ungarisch und kroatisch.
Quelle: Johann *Prikowitsch,* Drahtlose Telegraphie in der k. (u.) k. Armee und Marine, Band 2 (Wien 2016) Seite 397.

Abbildung 24: Auszug aus dem vierstelligen Friedensschlüssel Nr. 16 für den Chiffrant.
Quelle: Johann *Prikowitsch,* Drahtlose Telegraphie in der k. (u.) k. Armee und Marine, Band 2 (Wien 2016) Seite 399.

Abbildung 25: Ausschnitt aus dem 1. Teil der Wort–Chiffrenkodex mit Kenn- und Bestimmungsworten.
Quelle: Johann *Prikowitsch,* Drahtlose Telegraphie in der k. (u.) k. Armee und Marine, Band 2 (Wien 2016) Seite 402.

Abbildung 26: Chiffriertabelle und Dechiffriertabelle Nr. 8588 von 1914, in Postkartengröße.
Quelle: OeStA/KA NFA HHK AK 4. Armee AK 70, Chiffriertabelle 8588.

Abbildung 27 : Verteiler zu Chiffriertabellen zum Erlass, KM Präs. Nr. 8711/1915.
Quelle: OeStA/KA NFA HHK AK 4.Armee AK 70, Brief KM Präs. Nr. 8711, vom 10.Mai 1915.

10 Abstract

Seit etwa 2500 Jahren verlassen sich gekrönte Häupter und Generäle auf sichere Nachrichten, um ihre Völker und Armeen zu führen. Verschiedene Methoden zum Verbergen von Nachrichten, später Steganographie genannt, wurden etwa 2000 Jahre lang für vertrauliche Mitteilungen angewendet. In der gleichen Zeit entwickelten sich Verfahren, die den Text der Nachricht unverständlich machten, die Kryptographie. Parallel zur Entwicklung der Kryptographie entstand die Kryptoanalyse, eine Methode zur Entschlüsselung der Codes und Chiffren, ohne den Schlüssel zu kennen. Als Folge eines regen diplomatischen Lebens wurden die Kryptographie und Kryptoanalyse während und nach der Renaissance wichtige Dienste. Alle Staaten begannen "Schwarze Kammern" einzurichten, in denen Kryproanalytiker arbeiteten, um durch Briefspionage die Absichten anderer Staaten zu erfahren. Obwohl die Kryptographie eine lange Geschichte hat, dauerte es bis ins 19. Jahrhundert, bis die Kryptographie und Kryptoanalyse strategische Methoden entwickelte.

In den ersten fünf Kapiteln widmet sich die Arbeit der Beschreibung historischer Methoden, vertrauliche Nachrichten zu verschlüsseln, sowie der technischen und vertraglichen Entwicklung der Telegraphie. Im sechsten Kapitel werden die Methoden in der zweiten Hälfte des 19. Jahrhunderts bis zum Beginn des ersten Weltkrieges im Kontext mit der Einführung der Telegraphie beschrieben. Ab Mitte des 19. Jahrhunderts ermöglichte die Telegraphie eine rasche Kommunikation quer durch den Kontinent und durch die Meere nach der Verlegung von Unterwasserkabeln, womit ein globales Telegraphie-Netzwerk entstand. Der rasche Austausch von Nachrichten hatte einen dramatischen Einfluss auf die Diplomatie, Agenten und Militärorganisationen. Eine zweite Ursache für die rasche Entwicklung der Chiffrierung von Nachrichten war die politische Situation in der Habsburger Monarchie nach den Revolutionen im Jahr 1848 und der Entstehung des Neo-Absolutismus.