Was it a Sudden Shift in Professionalization?

Austrian Cryptology and a Description of the Staatskanzlei Key Collection in the Haus-, Hof- und Staatsarchiv of Vienna

Benedek Láng
Budapest University of Technology and Economics
1111, Budapest, Egry József u. 1
benedeklang@gmail.com

Abstract

Cipher keys and code tables in the archives are easy to recognize, but hard to locate. The Staatskanzlei materials preserved in the Haus-, Hof- und Staatsarchiv in Vienna include half a thousand cipher keys and code tables in large cardboard boxes. This exceptionally rich and concentrated cryptologic collection sketches beautifully the four-hundred years of Habsburg diplomacy, as it was precisely the State Chancellery (and its predecessor organizations) that controlled Austrian foreign policy. The paper provides the first detailed description of this collection which is fairly exceptional not only for its historical significance, but also because historians rarely find such a large collection of keys in one single place.

1 Introduction

Encrypted Austrian despatches did not constitute a challenge to foreign deciphering cabinets (particularly to the English Deciphering Branch) in the first half of the eighteenth century. Following the mid-century, however, the situation changed dramatically, and Viennese messages started resisting adverse codebreaking efforts efficiently. Meanwhile, Austrians became famous for being able to decrypt French codes (Ellis 1958, 73). This change had to do with the reorganization of the Austrian black chamber (the *Geheime Kabinets-Kanzlei*) under its newly appointed head, Baron Ignaz von Koch, and under the State Chancellor, Wenzel Anton Kaunitz, who initiated a complete turn in foreign policy, the so-called "diplomatic revolution." (Andrew, 2018, 277-279). The quick growth in professionalization did not remain unnoticed in international diplomacy, Baron von Koch famously complained: "Unfortunately we have the reputation of being too skillful in this art and as a result, the courts which fear that we could be in possession of their correspondence change their [cipher] keys and each time adopt ones which are more difficult and troublesome to decipher" (Kahn, 1967, 163-165).

This was the era when large and professional codebreaking units were already in function all over Europe: the so called black chambers, which were larger and already more organized than a small group of talented mathematicians and their fellow clerks, that used to constitute the typical codebreaker units of the 16th-17th centuries (Leeuw, 2015). The Austrian black chamber was one famous actor in this chapter of crypto-history (Auer, 2015; Pecho, 2015, Walter, 2018).

Though the successful emergence of the Austrian black chamber might have many – both organizational and technical – aspects, this paper addresses one specific question: how far is this change reflected in the encrypting methods applied?

A practical way to answer this question is to review systematically the cipher keys and code tables of the Austrian empire. Fortunately, an exhaustive collection of them survived in the archives of the State Chancellery of Vienna (within the Haus-, Hof- und Staatsarchiv). The Staatskanzlei sources contain nearly half a thousand keys in rough temporal and alphabetical order classified in nine large boxes (ÖStA HHStA Staatskanzlei Interiora Chiffrenschlüssel Kt. 13–21.) out of which the first six – including 480 cipher keys and code tables – form the basis of this investigation.

This exceptionally rich collection sketches beautifully the four-hundred years of Habsburg diplomacy (Láng, 2018). The State Chancellery controlled foreign policy from the mid-eighteenth century until 1848. Its documents – kept in the House, Court and State Archives – ultimately incorporated the key collections produced by its pre- and parallel organizations, the Hofkanzlei (1527-1558), the Reichshofkanzlei (1558-1806) and the Österreichische Hofkanzlei (1620-1848), hence the researcher is privileged to find a complete documentation of Austrian crypto-history in one place (Auer, 2015; Fazekas, 1998).

A complete list and detailed description of the archival items discussed in this article are available in the Decode database (Megyesi et al., 2019).[1]

2 Boxes no. 13 and 14

The first part of the first large cardboard box (Kt. 13. Fasc 19) has not much cryptologic significance, it contains ceremonial documents. It is in the following fascicle (Kt. 13. Fasc 20, fols. 1-257 Benannte Schlüssel), where the real story begins. These nearly 500 pages primarily – but not exclusively – contain 16th and 17th century cipher keys. These keys originate most probably from the collections of the predecessor institutions of the State Chancellery. Apparently, no security measures aimed at the destruction of the keys, which did not seem necessary in the center of the Holy Roman Empire, just the opposite, they scrupulously preserved and classified them. Not surprisingly, the most typical structure appears to be a one-page system, consisting of a homophonic method with three or four alphabets and a nomenclator table with approximately one hundred code words. Cipher alphabets are usually numbers, sometimes letter-groups. Inventive graphic signs are not missing either, particularly from the beginning of the period covered, but occasionally even from the 17th century.

On fols. 9-15 (and once again on fols. 15-19) one can see a rather rare homophonic system, where two letters correspond to each letter of the plain alphabet, while bigrams composed of letters appear also in the nomenclator table (this time the first letter is often capitalized). The list of nomenclators extend beyond four hundred. More than one hundred nulls – "errantes" as they are named in the system – are listed, and they have the same appearance as the other cipher letters, which make the system resistant. This table was used in 1568 by the Austrian ambassador next to the Pope: as usual in other collections as well, those systems seem to be the most advanced, that were used in communication with Italian political centers.

A beautiful example of a special subtype of nomenclators appears on fol. 28 used in relation to the Polish delegate (of which subtype one can see many more examples in the following boxes), where meaningful codewords, metaphors correspond to the name of political actors in the table. Dux is primus, Princeps is secundus, Pontifex maximus is bonus in a somewhat recognizable way, but when Imperator is gravis, Imperatrix is mens, and Palatinus Cracoviensis is species, the codebreaker quickly loses thread.

An exciting example of differentiating between encoding (chiffre chiffrant) and decrypting (chiffre déchiffrant) tables can be seen on fols. 32-33 and 34-36. The chiffre chiffrant is arranged in alphabetic order, while the chiffre déchiffrant is arranged according to the numbers of the cipher alphabet. This table is unfortunately undated, probably it survived from the 18th century, and it was used in relation to Berlin.

The following tables (that of Ogier Ghislain de Busbecq, the Habsburg delegate (of Dutch origin) to Suleiman between 1554 and 1562, and those Castaldo and Caraffa, all from the mid-16th century) share a preference towards sophisticated graphic signs in the alphabet, and towards no less sophisticated metaphors in the nomenclator table (Papa: Andromedes, Cardinalis: Antistes, Petrus Aldombrandinus: Amorius, Imperator: Benignus, Rex: Bruno, etc).

[1] https://cl.lingfil.uu.se/decode/database/search

A large double table system of Prince Eugene of Savoy from the years 1690 also appears to be in this collection: on fols. 90–103, one reads a well-structured encoding system composed of 2-4 numbers, while on fols. 104-123 the déchiffrant of the same system arranged according to the numbers – up to 2400.

As for the initial question of this article, the table of delegate Hoffman in London has special significance (fols. 152–157, Figure 1). It is a large system composed of numbers, clearly dated from the pre-Saatskanzlei period (1721, i.e. when Austrian codes were easy to break by the English codebreaking department). However, the system is so wide, composed of one thousand items and assigning three trigram homophones of trigrams to each syllables, that it is hard to imagine it was indeed vulnerable.

If one last example can be highlighted from the collection of this box, the choice would certainly fall on the 1583 table of Archduke Karl (fols. 243-244, Figure 2). This is a particularly beautiful system copied on parchment (as opposed to most of the others copied on paper): a three-page system with the usual preference towards beautiful graphic signs, combined with a few numbers.

Interestingly, the same fascicle is continued in the following box (Kt. 14. Fasc 20, fols. 259-429). The content, approximately 120 keys from the 16th-17th, and rarely from the 18th centuries, is not different either.

Besides the dominance of the usual one or two-page homophonic systems (named and dated in a larger proportion than in the previous box), fols. 132–135 should be highlighted, because these contain pre-printed lists comprising of an alphabet and a large list of nomenclators. The user, that is, the inventor of the cipher system, has no other duty than to fill in the sheet with randomly assigned numbers, giving birth to a new system. On these folios, one finds four different ways of filling in the table (i.e. four different cipher systems). One of these was used in relation to France, but it is not dated. On fols. 136-141, the same pre-printed tables remained empty. Such an automatized preparation of inventing new ciphers definitely marks an important moment in professionalization.

The 1570 system of Carolus Rym (fols. 291-302, Figure 3) is worth mentioning because of its use of nullities. As it was mentioned above, in the Austrian cipher systems there was a tendency to include all those *types* of symbols among nullities, which were otherwise used in the cipher, in order to avoid that the codebreaker can easily distinguish between nulls, symbols standing for letters and nomenclators on mere visual grounds. In Rym's system, however, a new type of null is introduced: typical conjunctions in Latin language (quapropter, deinde, simulatque, quoniam) as well as a few average words (mandavimus, dedimus, renunciatum). Usually, such words may be left as cleartext in encrypted letters. Using them as nulls, is a clever improvement.

On fols. 311-313, one reads again a nomenclator table with metaphors, which allow mapping up a whole power and alliance system of Europe: Papa: pater, Imperator Carolus: dominus, Rex Francorum: patronus, Rex Angliae: theologus, Rex Poloniae: amicus, Eques: vacca, etc. The editor of the system did not lack sense of humor.

In the last part of the box, there is some numbering confusion. In an un-numbered fascicule (or again, numbered as 20th?), we find again ciphers up to the early 18th century on 43 folios, and this is followed by a last fascicle with ciphers and instructions on 16 folios, quite mixed in date and nature.

3 Boxes no 15 and 16

In the following unit of the collection, the landscape changes perceptibly. While one or few page homophonic tables dominated the previous boxes, and multi-page code-tables (where alphabets play only a minor role) played secondary role, here the typical 18th century genre of cryptology, the code-table booklets dominate the collection. The genre of cipher keys becomes more uniform as cryptology enters into a new phase of professionalization. Another change is that most often than not, a new text type is attached to the tables: the "Instructions." While previous cipher keys were also often complemented with a few sentences that explained how they are supposed to be used, from the 18th century, separate two-page long instructions aim to help the user systematically.

The 15th box (fasciculus 21) starts with a large codebook containing an extensive four-digit system (fols. 3-14). However, the alphabetical order of the words and the sequence of the numbers grow parallel, which renders the otherwise strong, nearly 10.000-unit system vulnerable.

A smaller cipher table from 1750 follows (fol. 19), which was used in French relation. It shares the same strength and weakness as the previous one: it is a large, one-page table of nearly 2000 units, in which only odd numbers appear (even numbers are systematically nullities – as the separate French instructions explain on fols. 20-21), but again, the number sequence and the alphabetical order of the nomenclators coincide. Even though it is from the post-Staatskanzlei period (i.e. that is supposed to be very advanced cryptologically), this table rather demonstrates the usual law in history of science: evolution of the methods is not uniform.

Much more resistant is a French speaking system from Milano, that dates from as late as 1824 (fols. 38-47 and 48-53): it has two parts: chiffrant and déchiffrant: large format, multi-page booklets of four-digit numbers, with extensive instructions (Remarques pour l'usage de ce chiffre). Not only words, but usual word combinations are also encoded (such as "avec vous"; "à ces") months, numbers, nations, cities, rivers and person names separately, the alphabetical order not following the numerical one.

This fascicule (the 21st) as well as the following (fasc. 22) contain a lot of similar tables, most of them from the second half of the 18th century, and most of them named after the ambassador who used it. Usually, their measures exceed one thousand items, but do not go above 10 000. Many of them are written in French, a feature somewhat surprising in the center of the Austrian empire. This analysis will skip them now, as they are not structurally different from those discussed above.

Box no 16 goes back in time: its first part contains undated cipher keys from the 16th and the first part of the 17th centuries. Leafing through these 16 folios with the well-known, mostly one page homophonic tables, the reader quickly gets to the time of Emperor Charles IV (starting from fol. 17): 1711-1740.

On fols. 19-20, for example, one can see a system, in which the chiffrant and the déchiffrant parts are already separated, but these are not yet codebooks, rather large homophonic sheets, incarnating the typical cipher key of the period directly preceding the professionalization turn, that arrive with the formation of the Staatskanzlei in the mid-18th century. These sheets (as those on fols. 22-23, fols. 24-26) together with Leopold I's ciphers (separate fascicle within fasc 23, fols. 1-29), and even many from the time of Maria Theresa (1740-1780) (alt fasc 18/a: fols. 1-84) are typical for this transition period, easily distinguishable from the full-fledged codebooks contained by the previous box and discussed above. Contradicting our intuition, some of these keys belonging to the pre-codebook period are dated from 1752, and even from 1759 (Maria Theresa, fols. 19-22), which is a challenge to explain.

Fortunately, the box finishes with proper code-books (fols. 61-84) from 1770.

4 Boxes no 17 and 18

The shift in professionalization becomes complete in box no. 17.

Fascicule no 24 is the second part of Maria Theresa's cryptology (1740-1780). Cipher keys are always composed of three parts: the 2-4 page long instructions (such as on fols. 3-4), the chiffre chiffrant using 4 four-digits in alphabetic order (fols. 16-29) and the chiffre déchiffrant arranged according to the numbers (fols. 5-16). These large tables try to be inclusive as far as encrypted words, names and notions are concerned, they contain approximately 10 000 items, that is, ten times as large as the previously detailed one sheet homophonic tables (such as on fol. 60, which is clearly an exception in this box, true, it is undated). Instructions have a tendency to define nullities (errantes) in increasing sophistication. Most of them are in French in these times.

The next fascicule contains anonym keys from the time of Joseph II and Leopold II. Fols. 87-100 is a huge code-book from 1789, fols. 101-104, and 105-112 is another one from 1790, fols. 113-115, and 116-119 is a third one from 1792, all of them in French.

This is followed by a parcel containing the ciphers of Francis II (1792-1835). A 1803 key used in relation to St. Petersburg assigns characters to the comma, question mark, parentheses, and numbers that serve as special markers and they are meant to delete the previous or the following character (fols. 120-124 and fols. 126-131). This key is not entirely French anymore, it contains Latin and German words as well, probably with the intention of being as practical for letter writing (which often happened in a somewhat mixed terminology) as possible. The whole fascicule is composed of such booklets, sometimes even bound in

beautiful paper binding (fols. 194-8, from 1812, Déchiffrant pour la correspondence militaire).

And finally, box no. 18 (fasc. 25) is a collection of ten claves (fols. 1-144). The first is an un-named, relatively small (one sheet with three digit numbers), probably early system (fols. 1- 4).

This is followed by several multi-page booklets (separating the encoding and decrypting parts), with four digit numbers and with instructions – these times in German (fol. 38-40; 58-60; 78-80, 102-104, 115, 124-126, and 132-135). Alphabets are not separated anymore from the table, letters appear among the codewords, double letters and other characters. The very last one, the tenth cipher has instructions (fol. 140), but the tables are half empty. It is prepared with the words on a few pages, but the cipher characters are not assigned, the system remained unfinished (fols. 139-142).

5 Conclusions

What kind of answer can be given on the basis of this methodical analysis to the initial question? As for the dramatic change taking place in around in 1742-4 under the leadership of Baron von Koch, as a result of which Austrian ciphers started to resist the codebreaking attempts of English cryptanalysts, the results are ambiguous.

On the one hand, one can plausibly argue that important changes took place in these years, this is when the Staatskanzlei was formed, which took over the tasks of its predecessors. Only a few keys and code tables survived in the collection, that was used in relation to London, and many of these are not even dated. In general, however, comparing the complexity of the pre-1742 keys with the keys of the Chancellery dating from the second half of the 18th century, one can say that there was really a change. The majority of the former keys are composed of 1000 items, usually numbers from 1 to 999, and these are complex homophonic tables with nomenclatures. The majority of the post 1742 keys, however, are code books, several page long leaflets, usually composed of 10 000 items (four digit numbers) complemented with professional instructions.

On the other hand, there are too many exceptions from this rule. There are several huge Austrian codebooks already from the pre-1742 period (including for example one from 1721, London), which make the impression of being very hard to decrypt, and there are also many one-page homophonic tables from the post 1742 period, which seem to be easy to solve (including one for example from 1750, France). Having reviewed a large number of materials (almost 500 keys and codebooks), one can only claim with reservations, that a dramatic technical improvement was introduced in those years.

It is logical to suspect, nevertheless, that something else was really improved with the professionalization of the Chancellery. It is perhaps not – or not only – the cipher systems on a technical level, but rather their application: more care was paid when using the given cipher systems. It is not an over-interpretation of the archival material to suppose that scribes were following the "instructions," the descriptions attached to the keys, more carefully, and thus gave birth to better encrypted messages. Besides the systematic introduction of these "instructions", a consequent differentiation between chiffrant and déchiffrant tables was also introduced (chiffrant being alphabetically arranged, while the déchiffrant numerically arranged), which allowed a more practical use of the ciphers, and gave less temptation to arrange cipher keys horizontally or vertically in a way that made them vulnerable. But again, all this happened gradually in the previous and following decades, and not exactly in 1742.

Acknowledgments

This work has been supported by the Swedish Research Council, grant 2018-06074, DECRYPT Decryption of historical manuscripts.

I thank the Österreichisches Staatsarchiv, Haus-, Hof- und Staatsarchiv for granting the permission to reproduce the manuscript copies.

I thank István Fazekas and Géza Pálffy for calling my attention to the particularly rich collection of cipher keys and code tables discussed in the paper, Karl de Leeuw for many advices and lively discussions on the significance of the conclusions of the paper, Anna Lehofer for the meticulous work of preparing and uploading the copies of the keys into the database, and finally Beata Megyesi for making this research possible.

References

Christopher Andrew. 2018. *The Secret World: A History of Intelligence.* Yale University Press, New Haven.

Leopold Auer. 2015. Die Verwendung von Chiffren in der diplomatischen Korrespondenz des Kaiserhofes im 17. und 18. Jahrhundert. In Anne-Simone Rous and Martin Mulsow eds. *Geheime Post Kryptologie und Steganographie der diplomatischen Korrespondenz europäischer Höfe während der Frühen Neuzeit*. 153-170. Duncker & Humblot, Berlin.

Chiffrenschlüssel, Österreichisches Staatsarchiv, Haus-, Hof- und Staatsarchiv, Staatskanzlei Interiora, Kt. 13–18. For a list and description of the cipher keys, see: the Decode database: https://cl.lingfil.uu.se/decode/database/search

Kenneth Ellis. 1958. *Post Office in the Eighteenth Century: A Study in Administrative History*. Oxford University Press, Oxford.

István Fazekas. 1998. Az Osztrák Állami Levéltár nyomtatásban megjelent segédletei. (The printed assistances of the Austrian State Archives) *Levéltári Közlemények* 69: 195–219.

David Kahn. 1967. *The Codebreakers – The Story of Secret Writing*. Macmillan, New York; revised and updated edition: 1996. *The Codebreakers: The Comprehensive History of Secret Communication from Ancient Times to the Internet.* New York: Scribner.

Benedek Láng. 2018. *Real Life Cryptology: Ciphers and Secrets in Early Modern Hungary*. Amsterdam University Press, Amsterdam.

Karl de Leeuw. 2015. Books, Science, and the Rise of the Black Chambers in Early Modern Europe. In Rous and Mulsow eds. *Geheime Post.* 87-102.

Beáta Megyesi, Nils Blomqvist, and Eva Pettersson. 2019. The DECODE Database: Collection of Ciphers and Keys. In *Proceedings of the 2nd International Conference on Historical Cryptology, HistoCrypt19*, Mons, Belgium.2015.

Carolin Pecho. 2015. Der Habsburger-Code. Chiffrierte Briefe von Erzherzog Ferdinand an Erzherzog Leopold während des Erbfolgekrieges um Jülich-Kleve als Versuche der Gemeinschaftsstiftung (1609–1610). In Rous and Mulsow eds. *Geheime Post.* 137-152.

Maren Walter. 2018. Ein Maulwurf in Wien? Informationssicherheit, geheimdiplomatische Maßnahmen und Wissensgenerierung während der Vorverhandlungen des Westfälischen Friedenskongresses 1643–1644. In Guido Braun, ed. *Diplomatische Wissenskulturen der Frühen Neuzeit. Erfahrungsräume und Orte der Wissensproduktion*. 161–176. De Gruyter, Berlin.

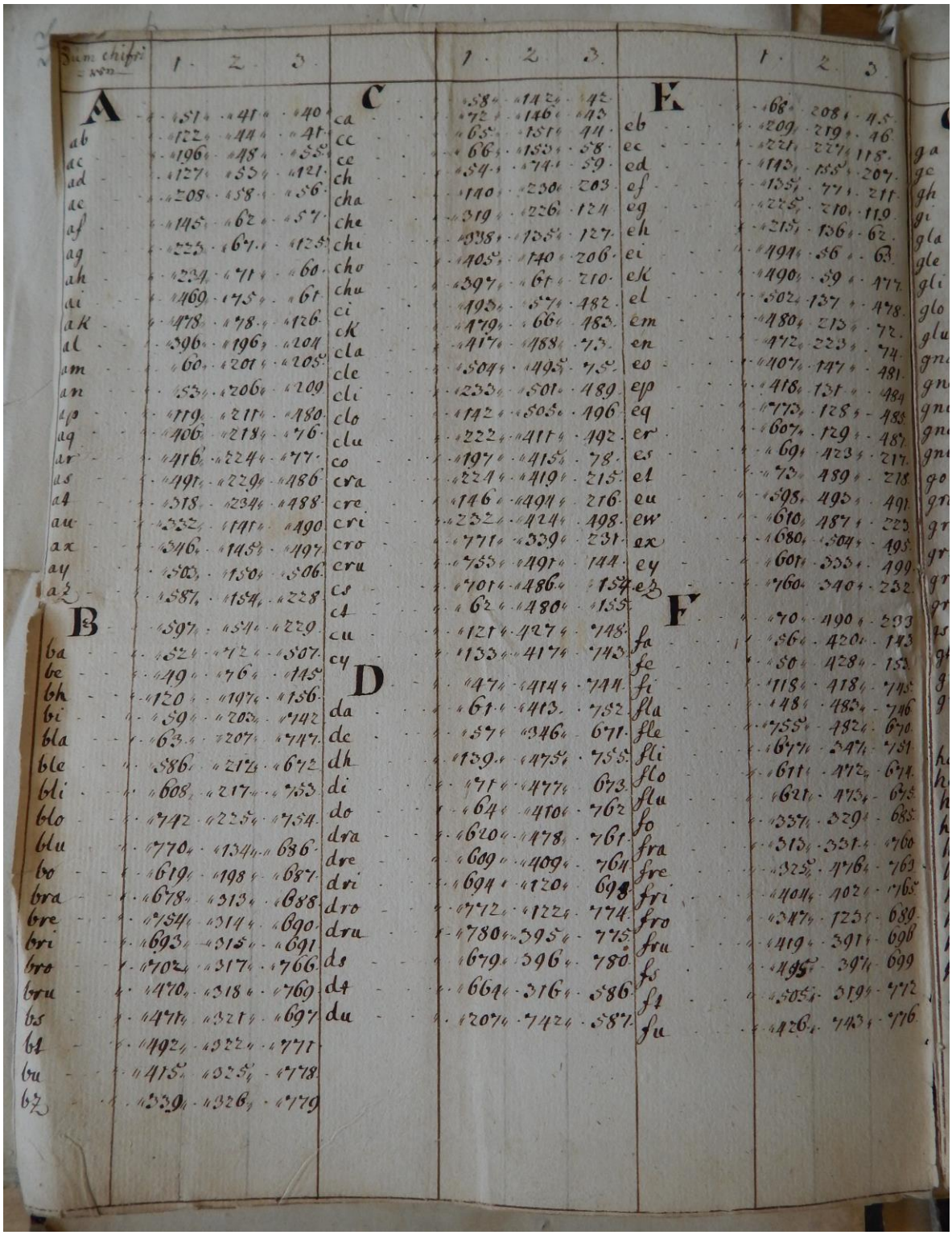

Figure 1. The first page of the cipher key of delegate Hoffman in London, 1721. ÖStA HHStA Kt. 13. fol. 152.

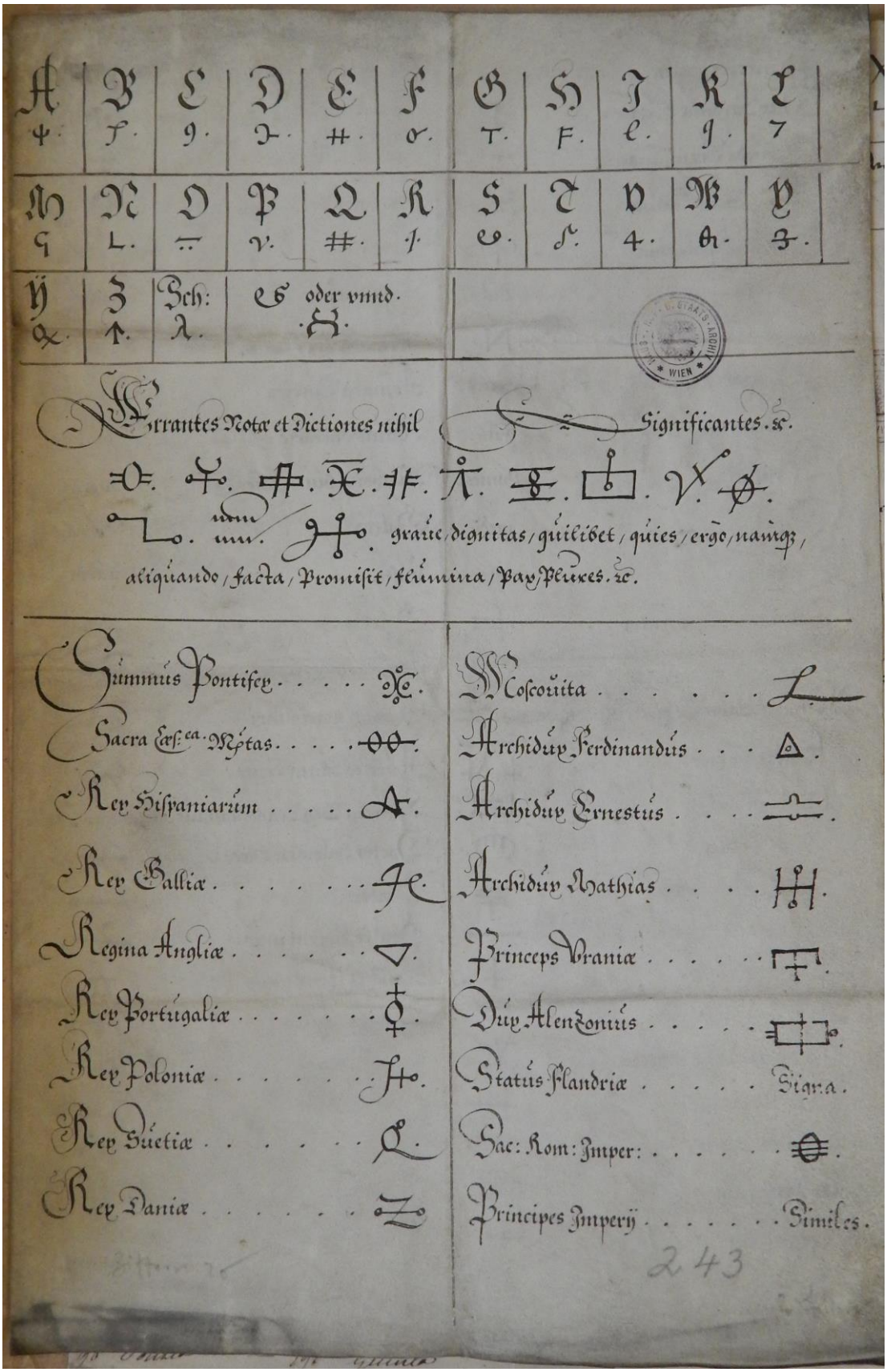

Figure 2. The table of Archduke Karl, 1583. ÖStA HHStA Kt. 13. fol. 243.

Figure 3. The instructions for the key of Carolus Rym, 1570. ÖStA HHStA Kt. 14. fol. 291.