IV. Ein Beitrag zur Geschichte der Dechiffirkunst.

Von

Dr. Heinrich Weber, Lycealprofessor in Bamberg.

Nachstehendes war bereits für den Druck vorbereitet, als ich auf die Mittheilung des Dr. Wagner über die Geheimschrift, richtiger Geheimsprache, aufmerksam wurde, deren sich die Stadt Nürnberg in den Correspondenzen mit ihren Gesandten im Anfang des 16. Jahrhunderts bediente, welche in Band 9. Seite 14—62 dieser Zeitschrift abgedruckt ist. Dieser Mittheilung folgten die „Studien zu einer Lehre von der Geheimschrift“ von demselben Verfasser, deren Fortsetzungen und Schluss erst abgewartet werden mussten, um zu erkennen, ob die Veröffentlichung meiner kleinen Entdeckungen durch jene nicht unnütz gemacht würde. Da nun dieselben in Band 13. S. 8—44 ihren Abschluss gefunden haben, so scheint es mir, als ob meine Funde eine kleine Ergänzung zu diesen Studien bieten könnten.

Zuvor sei hingewiesen auf eine Notiz in der „Innsbrucker Zeitschrift für katholische Theologie“, 1888 S. 379. f., welche den Lesern der „Archivalischen Zeitschrift“ vielleicht nicht allgemein zugänglich ist. Gerbert, als Papst Silvester II. (999—1003), hatte sich in seinen Briefen und Bullen einer Geheimschrift bedient, welche J. Havet, *L'écriture secrète de Gerbert. Académie des inscriptions et belles lettres. Comptes rendus des séances. Serie IV. t. XV. p. 94—112* (Separat Paris, Ricard 1887) als von der tironischen Schrift abweichend bezeichnet, aus dieser aber erklärt und deutet. Havet hielt Gerbert für den Erfinder dieser Schrift, da er dieselbe nirgends sonst fand. P. Viollet war dagegen der Ansicht, dass es verschiedene Schulen für tironische Schrift gegeben

habe, und dass Gerbert in einer solchen mit den von ihm benützten Zeichen bekannt worden sei. Havet stimmt dieser Vermuthung bei und bestätigt sie als richtig (a. a. O. 351—374). Er fand nämlich Gerbert'sche Noten in zwei Notariatsakten aus dem 10. Jahrhundert, welche Professor Cipolla im 25. Band der *Miscellanea di Storia italiana* in photographischer Reproduktion veröffentlicht hatte. Die ältere dieser Urkunden ist vom J. 969, also zwei Jahre vor der ersten Reise Gerberts nach Italien geschrieben. Weitere Belege für diese italienische Tachygraphenschule fand Havet in Urkunden des Archivs der Kathedralkirche zu Asti aus dem 10. Jahrhundert und in einer Cluniacenserurkunde aus derselben Zeit.

Wohl jedes grössere Archiv wird Aufzeichnungen in Geheimschrift enthalten. So auch das Kreisarchiv in Bamberg. Zwei solcher Aktenstücke finden sich in einem Fascikel, welcher vorzugsweise Correspondenzen enthält, die sich auf die Wahl des Johann Gottfried v. Aschhausen zum Fürstbischof von Bamberg (1609) und zu Würzburg (1617) beziehen. Sie stammen aus der Feder eines politischen Agenten in Rom, beide aus dem Jahre 1620, und geben Nachrichten über die Stellung der Curie zur Liga, besonders zu Bayern.¹⁾ Sie tragen keine Adresse, die Anrede lautet: Molto Illustrissimo Signore, im Context V. S. (Vostra Signoria), was wohl nicht die dem Fürstbischof gebührende Titulatur ist; die Unterschrift ist eine absichtlich unlesbar geschriebene Sigle. Der Text ist italienisch, die Eigennamen, Personen-, Orts- und Amtsamen sind fast alle durch Ziffern ausgedrückt und zwar in der Weise, dass der ganze Name durch eine Ziffer bezeichnet ist. Nur bei einem einzigen Namen, für welchen offenbar keine Ziffer vereinbart war, ist jeder Buchstabe durch eine Zahl ausgedrückt. Nach Einlauf der Briefe bei dem Adressaten setzte dieser oder dessen Geheimsekretär nach Anleitung des vereinbarten Schlüssels über die Ziffer das auszudrückende Wort, so dass nun die Correspondenz leicht verständlich ist. Im Nachfolgenden setze ich die im Original über die Ziffern gesetzten Worte in () an deren Seite.

So schreibt z. B. der Agent: Occorse a 137 (Ruspoli) trouarsi col 121 (Cardinale) 22. 6. 34. 35. 2. 44. 36. 10. 38. 14 (Bellar-

¹⁾ Siehe meine Schrift: Johann Gottfried von Aschhausen. Würzburg 1889. p. 85 ff.

minio) per certo negotio d'un suo amico spettante al 116 (Inquisitione¹⁾). . . . Volle 56 (il Papa) parlarli et hauere a bocca quell' informatione, che da altri ha in letere; in somma qui si chiude il ponto, che mouendosi 68 (il duca di Bauiera) et 69 (il duca di Sassonia) per 57 (l'Imperatore), l'Unione non puo resistere. Die Chiffirung des Wortes Bellarminio ist derartig, dass sie die Dechiffirung ohne Schlüssel sehr schwierig machen würde, indem zunächst das doppelte l nur einfach chiffirt ist, und indem für die beiden i zwei verschiedene Chiffren gesetzt sind.

Die Zahlen 68 und 69 sind auch öfter für die betreffenden Länder Bayern und Sachsen gebraucht. Weitere Chiffirungen sind: 70 (Boemia), 103 (Roma), 60 (Redispago), 92 (Cattolici), 105 (Germania), 137 (lo scrittore, auch io, der Agent in Rom), 127 (li Preti), 70 (il Conte Palatino). Einmal hat der Geheimsekretär 57 durch ein Versehen als Sassonia interpretirt, während es l'Imperatore bedeutet.

Uebrigens ist die Chiffirung keineswegs consequent durchgeführt. Mehrere Eigennamen finden sich chiffirt und an anderer Stelle ausgeschrieben; so: Bauiera, Sassonia, Boemia, Corte Romana, Roma, Cesare, il Re, Palatino. Weitere voll ausgeschriebene Eigennamen in den beiden umfangreichen Briefen sind: Alemagna, Germania, Austria, l'Imperio, Ongaria, li Austriaci, gli ambasciatori Bauaro et Magontino, Vienna, Napoli, Lombardia, Carolo V, Duca di Sauoia, Duca di Mantoua, Monferrato, li Spagnoli, Colonna. Wenn auch nicht für alle, so waren doch sicher für die Mehrzahl derselben Chiffren vereinbart gewesen. Jedenfalls war der über die Correspondenz gebreitete Schleier ein ziemlich durchsichtiger.

Nach der gewöhnlichen Annahme war die Chiffirkunst durch Richelieu in die diplomatische Correspondenz eingeführt worden. Da dieser 1616 Minister wurde, so mag die vorstehend erwähnte römische Correspondenz von 1620 auf die von der französischen Diplomatie ausgehende Anregung zurückgeführt werden.

Die im folgenden zu besprechende Anweisung zur Dechiffirung ist auf englischen Ursprung zurückzuführen; auf welchen Autor, muss dahin gestellt bleiben. Der Zeit nach würde die Anregung von Baco von Verulam († 1626) haben ausgehen

¹⁾ Die aus zwölf Cardinälen bestehende Congregatio S. Officii seu Inquisitionis.

können, welcher nach Wagner (Band 13, 9) ein sicheres Urtheil über den Werth verschiedener Geheimschriften und die Leichtigkeit oder Schwierigkeit, dieselben zu dechiffriren, hatte. Die von Wagner angeführten englischen Kryptographen Wilkins (1641) und Wallis (1647) fallen später. Die Veröffentlichung dieser Anweisung hat wohl kaum einen praktischen Nutzen; aber für die Geschichte der Dechiffirkunst und namentlich durch die Thatsache, dass ein englisches Original der für Deutschland bestimmten Bearbeitung zu Grunde liegt, mag sie immerhin von Interesse sein. In welchem Verhältniss die von deutschen Gelehrten gebotenen Anweisungen zur Dechiffrirung lateinischer Texte, deren Wagner Erwähnung thut, zu der unsrigen stehen, vermag ich nicht zu beurtheilen, da mir die betreffenden Werke nicht zur Hand sind. Jedenfalls ist sie um vieles älter, als die von Wagner besprochenen Druckschriften.

Nämlich in demselben Aktenfascikel des k. Kreisarchives in Bamberg, welcher die oben besprochenen römischen Correspondenzen enthält, finden sich zwei vergilbte, stark defekte Folio's mit der Inhaltsangabe: „Regulae ad recognoscendum Cifram incognitam“. Der Schriftcharakter weist auf den Anfang des 17. Jahrhunderts hin. Es ist nicht Abschrift von einem gleichlautenden Original; denn die mir vorliegende Schrift hat mehrfache Correkturen, welche auf ein Schwanken in den zu wählenden Ausdrücken hinweisen. Ebenso wenig ist es das Concept einer Originalarbeit; die Diction ist nicht die eines Mannes, der gewohnt ist, lateinisch zu denken, und den lateinisch concipirten Gedanken sofort niederzuschreiben; zahlreiche Härten im Ausdruck weisen vielmehr darauf hin, dass es eine Uebersetzung aus einem fremden Idiom sei. Bezüglich der Frage, welcher Sprache das Original angehörte, sind wir glücklicher Weise nicht auf Conjekturen angewiesen. Eine an zwei Stellen durchbrechende Gedankenlosigkeit des Uebersetzers zeigt, dass ihm ein englisches Original vorlag. Zweimal nämlich vergass der Schreiber, dass er eine Uebersetzung liefern wolle und schrieb einige Worte des vor ihm liegenden Originals ab, und diese sind englisch. Sofort aber korrigirte er sich, strich die *Lapsus calami* aus und gab den Gedanken lateinisch. Diese beiden sehr erwünschten Aeusserungen der Zerstretheit sind im Texte als Noten angeführt.

Regulae

ad cifram aliquam, sine characteres ignotos in Lingua Latina legendos.

1. Cum characterem Latinum explicare difficile sit ob regularum bonarum defectum, curandum tibi est, vt plures, hoc est quinque vel sex lineae vel ad minimum quatuor tibi scribantur, quo facilius characterum significata conijcere queas. Inde his utere regulis:
2. Si videris verbum quatuor literarum, cuius primae duae syllabae cum duabus vltimis coincident, erit illud verbum fere semper *sese* vel *rara*. Dixi fere semper; potest enim fieri, vt sit aliquod aliud, ut *rere*, *momo*; sed communissime erit *sese*.
3. Quodsi in fine alicuius verbi maxime longioris inueneris vltimo duas literas eodem ordine repetitas, communiter erunt *rere*, vt *miserere*, *arbitrarere*, *viderere* cum similibus.
4. Verbum trium literarum, cujus prima et vltima sint eadem, erit *non* communiter; sunt tamen et alia huiusmodi verba, vt *ala*, *ama*, *ede*, *ibi*, *imi*, *oro*, *sus*, *iui*, *ara*, *eme*, *sis*, *tot*.
5. Si in verbo quatuor literarum duae extremae cum duabus mediis¹⁾ coincident, illud verbum erit *esse* vel *illi* communissime; aliquando *sus*, *ecce*, *assa*, *arra*.
6. Si autem in simili verbo mediae fuerint similes, extremae dissimiles, poterit esse: *ille*, *tuus*, *erra*, *ossa*, *vlli* cum similibus.
7. Cum duae similes literae finiunt verbum, erit litera illa bis repetita „i“, vt *filij*, *Curij*, *Marij*; quodsi post sequatur adhuc altera litera finiens verbum, erit „s“, vt *filiis*.
8. Sed hoc limitandum; saepissime enim accidit, vt illa duplicata litera sit „s“ et sequatur „e“, vt *amasse*, *perdidisse*, *lassi*.
9. Quatuor literarum verba, in quibus prima et tertia litera, item secunda et vltima conveniunt, notabis, qualia sunt *Iris*, *amas*, *vnus*, *caeca*, *nunc*, *viue*, *raro*, *tute*. Secundi generis sunt: *vana*, *vini*, *mihi*, *tibi*, *sibi*, *visi*, *vici*, *vidi*, cum similibus praeterperfectis²⁾ temporibus verborum, item infinitiuis modis, vt *niti* cum similibus; nec non *nisi*, *modo*, *fere*, *sede*, *mene*, *rete* etc.
10. In quo notandum, quod in huiusmodi verbis saepius secunda litera est „i“ propter illos praeteritos perfectos, de quibus supra; deinde etiam propter illa verba *tibi*, *mihi*, *sibi*, *nisi*, quae frequentissime occurrunt. Si contingat, secundam literam non esse „i“, frequenter erit „o“, vt *volo*, *nolo*, *modo*, *foro*, *solo*, *coco*, *dolo* et similes ablatiui casus; possunt tamen et aliae literae esse in secundo loco, vt *praeter*, *prae*.

¹⁾ Richtiger: et duae mediae.

²⁾ Richtig: praeteritis perfectis.

11. Nullae literae in Latino sermone frequentiores „s“ et „t“; praecipue vero in fine verborum, maxime longiorum, adest saepe: „s“.
12. Si duas literas saepius verba terminare videas, earum primam esse „v“ (u), alteram vero „m“ vel „s“ probabiliter existima, vt *diuinus*, *diuinum*, *amatus*, *dilectus*, *dilectum* cum similibus. Alias potest prima litera esse „o“ vel „a“, vt *pulchras*, *formosas*, *magnos*, *robustos*, *robustam*, *paruam*; item „c“ vt *crudeles*, *crudellem*, *fortes*, *fortem* cum similibus.
13. Frequentes sunt vocales maxime in fine verborum, quamvis et consonantes saepe verba terminent, praesertim „s, m, t.“
14. In fine verbi trium literarum si diphthongum repereris, communiter erit illud verbum *quae*; aliquando tamen *suae*, *meae*, *tuae*, *irae*, *orae* cum similibus.
15. Littera¹⁾ reduplicata in medio verbi est frequenter „s“, vt *passer*, *curasses*, *quacassess*, *pessimus* cum similibus; quod porro „s“ praecedit, est vocalis.
16. Est enim regula, quod si inueneris literam reduplicatam, ea communiter est consonans, et litera, quae eam praecedit, sicut et quae subsequitur, est vocalis.
17. Litera sola inventa est semper „a, e, i, vel o“; communiter autem „a“ vel „e“.
18. *Qui*, *quae*, *quid*, *quod*, *quam*, *quem*, *quin*, *quum*, *quos*, *quas*, *quando* etc. aliqua istorum singulis fere insunt periodis; hujus regulae vsus in prima regula patebit.
19. Post q semper venit „v“ (u), vt *quis*, *qui* etc.²⁾
20. Ex his ergo duabus vltimis regulis insignem hanc regulam inueniendum „q“, tum „v“ (u) eliciemus; vbi proposita tibi fuerit cifra, quam interpretari debeas, observa principia verborum, maxime eorum, quae ex 3 aut 4 literis constant, et vide, vtrum literam aliquam reperiās, quae semper per totam istam cifram eandem literam sibi habeat coniunctam; si igitur talem inueneris literam, esse eam „q“ merito suspicari poteris; quae autem sequitur, eam esse „v“ (u). Et haec regula nobis regula Q dicitur, ex qua deinde multae aliae sane pulchrae procedunt.
21. Nam primo certum est, literam, quae „q“ et „v“ (u) sequitur, esse vocalem; quin etiam, quae fuerit, ex contextu cifrae non fiet difficile conjicere.
22. Deinde si alicuius verbi literam antepenultimam esse „q“, penultimam vero „v“ (u) animadverteris, vltimam esse „e“ conjicies; ita enim com-

¹⁾ Hier steht im Original A lett, einer der in der Einleitung erwähnten Lapsus calami, welcher wieder ausgestrichen ist.

²⁾ Dieser Regel geht dieselbe in englischem Idiom vorans: After „q“ comes always an „v“, as *qui* etc.; dieser Satz ist aber wieder ausgestrichen.

- munitur accidit, vt *tibique*, *mihiq*, *aliquae*, cum similibus. Potest aliquando fieri, vt sint aliae vocales, vt *aliqui*, *aliqua*, *aliquo*.
23. Quodsi in hoc casu literam vltimam non esse „i“ comperias, sed aliquam aliam vocalem, duas praecedentes literas esse „l“ et „i“ existimabis; hoc enim frequentissime evenit, vt *aliquo*, *siliqua*, *reliqui*. Idem dicendum, cum post „q“ et „v“ (u) succedunt adhuc duae literae verbum terminantes, vt *aliquas*, *siliquas*, *reliquos*, *aliquis*. Dixi autem: frequentissime; aliquando enim secus accidit, quamuis rarissime, vt in verbis *linguo*, *relinguo*, in quibus tamen tantum litera „N“ inter *li* et *qu* ponitur.
24. Si porro *qu* bis in verbo aliquo repereris, si verbum erit 6 literarum, erit *quoque*; si septem, erit *quinque*. Vides ergo, quam foecunda sit 20^a regula, quae tot bonos foetus pariat.
25. Debes notare maxime verba quaedam, quae ob repetitionem literarum, facilius dinoscuntur, et in cifra tua diligenter advertere, an tales occurrant; quales sunt: *rursus*, *jussu*, *iussi*, *jussit*, *summus*, *esses*, *illis*, *arram*, *erras*, *attamen*, *quandoquidem*, *vllus*, *mitto*, *curru*, *curro*, *possem*, *cuius*, *decedendi*, *manna*, *mappa*, *cappa*, *melle*, *pelle*, *felle*, *messe*, *ferre*, *velle*, *misisse*, *irascere*, *corporis*, *turtur*, *tutus*, *tortor*, *tantas*, *tanta*, *vaquequaque*, *vaquequo*, *admisisses*, *omississes*, *permisisses*, cum similibus; *quarum*, *quibus*, *quorum*, *circa*, *habebas*, *habebatur*, *lactitia*, *nonne*, *petitio*, *succurrat*, *superstitia*. Haec, inquam, et similia tibi seorsum notabis, quoniam postea in cifra inuenta facilius agnoscuntur et magnam cognita lucem indagationi tuae afferent.
26. Sed et hoc notasse velim, maximam in eo tibi adhibendam diligentiam, vt verba, quae in Dictionariolo¹⁾ tuo vel in proxima praecedente regula inueneris, accommodare ad alia possis, habito scilicet temporum, casuum, deriuationum respectu, vt si in cifra verbum *Essem* inuenias, ex verbo *Esses* (quod scilicet habes) agnoscas; similiter ex verbo *Corporis*: *Corpora*; ex verbo *petitio*: *petitioni*; ex *pelle*: *pellet*; ex *succurrat*: *succurrendo*; ex *velle*: *vellem*; ex *turtur*: *turtureus*; ex *tantas*: *tantum* cum similibus dinoscas.
27. Postremo hoc tibi sit maxime persuasum, totam fere hujus indagationis vim in verbulis trium, duarum vel quatuor literarum esse sitam. Quo fit, vt cifrae, quae his abundant, nullo fere negotio (fast ohne Mühe) explicentur; quae vero iis carent, magnam molestiam et laborem sui indagatoribus afferant. Ad ista ergo semper te conuertas et ex iis maxime characterum significationem eruere contendas.
28. Sed et debiles coniecturas saepe (praesertim cum in cifra paucas regulas inuenis) repudiare non debes; sed ex iis probandum, num certi

¹⁾ Sieh dieses am Schlusse.

aliquid conficere¹⁾ possis. Ex incertis enim coniecturis saepe certa consequuntur indicia.

Dictionariolum.

Verba duarum literarum.

A	C	Et	Ii	Ne	Re
Ab	Da	Ex	Io	Ni	Se
Ac	De	F	Is	No	Si
Ad	Do	G	It	O	St
Ah	E	Hae	K	Ob	Tc
An	Ea	Hal	L	Oh	Tu
As	Ei	Hi	Me	Os	Vae
At	En	I	Mi	P	Vi
Au	Eo	Id	Na	Q	Vt
B	Es	In	Nae		

Verba trium literarum.

Abi	Ara	Dea	Eme	Hae	Iro	Nám
Abas	Aro	Deae	Emi	Hei	Ita	Nas
Acu	Ars	Dei	Emo	Heu	Ite	Nec
Ado	Arx	Deo	Ens	Hác	Ito	Nes
Aer	Asa	Des	Eos	Hia	Iui	Neo
Aes	Ast	Del	Ere	Hio	Ius	Nil
Age	Aue	Dem	Eri	Hic	Iuo	Nix
Agi	Aui	Dic	Est	His	Leo	Noé
Aga	Aux	Die	Esu	Hoc	Lex	Nos
Aha	Axe	Diú	Eua	Hos	Lis	Nox
Ala	Axi	Dos	Eum	Huc	Lue	Num
Alae	Azo	Duc	Fac	Hui	Lui	Nux
Ali	Bes	Dúm	Fax	Iam	Luo	Obi
Alo	Bis	Duo	Fer	Ibi	Lux	Oda
Ais	Bos	Dux	Fex	Ibo	Mea	Odae
Aio	Ceu	Eas	Fio	Iis	Meae	Ode
Ain	Cio	Eat	Fis	Ima	Mei	Odo
Ait	Cis	Ede	Fit	Imae	Mel	Ohe
Ama	Cor	Edi	Fui	Imi	Men	Ole
Amo	Cui	Edo	G	Imò	Meo	Ope
Ano	Cum	Ege	Has	Imó	Mos	Opi
Anu	Cur	Ego	Hau	Iob	Mox	Ora
Ape	Das	Eis	Hem	Ira	Mum	Orae
Api	Dat	Eho	Haec	Irae	Mus	Ore

¹⁾ Richtiger conjicere.

Oro	Pio	Res	Sol	Tot	Vel	Vri
Osa	Pix	Reu	Spe	Tua	Ver	Vro
Osae	Prae	Rex	Sta	Tuae	Via	Vsa
Osi	Pro	Ros	Sto	Tui	Viae	Vsae
Oso	Pus	Rus	Sua	Tum	Vim	Vsi
Oua	Qua	Sal	Suae	Tuo	Vir	Vso
Oui	Quae	Sat	Sub	Tus	Vix	Vsu
Ouo	Que	Sed	Sue	Vah	Vis	Vti
Par	Qui	Seu	Sui	Vas	Vgo	Vua
Pax	Quo	Sex	Sum	Vbi	Vna	Vuae
Per	Rea	Sic	Suo	Vda	Vni	X
Pes	Reac	Sim	Sus	Vdae	Vno	Y
Pia	Rei	Sis	Tám	Vdi	Vos	Z
Piae	Rem	Sit	Ter	Vdo	Vox	Finis.
Pii	Reo					

Hoc Dictionariolum, vbi characterum significationem vis conjicere, semper prae manibus habere debes; mirum enim est, quantum laborem tollat et quam ad citam explicationem conferat.

Τελος : Θεώ δόξα και χαρις.