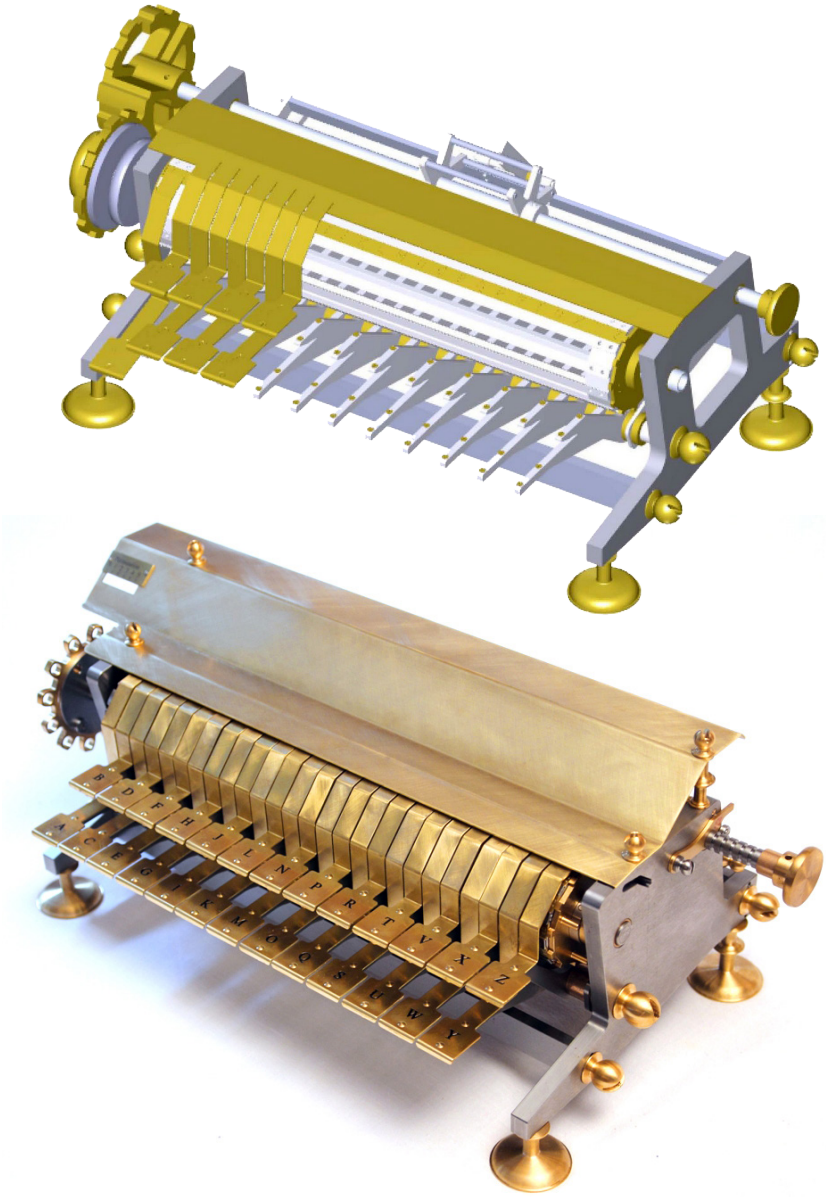
LEIBNIZ AND CRYPTOGRAPHY



Leibniz's machina deciphratoria under production by Klaus Badur and Wolfgang Rottstedt, using design suggestions by Richard Kotler to implement Nicholas Rescher's conceptual reconstruction of the device.

(top) Construction design for the Leibniz's Cipher Machine
(bottom) The Leibniz's Cipher Machine

LEIBNIZ AND CRYPTOGRAPHY

An Account on the Occasion of the Initial Exhibition of the Reconstruction of Leibniz's Cipher Machine

by

NICHOLAS RESCHER

UNIVERSITY LIBRARY SYSTEM,
UNIVERSITY OF PITTSBURGH

PITTSBURGH, PA

Library of Congress Control Number: 2012949833

Published by the Office of Scholarly Communication and Publishing,
University Library System, University of Pittsburgh, Pittsburgh, PA 15260. 2012.

Cataloging-in-Publication Data

Rescher, Nicholas.
Leibniz and cryptography : an account on the occasion of the initial exhibition of the reconstruction of Leibniz's cipher machine / Nicholas Rescher.
xii, 96 p. ; 23 cm.
Includes bibliographical references.
ISBN 978-0-9833584-2-8 (paper : alk. paper)—ISBN 978-0-9833584-1-1 (ebook)
1. Leibniz, Gottfried Wilhelm, Freiherr von, 1646-1716—Knowledge—Cryptography.
2. Cryptography—History—17th century. 3. Ciphers—History—17th century.
I. Title.

B2598.R453 2012 2012949833

For Professor Herbert Breger

My sole predecessor in concern for
Leibniz's work on matters of cryptology

Cryptolysis, ars solvendi aenigmata cryptographica, est summun specimen humanae penetrabililatis. ["Cryptology, the art of solving cryptographic enigmas, is the supreme specimen of human ingenuity.]

G. W. Leibniz
(to John Wallis, 1698)
[AIII,7, p. 759; AI,13, p. 300.]

Contents

Introduction

Reconstructing Leibniz's Cipher Machine

During the 2010-11 academic year I launched into an investigation of Leibniz's dealings with matters of cryptology. In the course of this inquiry I read with surprise in the only recently (2001) published volume of Leibniz's *Sämtliche Schriften* containing several 1688 memoranda that Leibniz prepared that autumn for his audience with Leopold I, the Holy Roman Emperor. In them he described his machina deciphratoria, the cipher machine he had devised in the 1670s and had already briefly mentioned in a 1679 memorandum for John Frederick, the Duke of Hanover.

The information given in those 1688 memoranda regarding the workings of this machine—and in particular, its reliance on the Staffelwalze that was at the core of Leibniz's celebrated calculating machine—proved sufficient to enable its conceptual reconstruction. My engineer friend Richard Kotler helped to fill in some of the details of the gearing, and Klaus Badur of Hanover, who had earlier reconstructed a version of the calculating machine, undertook to arrange for the production of a physical model in collaboration with Wolfgang Rottstedt. The fruit of these efforts is the focus of the present exhibition of this rediscovered machine.

Although there had been earlier cipher devices such as slides or wheels, Leibniz's remarkable apparatus was the first actual cipher machine. Vastly more reliable and easy to use, it had a sophistication not attained again until the Post-World War I era some 250 years after its day.

I am grateful to the University of Pittsburgh for allowing me to dedicate a portion of my research funding to the production of this model

and to Dr. Rush G. Miller, the University Librarian, for his cooperation in arranging for the present exhibition and his unfailingly supportive interest in the entire project. I am also grateful to Jeffrey A. Wisniewski, Kari E. Johnston, and John H. Barnett at the University Library System for their efficient support in regard to publication.

Details about Leibniz's machine and its historical significance are given in my essay on "Leibniz's Machina Deciphratoria: A Proto-Enigma Cipher Machine," in the journal *Cryptologia*. I am grateful to Dr. Craig Bauer, the editor of this publication, for permission to include this article in Chapter II.

Finally, I am grateful to three German Leibniz experts for their help with various aspects of this project: Dr. Herbert Breger, Dr. Sven Erdner, and Dr. Heinrich Schepers. To Dr. Breger belongs the distinction of being the first scholar to address Leibniz's interest in encipherment.

Nicholas Rescher
Distinguished University Professor of Philosophy
University of Pittsburgh

LEIBNIZ AND CRYPTOGRAPHY

An Account on the Occasion of the Initial Exhibition
of the Reconstruction of Leibniz's Cipher Machine

I

Leibniz's Forays in Cryptography

1. Cryptography's Place in Leibniz's Polymathic Project

It is unquestionably an exaggeration to say, with Voltaire, that men use speech only to conceal their thoughts from the view of others. But it is certainly the case that they sometimes do so.

The symbolic encoding of information and its concealment and revelation was of paramount interest to Leibniz throughout his entire career from beginning to end, and was a topic that stimulated his mind in many directions. And cryptography, so Leibniz tells John Bernoulli, is a part of this project that is well deserving the attention of a mathematician.[1] The *art de dechifrer . . . est une matiere encor demy-mathematique*,[2] and finding the key to a cryptogram is akin to finding the solution of equations in algebra.[3]

Thus in a brief 1674 sketch of the Art of Innovation (*ars inveniendi*) states that this includes the ars explicandi crytophemata and, like the latter, admits of pursuit via appropriate general rules.[4] And in a long letter to E. W. von Tschirnhaus of May 1678[5] Leibniz describes cryptography (the *ars deciphratoria*) as an integral part of the *scientia generalis* that has close connections with algebra and constitutes a key component of the *ars combinatoria*.[6] Despite the power of the analytic method it proves insufficient in cryptography, where a more extensive (*longior*) procedure of synthesis will prove necessary.[7] Moreover, encoding transforms the

Gottfried Wilhelm Leibniz (1646-1716)
Engraved by B.Holl, Published in London by W.S.Orr & Co.

foundation of a body of information from one format to another—much as with the representation of geometric figures from diagramatic to algebraic representation in Cartesian geometry. His note of 1678 on the *ars inveniendi* remarks that the *ars deciphrani* represents a sector of the field where analysis alone will not suffice for discovery, and observes that while analysis is generally more difficult, synthesis is more laborious.[8] As to the type of synthetic reasoning involved, Leibniz likens the type of reasoning invoked in decipherment to finding good moves at playing chess.[9]

That everything can be said by the use of numbers is a key thesis of Leibniz's universal characteristic.[10] And in a way, the object of the *ars cryptographica* is the inverse of the Leibnizian characteristic: the latter seeks to make language more perspicuous and transparent, the latter

more difficult of access. Coding and decoding of information in symbolic systems are, after all, inverse procedures and the steps that can make these processes simpler can be reversed to render them more complex and obscure. And Leibniz insisted that in this way advances in cryptography can serve to convey instructive insights into the ways of scientific inquiry. For as Leibniz saw it, cryptanalysis is something of a paradigm for scientific method, the *ars faciendi hypotheses*.[11] Thus he observes that the investigation of causes is easier when different phenomena exhibit a commonality, even as *facilius est cryptographemata solvere, si plures literas occultando sensu secundum eandem clavem scriptas*.[12]

In the Nouveaux Essais Leibniz writes: "L'Art de decouvrir les causes des phenomenes, ou les hypotheses veritables, *est comme l'Art de dechiffrer*."[13] For in scientific explanation "a hypothesis is like the key to a cryptograph, and the simpler it is, and the greater the number of events that can be explained by it, the more probable it is."[14] Leibniz accordingly endorsed fully the idea—already found in Bacon's *Novum Organon* and in the 1586 *Traicté des Chiffres* of the French algebraist and diplomatist Blaise de Vignière[15]—that science aims to decode the secrets of nature. In just this way he claimed in relation to the convervation of force that "j'ay toutes les raisons de croire que d'ay dechifré une partie de ce mystere de la nature."[16]

Leibniz saw what he called "the method of hypotheses" as a key tool of scientific inquiry and the deciphering of a cryptogram was his favorite illustration of the workings of this method of hypothesis-utilization:

> A hypothesis of this kind is like the key to a cryptograph, and the simpler it is, and the greater the number of events that can be explained by it, the more probable it is. But just as it is possible to write a letter intentionally so that it can be understood by means of several different keys, of which only one is the true one, so the same effect can have several causes. Hence no firm demonstration can be made from the success of hypotheses.[17]

To be sure, this method in its application to issues regarding nature is never certain and demonstrative.

For perfectly universal propositions can never be established on this basis (viz., induction based on the experience of particular cases) because you are never certain in induction that all individuals have been consid-

ered. You must always stop at the proposition that all the cases which I have experienced are so. But since, then, no true universality is possible, it will always remain possible that countless other cases which you have not examined are different.[18]

In empirical application to the contingencies of nature the method is always conjectural and yields no more than a probability. As Leibniz sees it, a meaningful decoding is its own verification[19] since in cryptography we deal with a finite body of text and so can attain demonstrative certainty in favorable conditions. However, the observable data of nature's "texts" are limitless so that our "decryptions" thereof afford no more than the moral certainty of high probability.[20] But of course an insufficiency of texts leads to an underdetermination of possibilities and defines description which, after all, requires a sufficiency of data: *aliquando enim tam pauca verba alphabeto incognito scripta habentur, ut prorsus impossible sit humano ingenio clavem reperiri*.[21] Accordingly, while Leibniz envisioned a deep methodological kinship between the use of hypotheses in scientific explanation and in cryptology,[22] he granted that clever guesswork can sometimes surpass the more laborious path of method. And he held that in "the art of deciphering . . . an ingenious conjecture often greatly shortens the road."[23]

Just as with his interest in combinatorics, so Leibniz's interest in a universal character also had a direct bearing upon cryptography.[24] For even as in translation the text of one language is encoded in the vocabulary of another,[25] so an artificial language like the universal characteristic functions in such the same way as encrypted communication. And a universal language can clearly provide an excellent nomenclator for coding. But mere coding is not as yet excipherment and is here that the *ars cryptographica* comes into its own.

Leibniz's' interest in these issues had been enlivened by reading John Wilkins 1668 *Essays towards a Real Character and a Philosophical Language* and he was also familiar with this scholar's earlier *Messenger: Showing how a man may with Privacy and Speed communicate his thoughts to a Friend at a Distance* (London 1641).[26] Wilkins was the first co-secretary of the Royal Society (along with Leibniz's friend Henry Oldenburg), and his work evoked much contemporary interest in cryptology. And already his early work in combinations the issues of codes and ciphers fell well within Leibniz's virtually boundless range of interest and information,

and cryptography had an integral and significant place within the project of *scientia generalis* that was ever a glint in Leibniz's eye. He viewed it as a natural field for the deployment of rules in rational procedure—exactly in the formalized manner to which he was always deeply partial.[27]

As a bibliophile, Leibniz was well aware of the literature on the subject. In 1689, during his Italian journey, he prepared an elaborate "must have" inventory for a *bibliotheca universalis selecta*, some 35 closely packed printed pages in length. This list included a dozen items on steganography cryptology, and verbal concealment.[28]

In May of 1683, Leibniz's long-time helper, collaborator and correspondent J. D. Brandshagen—and eventually one of his most useful links to England where Brandshagen spent much time[29]—wrote to Leibniz about a now-lost letter that Leibniz had written to him in April.[30] Brandshagen complains that the codes mentioned in earlier correspondence—based on the monoalphabetic cyphers issuing from JACOBUS and LABYRINTHUS[31] as key words—will not work in the present instance, but that SALOMONIS will do the trick in that the text can be deciphered on this basis. Already earlier on, Leibniz had recommended such a cipher based on QUIRNHEIM to his correspondent Johann Wilhelm Mers von Quirnheim,[32] alternating the direction of substitution.

And there can be no question that Leibniz had good theoretical insight into matters of cryptography. One clear sign of this is his brief paper on *Praecepta artis decriptoriae* of the middle 1680s.[33] Although it deals primarily only with the issue of finding the language of an encrypted text, it betokens a familiarity with the relevant literature. And in a letter of March 1693 to Count Platen, the Hanoverian prime minister, Leibniz forwarded to him a book entitled *Steganographie* by J. S. Haes, the librarian at the court of Hesse-Cassel.[34] He remarks that this work rightly notes the salient characteristics of a good cipher (1) that it be difficult to decipher, (2) that it be easy to write out, (3) that its use be hard to detect, with its messages easily mistaken for ordinary letters, and (4) that encipherment be simple.

His interest in cryptographical matters crops up at many places in Leibniz's correspondence. Thus in June of 1689 Leibniz reported to his great friend J. D. Crafft that he has received the "character-book" from Munich "und habe den clavem felicissime ausgefunden."[35] At some point in 1690 Crafft borrowed this book from Leibniz and their subsequent correspondence referred to it as "the encrypted book" (*das cifrirte Buch*).[36]

In March of 1691 Crafft promised to return it soon, and he explains the key to Leibniz.[37] At one stage, a postal intermediary between Leibniz and Crafft was Philip Wilhelm von Hörnigk (d. 1714), who became Wirklicher Geheimer Rat and archivist in Passau. In his correspondence with Leibniz during the 1680's von Hörnigk at first sometimes included a few encrypted passages.[38] In January of 1691 Leibniz sent him a letter in which he enclosed another to Crafft which reminded him to return the encrypted book. In his reply von Hörnigk remarked that the book was doubtless still in Crafft's possession.[39] The book dealt with alchemical matters, but its contents disappointed Crafft through their insufficiency of detail: "Es sind keine chymische process drinn, sodern alles auf Ertze gerichtet."[40] As early as Leibniz's service in Mainz, he and Crafft agreed to use a cipher based on the key word LABYRINTHUS for confidentiality in their communication. [41]

Leibniz's correspondence of the late 1690s indicates that the Bernoullis too had some interest in the *ars deciphrandi*.[42] Leibniz saw it as only natural that mathematicians should be interested in cryptography; he viewed cryptography as analogous to algebra, and finding the key to a cipher an analogous to finding the solution of a set of equations.[43] Moreover, Leibniz's interest extended from cryptography to cryptographers. For example, in response to a question, one of Leibniz's Parisian correspondents explained to him in a letter of March 1695, that Antoine Rossignol (1600-1682), Seigneur de Juvisy, conseiller du roi, and *célébre par les dechifrements* was Maitre des Comptes at the French court.[44] His interest in Viète and—as we shall see—above all Wallis further attests to this.

One of the few of Leibniz's discussions of cryptography that is more than perfunctory is a short paper of the mid-1680s labeled *Praecepta artis deciphratoriae*,[45] whose deliberations relate principally to determining the language of the text being deciphered. It does, however, indicate familiarity with the then-current publications the field. And one principle of which Leibniz was acutely aware and which he repeatedly stressed is that the smaller volume of encrypted material that is available, the more difficult the code is to break. Indeed, with a simple nonalphabetic (Caesarian) transposition cipher it is no more than an exercise in combinatorics to determine the amount of text required for a good chance of decipherment. (And here it also it becomes possible to graph the length of text against the probability of successful decryption.)

The Leibniz House in Hanover, Germany
Library of Congress, Prints & Photographs Division, Photochrom Collection, LC-DIG-ppmsca-00451. http://hdl.loc.gov/loc.pnp/ppmsca.00451

2. Leibniz and Secret Communication

Already from the outset of Leibniz's correspondence with Baron Boineburg they used a (simple monoalphabetic) cypher to conceal names and salient expressions.[46] And even Leibniz's very first letter to duke John Frederick of Hanover in March of 1673 bore witness to his awareness of the utility of encypherment in official correspondence.[47] Moreover, when Leibniz corresponded with the Hanoverian chancery secretary (*Kanzleisekretär*) Friedrich Wilhelm Leidenfrost, they regularly enciphered various names.[48] And he also sometimes employed a nomenclator code in sensitive scripts—especially in dealing with commercial and diplomatic matters—as well as issues relating to reunion of the churches.[49]

In Leibniz's plans for a comprehensive library, books on cryptology and related issues (steganography, codes, cyphers, etc.) always find a place.[50] And Leibniz appears to have shared this literature. One of his few explicit discussions of rules for cryptography, the "Praecepta artis deciphiratoriae" of ca. 1685[51] is substantially an extract from the *Mysterium artis sleganographiae* of L. H. Hiller (Ulm, 1682), where only monoalphabetic cyphers were considered.

Two episodes show clearly that Leibniz had little interest in secret communication as such. The one relates to steganography, the other to anagrams.

Steganography is the procedure of hiding secret messages in open texts by such devices, say, as lettering only every fourth word of the text count as part of the concealed message or using punctuation to signal the words that count (e.g. second after a period, third after a comma). With Leibniz this topic is inseparably connected with Johann Sebastian Haes (also Haas), librarian at the ducal library in Hesse-Kassel, a versatile scholar and an assiduous Leibniz correspondent during the 1690s. Haes wrote a book on steganography[52] a notice of which he sent to Leibniz in January 1692 in the hope that he would pass it on to Duke Ernest August.[53]

In a rather perfunctory manner, Leibniz conceded that steganography may indeed have some use.[54] But Haes does not let the matter rest. He exalts the merits of stenography,[55] and pleads with Leibniz to recommend his book to Count Platen,[56] the Hanoverian prime minister, as providing for more efficient cryptography than the established procedures. (Throughout early 1693 Haes became almost frantic about this issue.[57]) Leibniz clearly takes little interest in the matter, although he describes Haes to Platen as "son intention est belle et utile, sur tout aux grands seigneurs."[58] Haes ultimately became rather distraught about there being no reaction from Platen.[59]

As regards anagrams, Newton had famously projected one to stake his claim to his discovery of fluxions in the face of keeping its processes secret. And others too resorted to this practice.[60] Leibniz's correspondent, the eminent Dutch mathematician Christian Huygens (1629-95) publicized his solution to Bernoulli's suspended-chain (*catena*) problem by an anagram, exactly in the manner of Newton in relation to fluxions—and the fashion of the day. Huygens described this in detail to Leibniz who had also solved this problem,[61] but Leibniz disapproved of this secretive

proceeding.[62] But Huygens reiterated his view, insisting "je vous remontray la necessité du Chifre pour pouvoir connoitre ce qu'un chacun auroit trouvé au sujet du Problème de Mr. Bernoulli,"[63] and subsequently adding that Leibniz ought to give "vos inventions sous la couverture du chifre, comme je vous l'avois conseillé plus d'un fois."[64] But Leibniz marginally asks himself "pourqoi prendre cette peine inutilement" when publication is the natural pathway to priority.[65] Leibniz was no friend of mystery-mongering. As he saw it, the fruits of research should be available to the universal benefit of the republic of learning.

Leibniz's reaction to the issue of stenography and anagrams indicate that secret communication as such really had little interest for him. Cryptography, on the other hand, because of its clearly mathematical involvements, is something else again. Its theoretical interests, its relations to algebra, and its involvements in the *ars combinatoria* gave this topic an entirely different standing in the mind of Leibniz. And on occasion he put it to practical use as well.[66]

3. Leibniz's Wallis Project: 1697-1701

In the era of the War of the Spanish Succession all major European capitals had their Black Chambers where the needs of decipherment were amply provided for. All of these involved people of extraordinary talent. In England there was John Wallis (after Newton England's ablest and most creative mathematician), in Vienna there was Giuseppe Spedazzi[67] (who was also an able composer), and in Paris there was the great cryptographer Antoine Rossignol and his disciples.

As early as 1673 Leibniz had remarked that the "*de doctrina divinandi seu de hypothesibus . . . pars est doctrina de chiffris construendis solvendisque, quam vellem a Wallisio accurate tradi.*"[68] However, the latter 1680s witnessed renewed stimulus to Leibniz's interest in cryptography. In his (anonymous) review of Wallis's *Treatise of Algebra* (1685) in the June 1686 issue of the Acta Eruditorum of Leipzig, Leibniz noted the analogy between solving equations and deciphering cryptograms, and expresses a wish that Wallis should provide some example of his work in this area.[69] After Leibniz started corresponding with the man himself in early 1697[70], he reiterated this wish to Wallis[71] who responded that he has already sent come samples of his work to the *Acta Eruditorum*,[72] and

John Wallis (1616-1703)
© National Portrait Gallery, London / after Sir Godfrey Kneller, Bt, oil on canvas

went on to provide Leibniz with a copy of this material. When he saw Wallis' decipherment Leibniz was truly astounded, and in his subsequent correspondence with Wallis, Leibniz persisted with this quest for further details about this *summum specimen humanae penetrabilitatis*.[73]

Wallis' communication presented the decipherment of two encrypted French diplomatic communications. The ciphers were different but functioned similarly, the symbols in each being either single objects or groups of two or three, with some standing for letters of the alphabet and others encoding syllables or words. The encypherment was accordingly fairly complex through combining several distinct elements.

John Wallis (1616-1703)—"the father of British cryptography"[74]—had since 1649 been Savilian Professor of Geometry at Oxford where he con-

tinued until 1703. He was a scholar-mathematician of almost Leibnizian versatility and Leibniz's editor C. I. Gerhardt aptly termed him "the Nestor of English mathematicians."[75] He was an immensely gifted cryptographer whose services were deemed invaluable by every British administration from Oliver Cromwell to Queen Anne. He provided invaluable service to the crown (i.e., William III) in deciphering communications captured from French and Jacobiate forces in Ireland.[76] His splendid portrait by Sir Godfrey Kneller commissioned by Samuel Pepys now in the Examination Schools in Oxford speaks volumes. In the background here lies volume three of his *Opera mathematica* which contained the decipherment of those two 1689 diplomatic dispatches. The material deciphered by Wallis revealed the hostile intentions of "a treaty (or intreaty rather) of the French King [Louis XIV] with the King of Poland presently to make war on Prussia."[77] This achievement was rewarded by the elector (later king) Friederick III of Prussia by a handsome sum as well as the gold medal and chain which rests on that book in the Oxford portrait. A knowledge of the arcana of the cryptographic art clearly brought significant rewards. (And where remuneration was concerned Wallis was no less eagerly importunate than Leibniz.)

Wallis had been in Leibniz's thoughts for a long time. Already in his Mainz period, Leibniz had heard of Wallis and his cryptographic achievements,[78] and in his 1673 *De methodi quadraturarum usu in seriebus* Leibniz drew the analogy between the search for a rule in a series or tabulation with the search for the key to a cipher.

Perusal of Wallis' 1996 communication had a powerful impact upon Leibniz. He was impressed, indeed virtually awed—*presque étonné*—by Wallis' cryptographic achievements, deeming them amazing (*merveilleuse*)[79] and vaunting his skill as "virtually unequalled."[80] An extensive correspondence soon unfolded between them.[81] Leibniz had not just respect but admiration for Wallis's work in code-breaking, and valued it as rivaling and indeed exceeding the best that that cryptographic adepts of contemporary France were able to produce.[82]

What intrigued Leibniz especially was that while Wallis published some of his decipherments, he never disclosed his *method* for obtaining them.[83] And Leibniz was convinced that Wallis was only revealing the top of the iceberg in his published accounts, and that a great deal of additional information would actually be required as basis for decipherment.[84]

This reaction engendered what one might call "Leibniz's Wallis Project."[85] For throughout the years from 1697 to 1701 Leibniz again and again told his correspondents—above all those who might themselves have contact with this genius—that *Wallis must be persuaded to ensure the perpetuation of his cryptographic knowledge*. So in October 1690 Leibniz urged Henri Justel in London that Wallis should be persuaded to publish something on the *art de dechifrer*.[86] And in a letter to Halley in June 1692 Leibniz urges that Wallis should not allow his cryptographic insights to die with him.[87] Similar plaints went to various of Leibniz's English contacts.[88] And in a long letter to Thomas Burnett of February 1697, Leibniz urges that Wallis should be induced to write about the codebreaker's *art de dechiffrer* "in which he achieved amazing success already in his youth."[89] Moreover, he sent the same message to any Englishman in touch with Wallis, telling Alexander Cunningham "Je souhaiterois que M. Wallis nous voulut donner les lumieres qu'il a sur l'art de dechifrer,"[90] also telling Thomas Smith that "*Vellem vir egregius aliquid nobis daret de Arte solvendi aenigmata cryptographica, in qua vix quenquam parem sese habere ostendit.*"[91]

In a letter of 11 January 1697 Wallis sent to Leibniz his deciperment of an encoded French diplomatic dispatch together with his key.[92] But Leibniz was disappointed. For as he wrote to Otto Menke, the editor of the Leipzig *Acta*:

> Es wäre zu wündschen dass H. Wallasius nicht nur solutionem Epistolae cryptographicae, sondern auch modus solviendi geben hätte. Ich glaube aber dass er aus diesen einizigen brief clavem also wie er sie hier gegeben nicht finden können.[93]

And Leibniz reiterated this wish to Wallis himself, flatteringly describing his cryptographic work as *fastigium quoddam subtilitatis simul industriaeque humanae*.[94]

In the period between early 1697 and early 1701 there were ten exchanges of letters between Wallis and Leibniz. From the very start of this correspondence and recurring in all but two of Leibniz's contributions to the prolonged exchange (namely his letters of 4 August 1699, [No. XIV in Gerhardt's numbering] and of Spring 1700 [No. XVIII]), there is a stubbornly repeated request to the effect: "Seeing that you are now past 80 years old, do please take on an apprentice in cryptography so that your

methods will not be lost to posterity"[95] Moreover, Leibniz explicitly tells Wallis of his eager curiosity about his amazing (*mirifica*) skill.[96]

Immediately after the correspondence had been begun by Wallis in late 1696, Leibniz in his very first letter opens this campaign for a clever young man to become Wallis's[97] cryptographic apprentice. Commenting on Wallis' 1686 paper he continues: *His ego nunc meas preces adderem, nisi gravis aetas tua obstaret . . . Si qui tamen adessent Tibi juvenes ingeniosi et discendi cupidi, possent coram paucis verbis a Te multa discere, quae interesset non perire*.

Contact with Wallis and his work profoundly changed Leibniz's views of cryptography. Initially Leibniz was hopeful that rules of practice (*regulae*) could take one far in developing the *ars deciphratoria*.[98] Initially—at least up to 1674—Leibniz had hopes that decipherment could be widely achieved by methodical rules of procedure.[99] For Wallis carefully explained that cryptography is not subject to definite rules (*certis regulis*) but is a matter of ad hoc contrivances whose complexity is ever in the increase.[100] Codebreaking, so Wallis insists, is rather a rambling hunt (*vaga venatio*) than a method.[101] As Wallis saw is, there can be no general rules in cryptography because "every new Cypher almost being contrived in a new way, which doth not admit it any constant Method for the finding out of it."[102]

Reluctantly, Leibniz conceded that cryptanalysis cannot be practiced by following rules specific instructions (*praeceptis*),[103] an acknowledgement which evokes from Wallis a stress on the very special dispositions and skills that the craft requires.[104] In the end, Leibniz could not but admit Wallis' protestations that the cryptographic art consists in special devices that admit no general rules.[105] While it was a fundamental conviction with Leibniz that *ars* had to be founded in *scientia* and *praxis* based on the teachings of *theoria*, Wallis led him to the reluctant realization that cryptography might be an exception to the rule.

Initially in his 1686 review of Wallis' *Algebra* Leibniz spoke of cryptography itself as a *scientia* rather than as an *ars*. But corresponding with Wallis seems to have made him increasingly unsure of this. And he eventually conceded that *Cryptographematum solutionem certa methodo absolvi non posse*.[106]

Leibniz was, however, rightly convinced that the cryptographic art could certainly be taught by example.[107] (It was, in fact, though just such apprenticeship that the craft was actually transmitted by its mas-

ter-practitioners to their own sons or relations at the courts of Europe throughout the 17th century.)

As Leibniz saw it, a decipherer must be (1) clever (ingenious and equipped with natural sagacity—especially in mathematics) and (2) patiently hardworking (*sedentarius and porté à l'assiduité*) with *patientia laboris*.[108] But in due course he also added (3) being generally knowledgeable and erudite.[109] For example, in seeking the key to a cryptogram that is based on a key word substantive information regarding the context may well prove useful.[110] For in decipherment as in hermeneutics, knowledge of contextual information may prove critical as a guide to probability.[111]

To keep Leibniz at bay Wallis sent him a copy of his *Acta Eruditorum* paper.[112] But in the face of Leibniz's dogged persistence, he ultimately yielded some ground to Leibniz's insistence that it might be a good idea for him to take on an apprentice. But he stressed that—given that encryption is usually only used "in matters of great moment"—he could not proceed without royal approval (*inconsultis nostro principe*) seeing that "it could much inaccomodate our friends no less than our enemies if the art of revealing secret writing were widely known."[113] At last Leibniz became satisfied that he has at last made real progress.[114] After all, how could an intelligent monarch fail to foster so important an instrument of human knowledge? Leibniz's last surviving letter to Wallis closes with the plea that he should *tanto ingenii humani specimine ars inveniendi provehetur*.[115] But how was this venture to be funded?

Leibniz's hope of funding an apprentice cryptographer for Wallis found extensive and persistent expression in his correspondence with Ferdinand the hereditary prince of Tuscany.

During his Italian sojourn in 1698-90 Leibniz was put in touch with Prince Ferdinand de Medici of Tuscany (who later came to the throne as Ferdinand III), and impressed with the solution of a mathematical problem-challenge.[116] Leibniz deemed this mathematically interested prince as the ideal sponsor for a Wallis disciple. In a letter of November 1698 Leibniz mentioned a certain prodigy in mnemonics and then continued: "I know of someone—[viz. Wallis]—with amazing skill at deciphering, so skilled that I myself am awed at what I have seen him do."[117] He urged the prince to fund a young apprentice for each of these prodigies and offers to supply candidates, urging haste on account of Wallis' great age impressing upon Ferdinand the importance of cryptography.

In his response, Ferdinand suggests that he himself knows a young man capable of developing both skills—mnemonics and cryptology.[118] Replying in January of 1699 Leibniz urged the claims of his own candidate for the mnemonics post and indicates that the cost would come to at least 400 Roman scudi per year with even a single year able to produce good results.[119] The prince responded in February of 1699 by wishing Leibniz good luck with the project.[120] Leibniz still did not let the matter rest but returned to it again in relation to his demarche on Wallis who, regrettably, *n'a pas encore pu se resoudre à ce qui est desiré*.[121] Finally in his response of June 1700 the prince dryly encouraged Leibniz to pursue his own effort in this direction.[122]

Despairing of further progress in this Italian direction Leibniz turned elsewhere, suggesting in February 1699 to Paul von Fuchs, the versatile minister of state in Brandenburg that the elector there should fund a disciple for Wallis,[123] and observing that France had been well served by employing cet admirable dechifrateur, the notable algebraist François Viète.

To identify a suitable candidate for his projected Wallis apprentice, Leibniz wrote in March of 1699 to the polydidact Johann Andreas Schmidt (ca. 1660-1726)—whom he had supported for appointment as professor of theology at the University of Helmstedt—asking him to recommend a suitable young scholar and describing the needed qualification of combining nature sagacity with practice.[124] In his reply Schmidt suggested an otherwise unidentified young man in Jena.[125] And in December 1698 Leibniz pressed M. G. Block for particulars regarding a young Swedish calculating prodigy, unquestionably with a view to his Wallis project. [126]

Nor did Leibniz neglect possibilities closer to home. In March of 1699 Leibniz prepared a memorandum for the periodic joint-session of the privy councilors of Hanover and Celle[127] in which he urged his ongoing plan for finding a young apprentice for Wallis. He wrote:

> The most celebrated decipherer now living in Europe, is found in England. He is a superb mathematician and stands in correspondence with me. Since he is now a man of eighty years it is of concern that the great things he had achieved in this art will be lost with him. I have often remonstrated with him for the public good that he finally be prepared to instruct in some

> suitable young man who is gifted with a similar inclination to calculation and effort.[128]

In his proposal Leibniz claimed (with questionable accuracy) that in the end Wallis agreed with his suggestion.

Finally, Leibniz seems to have found his man. In April of 1699 he wrote a long and elaborately detailed letter to the celebrated philologist Johann Gabreil von Sparwenfeld (d. 1627), Master of Ceremonies at the court of Charles XI of Sweden, detailing at considerable length his project of a Wallis-disciple.[129] He raises the problem of funding the project and mentions a Mons. Block for the job, describing him as "un honneste homme, et qui merite d'estre favorisé." But just to play safe, he continued: "Je vous supplie au reste du vous souvenir du garçon Finnois parent de M. Brenner et de ce garçon qui peut faire des grands chifres dans sa teste." Leibniz evidently nursed hopes that the court of Sweden might take up the good cause with financial support. He characterized the *art de dechifrer* as "un des plus grands echantillons de l'esprit humain," and he describes his friend Wallis as "asseurement des premiers en Europe pour cela" whose achievements "m'ont causé de l'étonnement." Having repeatedly asked him to publish his methods only to have him counter that "il n'y a point de règles generales dans cet art," has urged that he should take an apprentice to learn by example what cannot be transmitted by discourse. Leibniz then elaborated his plea that some great prince should fund such an apprentice in the interests of "le bien public, et particulierement sur l'avancement des sciences." In his reply Sparwenfeld informed Leibniz that he is unable to suggest someone suitable for apprenticeship in cryptography, a subject "dont vous parlez si juste et si bien."[130]

In fact Leibniz had already had substantial epistolary dealings with M. G. Block, some even touching on cryptology. In July of 1698 Block had written a long letter to Leibniz with much autobiographical detail in which he states that the late Baron R. C. von Bodenhausen has entrusted to his executors some papers with "observations, proces et curiosités de le nature, de la Medicine, de la chymie, etc." of which "la plus grande partie dont il estoit jaloux est ecrite avec un chifre d'une telle façon, qu'il semble presqu'impossible de la dechifrer."[131] Bodenhausen had entrusted the cipher to Block whose own opinion of this material was low. However, Leibniz made efforts to get hold of it as well as further Bodenhausen

papers.[132] Earlier on, in his own correspondence with Bodenhausen, Leibniz had repeatedly recommended using his favorite LABYRINTHUS cipher.[133]

But as regards Block also Leibniz did not put all his eggs in one basket. In July 1700 Alphonse des Vignoles (1649-1744), destined to be Leibniz's successor as director of the mathematical section of the Berlin Academy, wrote to him in response to a query about potential cryptologists that he has met "un Avocat de Berlin nommé M. Bauermeister qui est fils d'un Conseiller de Bernbourg" who possesses some knowledge of deciphering.[134] Moreover, he also knows of another promising young man called Cibrovius who is reported as having *une disposition admirable pour dechifrer*.[135] Gradually Leibniz accumulated some possibilities.

It appears from this proliferation of contacts that Leibniz simply did not care who—be it Hanover-Celle, Tuscany, Brandenburg, Sweden—should supply or fund the Wallis apprentice as long as this was done before Wallis' remarkable skills became lost upon his death. Only when it was clear that this unhappy event was imminent did Leibniz give up on his project. (See Display 1.) Seemingly, the secret cipher that Leibniz wanted most urgently to decrypt was that of Wallis's *cryptological modus operandi*. Wallis himself, however, was not receptive, insisting that the diffusion of cryptographic knowledge would do more harm than good: "*Nostris utique Amicis non minus quam Inimicis magno fore posset incommodo, si Ars, occulte scripta recludendi, passim innosceret.*"[136]

4. The Aftermath

Leibniz's Wallis project was not entirely in vain. David Kahn summarized the situation as follows:

> [Worried] that Wallis and the art might die together, [Leibniz] pressed his request that he instruct some younger people in it. Wallis finally had to say bluntly that he would be glad to serve the elector [of Hanover] in this way if need be but he could not share his skill abroad without the king's leave. The shrewd old cryptanalyst, who was frequently asking for more money for his solutions, then used Leibniz's arguments to his own advantage in successfully urging the secretaries of state to pay for his tutoring

Display 1

The Chronology of Leibniz's Wallis Project

- 1690-1696. Leibniz tells various correspondents that Wallis should be urged to write more about the *art de dechiffrer*.
- March 1697. Leibniz first recommends Wallis himself to take on an apprentice in the ars decriphrendi.
- November 1698. Leibniz begins urging Ferdinand of Tuscany to fund a Wallis apprentice. (A I 16, p. 576.)
- December 1698. Leibniz asks M. G. Block for details regarding a young Swedish calculating prodigy. (A III 7, p. 969.)
- February 1699. Leibniz urges von Fuchs, Privy Councillor in Berlin, to secure Brandenburg funding for a Wallis apprentice. (A I 16, pp. 577-78.)
- March 1699. Leibniz urges the Celle-Hanover Hauskonferenz to fund a Wallis apprentice. (A I/6, p. 121) He later reiterates this plan to Count Platen, the prime minister.
- March 1699–August 1700. Leibniz asks J. A. Schmidt of Helmstedt/Marienthal to recommend a suitable prospect as cryptographic apprentice, and elicits the nephew of former Professor Hoffmann of Jena. (A I 16, pp. 639, 656, 662.)
- April 1699. Leibniz explores funding for Wallis's disciple with von Sparvenfeld in Stockholm, and suggests to him that he has a promising prospect in view, viz. M. G. Block. (A I 6, p. 727.)
- March 1700. Wallis seemingly yields to Leibniz's repeated urgings to take on an apprentice, provided that William III is agreeable. (GMath. IV, p. 76.)
- July 1700. Alphonse des Vignoles writes from Berlin that he can suggest two plausible candidates for the Wallis apprenticeship. (G. C. Bauermeister and C. L. Cibrovius).

> of his grandson [William Blencowe] in cryptanalysis. They agreed in 1699, but it was not until Wallis wrote the king in 1701, saying that the young man had made such good progress that he had solved one of the best English ciphers and a very good French one, that they were both officially appointed as Deciphers and jointly granted £200 a year, retroactive to 1699.[137]

The fact of it is that Leibniz's importunities provided Wallis with ammunition for his own agenda. He took care in 1700 to declare his "having been solicited by Mijn Heer Leibnitz, more than once, on behalf of the Elector of Hanover."[138] In 1702 Wallis' ill-fated grandson William Blencowe (1683-1712)—then a youth of nineteen—succeeded his grandfather in the service of William III and he became the first Englishman bearing the official designation of "Decipherer."[139] For a time he headed the London's "black chamber" operation which later, after George I's accession, was later greatly strengthened by the accession of Hanoverian talent and methods. Various Hanoverian cryptologists "who had gained their experience during the War of the Spanish Succession" eventually figured importantly in Britain's Secret Office.[140] This included Johann ("John") Lampe who entered the service in 1724, and was appointed official Decipherer in 1729.[141] J. E. Bode who came in 1732,[142] and also Philip Heinrich ("Henry") Zollman (d. 1748), appointed ca. 1732 and designated Translator of German Language in 1735.[143] The sons of Ludwig Ernst Neubourg were especially prominent, Philip F. Neubourg becoming Decipher in 1750 and George W. in 1753.[144](After the accession of George I, cryptographic operations also continued in Hanover, often in cooperation with London.[145])

During the time of Hanover's tie to Britain under the four Georges there was a close partnership between the cryptographers of the two states.[146] And in fact throughout its history, British cryptography has worked in close cooperation with that of other nations: Holland in the reign of William III, Hanover in the reign of the Georges, and the U.S.A. in the reign of Elizabeth II.

The foremost 17th century cryptologists tended to keep the secrets of their art *en famille* by training up sons or close relations. This was true not only of Wallis in England, but also with Rossignol in France's service and the elder Neubourg in that of the Hanoverians. This sort of

development was not, however, something that Leibniz had intended nor indeed something which, given the rigorous secrecy involved, he would have welcomed.

How are we to explain Leibniz's Wallis project with its intensive dedication to finding a young scholar to be trained up in cryptology by Wallis? Two possible explanations come to mind:

1. The idea proposed by Wallis and generally echoed since that Leibniz here acted to secure an asset for Hanover.[147]

2. The idea that Leibniz was being candid in his repeatedly stressed contention that he was acting in the interests of fostering an important branch of human knowledge.

The fact that Leibniz proceeded in so many different directions—not just Hanover but Tuscany, Sweden, Brandenburg, and Britain—speaks strongly for the second of these.

To be sure, Wallis himself, and most everyone since, has thought that Leibniz sought the Wallis apprenticeship in the interests of the Elector Hanover.[148] But this does injustice to Leibniz's cosmopolitarianism. We can take his own declarations at face value: he looked to the benefit of the republic of learning. In commenting on the resumptions of the work of the French Academy after the Peace of Ryswick, Leibniz wrote:

> Provided that something of consequence is achieved, I am indifferent whether this is done in Germany or in France. For I seek the good of mankind. I am neither a phil-Hellene nor a philo-Roman, but a philanthoropos.[149]

No episodes in Leibniz's life more clearly attests to the truth of this claim than his Wallis project. Leibniz viewed decipherment as a resource of human understanding rather than a tool of espionage and regarded its development as an exercise in human ingenuity rather than as an instrumentality of state power. As he saw it, the art that mirrored at the level of human artifice the work of natural science in its mission "to decipher the secrets of nature" is then-current parlance. Whether that young Wallis-trained cryptanalyst was Italian or French, German, Italian, or English, Dutch or Swedish was indifferent to Leibniz. What mattered was that a significant sort of knowledge be preserved for mankind. As Beeley has

justly put it: "Leibniz promised himself greater insight into his projected ars inveniendi through the analytical methods applied by Wallis."[150] His invocation on the benefit of mankind here was perfectly genuine. As the editors of A III 7 have rightly observed (p. LXVI) Leibniz's paramount aim was "Die Förderung der *ars inveniendi,*" because he viewed cryptology as "f*astigium quoddam subtilitatis simul industriae humanae*" (ibid., Nr. 146) and a "*summa specimen humanae penetrationis*" (ibid, Nr. 184). It was this indifference to local loyalties which rendered Leibniz—whose foreign correspondence was doubtless monitored by the postal censors along with the rest—suspicious in the eyes of Hanoverian officialdom.[151]

Leibniz was genuinely impressed—and somewhat puzzled—by Wallis' cryptological achievements. For Leibniz was a dedicated theorist who could not quite believe that there were no clear-cut cryptological methods, rules and devices—formalized processes by which decipherment could be achieved. But he eventually came to sense that the advantage Wallis had over him was not one of the theoretical competency in mathematics but one of applied practical *exercitum*, and would doubtless have liked to give a clearer insight into the hidden arcana of the enterprise. And something else also came to view.

Early on, Leibniz believed that his formalized scientia universalis is such that "*hac arte ea tantum (convenienti studio athibeto) posse obteneri quaecunque ex datis quantocunque ingenio possint elici.*"[152] But Wallis' work convinced him that an ingenuity transcending mere application and procedural diligence would sometimes be required.

The written record leaves little doubt that it was rather a mixture of personal curiosity and impersonal concern for the interests of learning for its own sake rather than any desire for Hanoverian benefit that led Leibniz to importune Wallis with regard to cryptology. But if it had been Leibniz's ambition to secure the cryptographic knowledge of Wallis for the benefit of the house of Brunswick (which assuredly it was not!) this nevertheless came to be realized in an ironic variation. For even as Leibniz was searching for a prospective Wallis apprentice, young adepts in the *ars cryptographica* were already coming into place, including not just Wallis' own grandson, but also the trainees of Zachariae, the founding father of Hanoverian cryptography. It is just that their cryptographic contributions were not destined for the advantage of the republic of letters and learning, but rather for unveiling the dark secrets of diplomatic and political

statecraft. And these developments did indeed ultimately redound to the benefit of the House of Brunswick—albeit in London rather than Hanover.

Leibniz's interest in fostering cryptography never abated—even in his 70s. When he learned that the young son of his friend Theobald Schöttel, the Imperial Kammertürhüter had solved a magic cube problem, he expressed his admiration and added: "Er wuerde derowegen auch vortreflich in der Deciphrir-Kunst zu rechte kommen, und möchte ich also wundschen dass er sich darinn von H. Spedazzi, und in die Algebra und Geometri von H. Marinoni unterweisen liesse, so würde er es zu wunderdingen bringen können." [153]

5. Leibniz as Cryptographer

To what extent was Leibniz himself involved in cryptographic practice? As best we can tell on the presently available evidence—very little. In correspondence with Baron Boineburg during Leibniz's Mainz service they standardly enciphered various names and brief expressions.[154] And in his letters to Leibniz on matters of international politics, Boineburg's secretary Jakob Münch enciphers several proper names and short expressions.[155] And in Leibniz's long 1674 letter to Johann Linker, counselor in electorate of Trier, giving a *tour d'horizon* of European political affairs, various names and brief expressions are enciphered.[156] As best we can tell, in exchanges with him Leibniz here—and throughout his correspondence—used codes and ciphers only for names and brief phrases and never with continuous texts.[157]

Notwithstanding the importance he clearly attached to cryptology, there is throughout the vast range of the as-yet published Leibniz-correspondence little sign that he himself was later significantly engaged with actual encryption or decryption. Thus Otto Grote in corresponding with Leibniz during his (Grote's) 1692 mission in Vienna used a cipher for occasional words, this is an uncommon instance in Leibniz's vast political correspondence.[158] And yet another correspondence relates to Pierre de Falaiseau (1649-1726), a Huguenot exile in Berlin who initially served as a Brandenburg diplomat in several European capitals, but then settled in England. After 1702 he became Leibniz's principal informant regarding English political affairs.[159] In a letter to the Elector Georg Louis, Leibniz described him *de la confiance des principeaux des whigs*.[160] Falaiseau's let-

ters to Leibniz were sent via Holland outside the postal system through the Dutch-Portuguese bankhouse of Mesquite. In a letter to Leibniz the Electress Sophia complains that the correspondence with Falaiseau had suffered some puzzling interruptions, its use of a cypher notwithstanding.[161] It is clear that despite the precautions taken by Falaiseau his correspondence with Leibniz and Sophia was far from secure.[162]

Leibniz's prime partner in coded correspondence was his longstanding friend and business partner Johann Daniel Crafft to whom Leibniz spoke of "unser Zipher Labyrinthus".[163] As of the start of their correspondence in 1672, Crafft proposed using the monoalphabetic cipher based on the key word LEIBNYZ, and he immediately put it to work by enciphering various names and brief expressions.[164] Later on he further suggested simplifying matters via the pairing

L E I B N Y Z A C D F G
H K M O P Q R S T U W X

With each letter being replaced by its paired opposite, thus rendering Gott mitt unds as xbcc imcc dpa.[165] But there were occasional encipherment errors, and Crafft sometimes complains that he "*verstehe es, wie jetzt, bissweilen gar nicht*".[166]

Another Leibnizian foray into encription occurs in relation to an anagram on the expulsion of the Turks from the Holy Roman Empire which was sent to him in 1688.[167] Here Leibniz employs a Latin verse as key for a numerical encipherment of texts.

1	2	3	4	5	6		7	8	9	10	11	12		13	14		15	16	17	18	19	20
T	U	R	C	A	S		E	U	R	O	P	A		D	I		V	U	L	S	O	S

21	22	23	24	25	26	27	28		29	30	31	32	33
O	P	P	R	I	M	E	T		A	R	M	I	S

This gives rise to the cipher:

A	B	C	D	E	F	G	H	I	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
5		4	13	7				14	17	26		10	11		3	6	1	2	15				
12				27				25		31		19	22		9	18	28	8					
29												21	23		24	20		16					
															30	33							

On this basis the other verse of the anagram obtains a numerical encipherment as per:

17	7	10	11	19	17	13	2	6		22	3	14	26	8	18
L	E	O	P	O	L	D	U	S		P	R	I	M	I	S

5	15	20	1	9	25	12	4	16	33		32	31	23	27	24	29	28	21	30
A	U	S	T	R	I	A	C	U	S		I	M	P	E	R	A	T	O	R

The use of multiple alternative encriptions of one selfsame letter affords a straightforward way of putting obstacles in the way of frequency analysis.

Early in 1697, Leibniz sent a long letter to Fr. Claudio Filippo Grimaldi in Peking,[168] to which he appended a postscript in which he suggested that in view of the prospect of interception during the long transit they might of confidentiality employ a simple monoalphabetic transposition cypher:

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

And now, as Leibniz said, *Pekin* would be rendered *uorfg*.[169] This LABYRINTHUS encipherment was long a favorite of Leibniz's and was often used in his. For not only does he recommend it here, but also he had used it previously in confidential communication.[170] It is—as Leibniz certainly realized—an extremely elementary device, though one that would presumably be adequate for the needs of the occasion.[171] All the same, it is striking how rarely Leibniz himself actually used excypherment after the early time of its mandatory use in correspondence with Baron Boineburg and his associates. (The immense Leibniz Nachlass—consisting of some 60,000 items of roughly 200,000 pages—affords little more than the few items discussed in this essay.)

To all visible appearances, Leibniz had no exposure to the sophisticated cryptographic practice of the "black chambers" of his day—not even in his immediate Hanoverian proximity. His surviving discussions of the subject "move solely in the sphere of mono- and polyalphabetic cypher and contain nothing that could not have been gathered from countless publications in deciphering which had appeared since the Renaissance."[172]

Herbert Breger is correct here when he writes that "Mir ist kein Brief

aus der [enormen] Leibniz-Korrespondenz bekannt, der mit einem Code auf dem in der zeitgenössischen Diplomatie üblichen Schwierigkeitsnivean verschlüsselt wäre."[173] The materials of LH V VI 4 do seem to afford an instance when Leibniz encountered such a code—and it apparently defeated him.[174]

It seems clear that Leibniz—unlike Wallis—was someone whose interest in cryptography was entirely theoretical, and exactly this may well be why he deemed Wallis's work in this arena as something of special importance and value. To be sure, Leibniz did offer various insightful observations on general principles. In particular, he emphasized that just as in algebra a set of equations can be undeterminate, just-sufficient, or over-determinative of the situation so a set of encrypted texts can underdetermine, determine, and over-determine the key needed for a solution.[175]

All the same, As David Kahn has commented

> The authors [of the early works on cryptology] borrowed their knowledge from earlier volumes and puffed it out with their own hypothesizing, which seems never to have been deflated by contact with the bruising actuality of solving cryptograms that they themselves had not made up. The literature of cryptology was all theory and no practice. The authors did not know the real cryptology that was being practiced in locked rooms here and there throughout Europe by uncommunicative men working stealthily to further the grand designs of state.[176]

In substantial degree this stricture applies to Leibniz as well. After all, actual cryptanalysis is enormously time consuming, and time is something which Leibniz did not have all that much amidst his innumerable enterprises and activities. Nor was Leibniz blind in his own limitations and exaggerate his competency in the field. Thus Leibniz says that while he has some promising ideas about cryptography he cannot claim much practical experience in the area: "So habe ich noch einige hofnung dass wiewohl ich in dieser materi mir [nicht] gross exercitium anmassen kann…)"[177] While Leibniz always espoused the idea of a combining theoria cum praxis, in the present case the limitations of time and circumstance imposed upon him a restriction to the former realm alone.

But just this, it would seem, is what impressed and intrigued Leibniz about Wallis and the seeming magic that enabled him to fit bril-

liant cryptanalytic work into a demanding career of writing, research, and administration.

6. Brunswick Cryptanalysis

Leibniz himself was not a practicing cryptanalyst but he actually was surrounded by people who were. To begin with there was, as we have seen, Wallis himself. Moreover, when Leibniz was on final visit in Vienna during 1712-14 he was in regular touch with the abbot Giuseppe Spedazzi, the polymath musician who was a senior official at the imperial court in Vienna and was the prime codebreaker there. (It was he who informed Leibniz that he could not head the projected imperial academy of sciences without becoming Catholic.) Leibniz corresponded with Spedazzi between May of 1713 and November of 1716 and took a supportive interest in him and his work.[178] As late as 1716, in writing to Imperial chamberlain Theobald Schöttel, Leibniz regrets that Schöttel's son did not avail himself of contacts with Abbé Spedazzi to obtain some instruction in cryptography.[179] Clearly, an interest in these matters prevailed to the end of his days, although in the main their correspondence was focused in the creation of a national bank in Vienna as well as the founding of the Imperial Academy of Sciences.

But even far closer to home there was a flourishing cryptographic industry. The Hanoverians ran an elaborate and efficient cryptographic service in which the Brunswick dukedoms of Callenberg and Celle functioned as one. Several postal interception stations were in operation. That at Nienburg intercepted post between France and the Nordic countries. That at Gifhorn processed north-south post between Wolffenbüttel and Braunschweig on the one side and Hamburg and the north on the other. The Thurn and Taxis station at Sulingen also provided material. Mail was screened for items of interest and these were expertly opened, copied, and resealed. Coded material was given for decryption to Johann Albrecht Zachariae or his pupils Ludwig Ernst Neubourg¸ and Johann Philipp Schlemm, all among Europe's ablest and most experienced codebreakers.[180] Johann Albrecht Zachariae (ca. 1630-1701) was the s*ecrétaire des depeches* to the Hanoverian Cabinet and the War Office (*Kammer-und Kriegsrat*) which he ultimately headed.[181] A master decipherer, he taught the cryptographic art to his son-in-law, Johann Philip Schlemm (1672-

1733) who succeeded him as Confidential Secretary to the Cabinet in 1701,[182] and he also taught the chancery official Buetemeister[183] as well as Ludwig Ernest Neubourg (d. 1713) who later became Hanover-Celle's principal cryptologist.[184]

Leibniz had some routine official correspondence with Zachariae dealing with mere postal payments early on and later with rather a perfunctory exchange of news items during Leibniz's Italian journey during 1689-90.[185] They never touched even remotely on matters of cryptography. And Leibniz had some dealings with Schlemm and was at odds with him over his (Leibniz's) use of the ducal post for personal communications.[186] In an intriguing account of "The Black Chamber in the Dutch Republic during the War of the Spanish Succession and its Aftermath, 1707-1715"[187] Karl de Leeuw writes:

> It is astonishing that these small principalities produced a band of codebreakers of their own precisely at the moment when it was needed. The explanation might be found in the presence of Wilhelm Leibniz who combined, just like Wallis, a strong analytical mind with an interest in language and grammar in particular. Leibniz does not consider himself to be a great codebreaker but he might have helped to develop an analytical framework for people who were more gifted as cryptanalsists than he was himself.

This explanatory conjecture is very questionable, and something rather different seems to be at work. The conspiratorial atmosphere the Reformation struggles and the internecine strife of the 30 Years War produced a seed-bed for secret communication. And in the Brunswick orbit the influence of duke Augustus II, "August the Younger" (1579-1666)—Duke of Brunswick-Lüneburg and near relation of King George I—was almost certainly critical in establishing the effective Black Chamber of Duke George William of Brunswick-Lüneburg in Celle. The duke was not only interested in cryptography but himself contributed to its development in his *Cryptomenytices et Cryptographiae libri IX in quibus a planissima Steganographiae a Johanne Trithemio...enodatior tradita* (Lüneburg, 1624), published under the pseudonym "Gustavus Selenus".[188] This treatise contains some cipher systems and supported the use of Trithemius' alphabetic tabulation.[189] It was likely in the wake of George William's influence that Johann Albrecht Zachariae was drawn into the secret arcana of this craft.[190]

There is no sign that Leibniz had any correspondence with Bütemeister or with Ludwig Ernst Neubourg, the cryptographic experts of the chancery of Celle and later Hanover.[191] Their excellent work was much appreciated by those who knew of it. In a letter after Neubourg's death, the electress Sophia said he was regarded as "one of the wonders of the century."[192] The house of Brunswick ran a world-class cryptographic operation and was willing to pay for it.

The joint house-conference of senior Celle and Hanoverian officials of 28 September 1701 established a bonus for those decipherers who provided a key (*clavis*) to a new code. It consisted of 24 taler in Hanover and 30 in Celle.[193] Somewhat to the dismay of Hanoverian officialdom, Neubourg, their prize cryptanalyst, also received from 1707 to 1711 an annual gratuity of 100 guilders from Holland.[194]

At home as well as later on in Britain, all the reigning Brunswick-Lüneburg princes took a strong personal interest in the products yielded by their work of their cryptanalysists.[195] When George Louis became king George in London some of the major Hanoverian cryptanalysts followed in his wake, in particular Bode, Lampe, Zollmann, and Neubourg, and their work in the Secret Branch yielded him and his successor a substantial output of great value.[196] The government now took full advantage of the Post Office Act of 1711 which authorized the interception of mail. What was generally called "The Secret Office," adjoining the Foreign Office at the Controller's house, had no official existence. Its head, aptly called "the Secret Man," was employed in the Post Office under the direction of the Secretary of State with a salary of £200 a year, doubled in 1702 and paid by the Post Office Secretary. The entire operation was strictly secret "for reasons where it would be superflous to mention," and included openers, decipherers, and translators—an entire "Secret Department," with an annual budget of around £2000. The early Georges took a close interest in the work.[197]

By and large, the Deciphering Branch of "the Secret Office" relied for its most demanding technical expertise on notable scholars who had other posts in the world of learning and provided this service on a "free lance" basis. These experts secured their material by special messengers from Whitehall and worked in the field under oath of secrecy. The Branch had no formal structure or chief: the official Decipherer was no more than *primus inter pares*.[198] Blencowe, Wallis's grandson, was the first of these.

7. Leibniz was "Out of the Loop"

In a letter to Count Platen, the Hanoverian prime minister Leibniz stated that despite the importance of the *ars cryptographica* he himself could not lay claim to significant practice (*exercitium*) in decipherment.[199] And it is clear that the Hanoverian administration was prepared to take him at his word here. For it appears that Leibniz himself was never asked to help with decipherment.[200] Nor is there any visible sign that he was aware of the scope and sophistication of Hanover-Celle's cryptographic efforts.

When Leibniz made his presentation to the March 1699 Hanover-Celle *Hauskonferenz*, the knowledgeable privy counselors must have been amused. They clearly had no incentive to fund a Wallis apprentice seeing that their own operatives were more than competent to provide fully for their requirements. Brunswick officialdom certainly did not need to be persuaded by Leibniz of the significance of cryptography. In fact as far as Hanover's official cryptographic efforts was concerned, Leibniz was almost entirely "out of the loop." Almost—but not quite entirely, for when the elder Neubourg died in April 1713, Leibniz—writing from Vienna—recommend as his successor Filippo Oduardo D'Ussol, a Piedmontese nobleman reputedly expert in decipherment, who did not get the post, which instead went to Schlemm.[201]

Leibniz's correspondence with the Zollmanns has interesting features. With the father Johann Ludwig, a privy councilor in Zeitz there was a cordial exchange between colleagues on matters of common interest, marked by a touching persistence on the elder Zollmann's part to enlist Leibniz's support in furthering the career interests of his son who eventually moved to London. The letters from the son to Leibniz are quite different—crisp, business-like, and focused on P. H. Zollmann's role as postal expediter. (For example, he handled the Leibniz-Clarke correspondence mediated by the Princess of Wales in London.) Later on there are also occasional brief bulletins regarding English affairs in which a Hanover-restricted Leibniz might be interested. But never is there any even remote hint of anything relating to interception and cryptanalysis.[202]

It seems clear that Leibniz had no real idea of the extent to which Hanover's administration intercepted and monitored postal communications, nor of the regularity and sophistication with which encrypted communications were subject to cryptographic analysis. Indeed, since he himself maintained an elaborate foreign correspondence and his loyalty to

Hanover vis-à-vis Berlin and Vienna was much under suspicion, it seems more than likely that Leibniz was on the receiving rather than producing side of Hanoverian efforts at postal surveillance.[203]

Georg Schnath has it that Leibniz "scheint nie oder nur ganz selten zur Entzifferung von verschlosslten Schriftstücken herangezogen worden zu sein."[204] As best one can tell, Schnath might have spared himself that *nur ganz selten*. But for Leibniz this was substantially a matter of indifference; his interest in cryptography lay in the theory of the matter, and not its actual practice.[205]

8. Leibniz's Cryptological Brainstorm

Late in the 15th century Johannes Trithemius (1462-1526), abbot of the monastery of Sponheim, introduced the idea of polyalphabetic encipherment with where each successive letter was encrypted by a different monoalphbetic transposition.[206] While such an encryption is quite difficult to break, it is also laborious to use, be it in encryption or decryption. In his early thirties Leibniz conceived of an ingenious way of addressing this problem.

Early in 1679 Leibniz sent to his master, Duke John Frederick of Hanover, one of his occasional long memoranda on achievements and projects. He here outlined the capacities of his calculating machine, and then continued as follows:

> Cette machine d'Arithmetique m'a fait songer à une autre belle machine qui serviroit à mettre les lettres en chiffres, et à les dechiffrer: et cela avec une tres grande promptitude et d'une façon indechiffrable aux autres. Car je remarque que la pluspart des chiffres dont on se sert communement sont aisés à déchifrer; et ceux qui sont difficiles à dechiffrer, ont coûtume d'estre difficiles à écrire, ce qui les fait abandonner par des personnes occupées. Mais par cette machine une letter entiere seroit presque aussi aisément mise en chifres et dechiffrée par celuy qui a la machine, que copiée.[207]

Nor was this a transitory whim. For in his memorandum of August/September 1688 for an audience with the Emperor Leopold I, Leibniz again reverted to this *machina deciphratoria*, affirming that it enables

the user "in underschiedenen ziphern gleich [zu] correspondieren."[208] The editors of the great Leibniz edition voice uncertainty as to whether Leibniz ever actually had the machine constructed.[209] However, in view of the secrecy in which he veiled this effort it is unlikely that he did so. In a memorandum for Leopold I, in discussing his mechanical inventions, Leibniz characterized as *inventa mea utilissima* and says that apart from his calculating machine and his chronometric devices, these have for the most part been kept secret because they might possibly be misused.[210] And he wrote:

> Two machines of mine remain to be discussed. However, I scarcely dare even to mention them because of their great significance. For they could bring about a revolutionary change (eine überaus grosse enderung) in military affairs, should they be known and used by one single power before beings discovered by others.[211]

It seems clear that Leibniz was not going to have this mechanism constructed unless and until some great prince showed an interest. He seems to have thought that the fewer who knew of this the better. His discussion of the *manchina deciphratoria* made it clear and explicitly that Leibniz intended his cipher machine only for *ein Potentat oder hohe Personen*. Accordingly, this apparatus was Leibniz's most closely guarded secret. Although he was often prepared to boast of his innovations and inventions yet this one was only mentioned in private memoranda preparatory for viva voce presentations to princes. And as a result of this secrecy, virtually all that we know about the *machina deciphratoria* came from Leibniz's pitch of it to the Emperor. It is, thus, questionable if the machine was ever actually constructed.[212]

As best we can tell this is a conceptual device that Leibniz never had produced. And while in some respects it resembled Leibniz's calculating machine—in particular by a carrying operation governed by the Leibnizian *Staffelwalze*—the stepped-drum mechanism that still called the "Leibniz-wheel," that was the crux of his calculator—with its decimal carrying feature readjusted to produce a shift to the next alphabetic slide (until an eventual return to the first).[213] Here, however, the apparatus was operated not by turning a dial but rather by pressing a key "just as with a clavicord."[214] (Shades of Enigma!) The machine itself functioned "aus gleichen principio wiewohl viel leichter" as the *machina arithmetica*. It

stepwise produced the encrypted text, which the user simply had to copy off. (No typewriters yet!) For details see Appendix 2. Used in mechanical calculating machines for over 200 years, the Staffelwalze is custom-made for cryptographic employment in a stepped Trimethian encypherment where letters are successively encoded in a different monoalphabetic cypher. But in any case the conception of a cryptographic machine is one which, like many other ingenious ideas, makes its first appearance in the fertile mind of Leibniz. Yet while it stayed there in his day, it might possibly have emerged but for a fortuitous concatenation of circumstances.

In early August of 1716 Leibniz's chief, King George I made his first return visit to Hanover, and then went on to Bad Pyrmont to take the cure, Leibniz travelled there from Hanover to meet with him on 4 August. On that very day Johann Ludwig Zollmann came to Hanover to visit Leibniz, followed the next day by his son, Philip Heinrich.[215] The younger Zollmann had been trained in Hanover's excellent black chamber, and upon following George Louis to Britain after his succession to the throne there, had entered the service of England's Secret Office and had become one of London's prime cryptographers.[216] The Zollmanns lodged in the same Schmiedestrasse house where Leibniz had been living since 1698, the prime object of their visit being to secure information about the latest, improved version of Leibniz's calculating machine.[217] A fortuitous mismatch of schedules destroyed the opportunity for informative interaction between Leibniz and the Zollmann regarding the potential of his great brainchild. It would thus seem that at least one contemporary was not blind to the potential use of Leibniz's arithmetical machine for cryptographical purposes. A recent writer holds that "cryptology has consummated its union with mathematics through the computer."[218] It appears that Leibniz was already a matchmaker here, although his death only a few weeks later terminated any prospect of a productive union.

It is clear in this connection that an intriguing historical opportunity was missed at this point. As things stand, Leibniz's cryptographic machine was his most closely guarded secret —to be revealed only to princes. But it is possible that at this late hour of his life he might have described it to Zollmann who would certainly have taken it back to London's black chamber. And what might have happened then stirs the imagination.

II

Leibniz's Machina Deciphratoria

(A Seventeenth Century Photo-Enigma)

1. Leibniz's Descriptions of his Cryptographic Machine

G. W. Leibniz (1646-1716) was the quintessential Renaissance man, a German Leonardo da Vinci, but with a difference. For instead of focusing on the plastic arts like Leonardo, Leibniz worked more abstractly—with mathematics. He invented the calculus, topology, determinants, binary arithmetic, symbolic logic, rational mechanics, and much else besides. But like Leonardo, Leibniz also constructed machines: wheels that ran on treads, windmills that worked by scoops, and an arithmetical machine that was—and still is—one of the wonders of the world of geared engineering. A great deal is known about Leibniz's amazing achievements, but there are still some surprises left.

Early in 1679 Leibniz sent his then master, John Frederick, the reigning duke of Hanover-Calenberg, one of his occasional long memoranda regarding his achievements and projects. After discussing his now-famous calculating machine,[219] he continued as follows:

> This arithmetical machine led me to conceive another beautiful machine that would serve to encipher and decipher letters, and do this with great swiftness and in a manner indecipherable by others. For I have observed that the most commonly used ciphers are easy to decipher, while those difficult to decipher are generally

> difficult to use, so that busy people abandon them. But with this machine of mine an entire letter is almost as easy to encipher and decipher for one who uses it as it is to copy it.[220]

This representation to Duke John Frederick of February 1679 is echoed in the draft of another memorandum of that October of that year, where Leibniz notes that "I am going to have intensive work done on the *machina arithmetica*" and after hopefully remarking that "I have no doubt that your serene highness will provide [financial] assistance for this" and then adjoins the marginal comment: "and the same applies to the cipher machine."[221] As far as Hanover is concerned, however, this is the last we hear of it. And throughout his vast correspondence, Leibniz never discussed this device. However, from early May of 1688 to early February of the following year, Leibniz paid a long visit to Vienna, and in late October 1688 he requested an audience with the Emperor Leopold I which was granted in early November, realizing a wish that Leibniz had entertained for decades.[222] Leibniz made extensive preparations for this audience, in which his cipher machine played a small but significant role in a way that dropped from sight completely until the publication of his preparatory memoranda in 2001 in the academy edition.

During August-September 1688 he prepared a detailed list of "talking points" to his presentation.[223] This was then recast into a form for oral presentation, and then developed into a detailed and polished version presumably to be left behind after the audience for study by the emperor's advisors.[224] In sum, Leibniz went to extraordinary lengths to prepare for a discussion which was intended to cover in great detail the entire range of his own accomplishments and sketched out a considerable series of projects for contributing to imperial interests, in the hope of securing the appointment (and salary) of an Imperial Councillor (Reichshofrath).

Everything that we know about the nature of the *machina deciphratoria* is derived from these princely memoranda, since, for the rest, Leibniz shielded his machine in deep quiescence. But in his notes for that audience with the emperor Leopold I in Vienna in August/September 1688 he wrote:

> Then too there is my *machina deciphratoria* with which a ruler can concurrently correspond with different ministers, and without much effort both writes in a cipher that he wishes to use and comprehend a letter sent to him in cipher. This is done much as

> with using a musical instrument or clavichord, so that the text appears by touching the piano keys and only needs to be copied.[225]

And in a short outline for his long memorandum Leibniz spoke of "My cryptographic machine, which places many ciphers at a ruler's disposal and resembles a clavichord."[226] Then in amplifying these notes into an elaborate memorandum, Leibniz, after discussing his calculating machine, wrote:

> On a similar principle, though far simpler [than my calculator], I have discovered a *machina deciphratoria* for use by great personages. It is a smallish mechanism (*machinula*) that is easy to transport. With it a great ruler (*ein grosser herr*) can concurrently use many virtually unsolvable ciphers and correspond with many ministers. While both encipherment and decipherment is [ordinarily] laborious, there is now a facility enabling one to get at the requisite ciphers or alphabetic-letters as easily as though one were playing on a clavichord or other [keyboard] instrument. The requisite letters will immediately emerge, and only need to be copied off.[227]

While Leopold I requested Leibniz to pursue some of his proposals, the *machina deciphratoria* was not among them. In view of the extraordinarily effective work of his own efficient black chamber in Vienna, Leopold was apparently not minded to spend money on its construction.[228]

Even the sparse indications of Leibniz's memoranda provide a wealth of information about his *machina deciphratoria*. Given this detail, and considering what is known about Leibniz's calculating machine—and also about his ideas regarding cryptography—a conjectural reconstruction of his cryptographic machine is readily possible.[229]

2. A Conceptual Reconstruction of Leibniz's Machina Deciphratoria

Late in the 15th century Johannes Trithemius (1462-1526), abbot of the monastery of Sponheim, introduced the idea of polyalphabetic encipherment where each successive letter was encrypted by a different monoalphabetic transposition.[230] While such an encryption is quite difficult to break, it is also laborious to use, be it in encryption or decryption. However, while still in his early thirties Leibniz conceived of an ingenious machine for addressing this problem.

Compared to Leibniz's calculating machine, his cryptographic machine is a very simple device. Its salient features are as follows. The machine is operated by a piano keys marked A, B, C etc. for the 22 letters of the *Latin* alphabet plus v and w. Inside there are two rotating drums running sideways above and in front of the keyboard. An activating drum is turned by the piano-keys to make a partial (60°) rotation with each key stroke. A second display drum has an outer (hexagonal) surface to which the output letters for encipherment and decipherment are affixed. This display roller is linked to the aforementioned activating drum via a stepped drum (Staffelwalze) in such a way that it makes one partial (60°) rotation with every *N* key-strokes.[231] This parameter *N* is adjustable via the Staffelwalze to have a pre-assigned value anywhere between 1 and 6 thereby fixing in a changeable way the number of keystrokes required to produce a 60° rotation of the display drum.

It is clear that this visualization encapsulates all of Leibniz's descriptive specifications for this machine. And such a device could readily be contained in a box sufficiently small to escape notice among the impedimenta of a travelling prince.

At the heart of his device thus lay the Leibnizian *Staffelwalze*—a stepped-drum mechanism that is still called the "Leibniz-wheel," that was also the crux of his calculator—with its decimal carrying feature readjusted to produce a shift to the next alphabetic slide (until an eventual return to the first). Used in mechanical calculating machines for over 200 years, the Staffelwalze is custom-made for cryptographic employment in a stepped Trithemian encypherment where letters are successively encoded in a different monoalphabetic cipher.

In the cipher machine the linear motion of depressing a key is transmuted into the circular motion which actuates the rotation of the Staffelwalze in such a way that with every *N*th keypress the output drum turns by 60° and the substitution alphabet is changed. This transmutes the substitution at issue into a polyalphabetic one, similar to the familiar Vigenère cipher but without the cryptographic weakness of its alphabetic regularity. The machine's salient advantage is that of automaticity—any laborious lookup of keys or ciphertext being averted.

In using the machine the operator inserts several (i.e., six) letter slats on the display drum, each containing a different permutation of the alphabet, onto the sides of a horizontal hexagonal rotating drum. In

front of each letter on the slat is a key, as on a harpsicord and when the key is struck the corresponding slat-latter becomes indicated. If only monoalphabetic encipherment were wanted, one would simply match the plaintext letter on the keyboard with the corresponding letter above it on the slat.

The operational components to Leibniz's cipher machine are thus two:

I. A hexagonal alphabet drum on which there are affixed six slats A[1] to A[6] each containing a scrambled alphabet chosen from a box containing various alternatives.

II. A "stepped drum" which determines whether or not that hexagonal alphabet drum will rotate (by 60°) to the next alphabet slat when a letter is keyed in.

To prepare the machine for action, the user must (1) affix six alphabet-scrambling slats to the hexagonal alphabet drum, and (2) insert a stepped drum into the device. Moreover, one of the drum's six rotation patterns must be selected.

The machine then functions as follows. When the first plaintext letter is keyed in, the resulting output encrypted is its monoalphabetic pairing mate from the selected starting alphabetic slat A[i]. Now in general, as a given plaintext letter is keyed in for encipherment, the device either rotates the alphabet drum to the next alphabet slat or remains fixed *pro tem*—the choice being determined by the operation of the stepped drum.

The stepped drum has six settings that determine the rotation sequence. The drum with which the machine is provided in the version now being recreated in Hanover will have built into it the following six rotation patterns:

1 0 0 0 0 0
1 1 0 0 0 0
1 1 1 0 0 0
1 1 1 1 0 0
1 1 1 1 1 0
1 1 1 1 1 1

Here 1 indicates *one* (60°) rotation forward of the alphabet drum, and 0 represents rest (i.e., zero-rotation fixity). One of these rotation patterns must be selected at the outset, as well as the starting alphabet.

In using the machine the operator inserts several (i.e., six) alphabetic letter slats on the display drum, each containing a different permutation of the alphabet. The machine functions via a keyboard, as on a harpsicord. Each key represents a letter, and when the key is struck a corresponding slat-letter becomes indicated. If only monoalphabetic encipherment were wanted, one would simply match the plaintext letter on the keyboard with the corresponding letter above it on the slat.

For example, let the top slat read EDACFB, while the keyboard in front reads ABCDEF (this simplified six letter alphabet will serve for an example). Then the message BE A BAD BED is encoded as DF E DEC DFC. Leibniz of course, realized that this would not provide a secure encryption, and so used his stepped drum to make the encryption poly-alphabetic. Hence the complex rotation of alphabets as controlled by the stepped drum.

The machine accordingly so functions that each time a key is depressed, its stepped drum (Staffelwalze) turns, say, 60 degrees (where there are six steps on the drum). After a certain number of letters are depressed (say three), the hexagonal alphabet drum turns so that another slat appears. The setting of this stepped drum determines the rotation sequence.

Thus with starting alphabet 1 the rotation pattern 1 1 1 0 0 0 (for example) would deliver the sequence:

1 – 2 – 3 – 4 – 4– 4 – 4 – 5 – 6 – 1 – 1 – 1 – 1 – 2 – 3 – 4 etc.

As the encription proceeds the alphabet drum rotates through its six letter-slats cyclically in the indicated manner.

Cryptographically this means that each stepped drum will provide for five out of $2^5 = 64$ different possible sequential patterns of alphabet-scramblings. (With 13 stepped drums every possibility can thus be provided for.) The prospect of a huge number of alternatives comes about through the multitude of alphabetic scramblings available for those alphabetic slats. The contribution of the stepped drum is to complicate the prospect of cryptographic frequency analysis.

In theory a more sophisticated version of the machine could be made by having a second stepped drum that so operates as to cycle the basic one through its six alternatives. Moreover, additional cryptographic security can obviously be achieved by an occasional interchange among the encipherment slats—or by replacing them altogether.[232]

With six randomized letter-display slats randomly chosen from a 10 x 10 box of 100 possibilities, and multiple possible variations for the Staffelwalze, Leibniz's cipher machine affords an impressive degree of cryptographic security—especially considering the relatively modest amount of traffic at issue in 17th century diplomatic correspondence.[233] With N variations and pre-programmed slat changes, Leibniz's machine provides for an aperiodic polyalphabetic substitution unsurpassed in security by cipher machines before the end of World War I.

The cryptographic security of the Leibniz machine rests on three considerations:

1. That successive letter-inputs can receive their correlative outputs via different letter slats each bearing arbitrary reorderings of the alphabet.

2. That the shift from one letter slat to the next can occur at ongoingly variable rates as controlled by the stepped drum *Staffelwalze* (Leibniz gear).

3. That both the rotating letter-output slats and the rotation-controlling stepped drum can be varied via interchangeable alternatives to prevent texts of great length being generated on the same principles.

The use of wooden letter-slats from polyalphabetic encipherment goes back to the *Arte steganographica* of Kircher's *Polygraphia nova et universalis ex Combinatica arte delecta* (Rome: Varesius, 1663).[234] What Leibniz's cipher machine does is to effect a polyalphabetic substituion of the same sort effected by Alberti's cipher disk or Kircher's cipher slides, but to eliminate all the laborious (and error-inviting) physical letter-matching. Leibniz's *machina deciphratoria* renders the entire process automatic and fail-proof by mechanization.[235] And so it seems fair to say that Leibniz's keyboard-operated apparatus is a milestone in the long history of cryptography. It clearly marks the transition from cryptographic *devices* (such as the cipher slide or wheel) to cryptographic *machines*.[236] In this regard as in many others Leibniz was far ahead of his time.

Various comparisons are suggestive.[237] In the summer of 1786 Conrad Fredrik Gripenstierna, a former army officer, presented to king Gustav III of Sweden a memorandum describing a cipher-device consisting of

57 wheels fitted about a common axel and enclosed in a long cylinder. Each wheel works an array of letters and markers displayed on opposite sides. It was designed for use by two persons and was very cumbersome to operate.[238] This apparatus clearly lacked the automaticity of Leibniz's century-prior machine, whose use of a keyboard was two centuries before its time. However, Leibniz's apparatus was in some regards akin to Arvid G. Damm's machine A-21 with its sliding revolving drum with 26 alphabetic faces. But this WWI-era machine, while rather more sophisticated than Leibniz's, came along only much later (in 1918).[239]

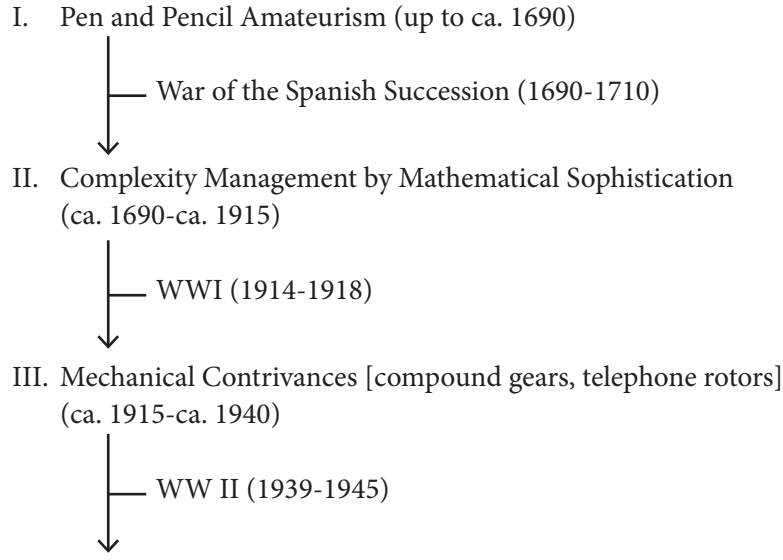
Leibniz's cipher machine actually enjoys important cryptographic merits. The Vigenère cipher affords an instructive contrast here. This so-called *chiffre indechiffrable* was broken publicly in the 1860s by Frederich W. Kasicki (and secretly earlier on by Charles Babbage in the 1850s) through exploiting the regularity-pattern of its recourse to a "Vigenère Square" array of alphabetic sequences. However the Leibniz machine will not manifest any regularity in its mono-alphabetic input. Moreover, its use of a Staffelwalze (stepped drum)—and especially in a manner that admits of exchangeable variations—effectively eliminates the cyclic regularity that eases the code-breaker's task. Other variations can also readily be introduced into the operation of the machine. Thus in a letter to Mertz von Quirnheim[240] Leibniz suggested attempting enciphermemt proceeding between a code and a decode mode. This process would be adopted to use of the machine by alternating the code/decode setting after every N strokes. And last but not least, a salient advantage of Leibniz's machine lies in its mechanical automaticity of its operation. Not only does this contribute to the ease and efficiency of its use, but it countervails against the sorts of operating errors that often aid the code-breaker's work.

In this regard, a look at the historical situation as sketched in Display A is instructive. It depicts the successive levels of cryptological sophistication as impelled through successive state-of-the-art change by the requirement of increasingly sophisticated methods contrived under the pressure of wartime requirements. And it serves to indicate that Leibniz's machine achieved the level III sophistication of the World War I era already in the era of the level II sophistication of the War of the Spanish Succession.

The cyclic alternation between improving the existing state-of-the-art in encryption and in code-breaking is typical of any technological arms-race. But Leibniz's device was a massive chronological anomaly.

Display A

The Four Historical Stages of Cryptanalysis



The cyclic alternation between improving the existing state-of-the-art in encryption and in code-breaking is typical of any technological arms-race. But Leibniz's device was a massive chronological anomaly.

For an effective cryptological attack of his cipher machine would call for the mechanized sophistication of the 1930s in the time of the 1670s. The Leibnizian *machina deciphatoria* was some 250 years before its time. e.g., IBM tabulators using punched Hollerith cards.

Like the ENIGMA, Leibniz's cryptographic machine takes a keyboard-provided alphabetic letter input, does its letter scrambling, and then provides an alphabetic letter output. Of course there are differences. In the one case the mechanism is electrical, in the other mechanical. The one uses multiple letter rotors, the other a single set of revolving slats. The one has a typewriter, the other a piano-style keyboard. But all these simply reflect differences in the technological state of the art. In basic concep-

tion—in spirit—the two machines are kinsmen and given the extent of the analogies at issue, no more than allowable exaggeration is involved in characterizing Leibniz's cryptographic machine as a proto-ENIGMA in its generic modus operandi.[241] It too dispensed with manipulating clumsy devices like slides and wheels, and in ease of use—speed, efficiency, reliability—is on a par with its famous successor.

3. The Fate Of Leibniz's Cryptological Brainstorm

Leibniz's discussion of his cipher machine made it clear and explicit that he intended it only for "a potentate or high person". In his memorandum for the audience with emperor Leopold I Leibniz observed that:

> The mechanisms I have thought out (except the arithmetical machine and those for improving clocks) have for the most part been kept secret and mentioned to virtually no-one.[242]

It seems clear that Leibniz was not going to have his cipher machine constructed unless and until some great prince showed an interest.[243] He seems to have thought that the fewer who knew of it the better.

As a result of this secrecy, virtually all that we know about the machina deciphratoria came from Leibniz's pitch of it to the Emperor. In first presenting Leibniz's memoranda for Leopold I, the editors of the German Academy's great Leibniz edition comment: "It yet remains unknown if Leibniz actually intended to construct such a [cryptographic] machine or even brought it to reality."[244] In view of the secrecy in which he veiled this effort it is, however, very unlikely that he did so.[245] The fact is that this apparatus was Leibniz's most closely guarded secret. Although he was often prepared to boast of his innovations and inventions yet this one was only mentioned in private memoranda for viva voce presentations to princes. But John Frederick and Leopold (and their advisors) were not interested in Leibniz's cipher machine, apparently because they mistakenly had an all too common confidence in the security of their existing procedures. The conception of a cryptographic machine is one which, like many other ingenious ideas, makes its first appearance in the fertile mind of Leibniz.

Work on his cipher machine impinges on various Leibnizian projects. Obvious here is its connection with Leibniz's longstanding interest in combinatorics, as well as his work on the symbolic rendition of information

that figured importantly in his logical work. But its most significant feature is its direct bearing on Leibniz's project of a *calculus ratiocinatur*. In this regard, the general idea of the mechanization of thought came to concrete fruition in two of Leibniz's ventures into machine development—the calculating machine on the one hand and its offspring the cryptographic machine on the other, the one being directed at the cognitive manipulation of numbers and the other at that of symbols. Thus overarchingly there stands a principle which this apparatus shares with Leibniz's calculating machine—namely the idea of a complete mechanization of the cognitive process of transmuting a given input-problem (a calculation on the one hand and a text on the other) into a desired output-answer (the required quantity in the one case and the required test-encoding in the other). The machine is a physical embodiment of the Leibnizian precept that the crux of reasoning lies in the injunction *calculemus* ("Let us calculate!")

Accordingly, in his philosophy of nature Leibniz astutely combined a foreground mechanism with respect to concrete phenomena with a background idealism with respect to explanatory principles:

> All the particular phenomena of nature could be explained mechanically if we were capable enough...) But I hold, nevertheless, that we must also consider how those mechanical principles and general laws of nature themselves arrive from higher principles and cannot be explained by quantitative and geometrical considerations alone.[246]

Leibniz was thus a self-avowed metaphysical mechanist who believed that the phenomena of nature could be explained on mechanical principles, and as such was prepared to regard the man and mind alike as a machine. But with a crucial difference, the machine at issue being of a very special sort, since mental operations are certainly not the product of machines as we know them. And just this was the salient point of Leibniz's famous Windmill Analogy:

> One is obliged to admit that *perception* [i.e. mental activity] and what depends upon it is *inexplicable on mechanical principles,* that is, by figures and motions. In imagining that there is a machine whose construction would enable it to think, to sense, and to have perception, one could conceive it enlarged while retaining the same proportions, so that one could enter into it, just like

> into a windmill. Supposing this, one should, when visiting within it, find only parts pushing one another, and never anything by which to explain a perception.[247]

Leibniz was thus prepared to hold that mental processes lie outside the capacity range of mechanical contrivances of *the usual sort*. And on this basis, Leibniz emphatically rejected the crude machine theory of Julien Offroy de la Mettrie's 1748 *L'Homme Machine* more than half a century before its time.[248]

There is, however, another very different aspect of the matter:

> Each organic body of a living being is a kind of divine machine or natural automaton which infinitely surpasses all artificial automata. For a machine made by human artifice is not a machine in each of its parts. For example, the tooth of a brass wheel has parts or pieces which to us are no longer artificial things, and no longer have something recognizably machine-like about them, reflecting the use for which the wheel is intended. But the machines of nature, namely living organisms, are still machines even in their smallest parts, ad infinitum. It is this that constitutes the difference between nature and artifice, that is, between divine artifice and ours.[249]

In rejecting the idea of the mind as an *ordinary* (artefactual) machine, Leibniz is nevertheless prepared to see it as an infinitely more complex *natural* machine of divine artifice. And in such an infinitely more sophisticated "machine," the mental and physical operations are not separate factors that are causally interconnected, but features of one integrated and coordinated harmoniously uniformity of process. A difference of degree here makes for a difference in kind as between the machines of nature and the machines of human artifice.[250] For there now comes the daunting challenge: how can physical and mental processes possibly be harmoniously integrated and coordinated? How can a mere mechanism be conceived of as involved in the performance of such mental processes as reasoning and symbolic communication.

Leibniz was here reacting against contemporary Cartesians who saw the human body as a machine managed by a mind-being who steered its operations like a coachman steers a coach (as per what Gilbert Ryle

mocked as the "ghost in the machine" [251]). This requires the mind to be just one more constituent of the overall make-up of the machine. (Just this is what the windmill story was designed to refute.) Instead, Leibniz held that mind is not a matter of what the machine contains by way of constituent parts or components, rather is a matter of what it does by way of operative functioning. Intelligence is neither an internal component of the machine nor an external operator of it: instead, it resides in the way in which the machine operates—so to speak, in the software that characterizes its functioning rather than in the hardware that constitutes its operations.

Yet how can one get one's mind around the idea of a machine that can carry out mental functions? In Egg-of-Columbus fashion, Leibniz set out to solve this conundrum by actually designing machines that could do the job of performing mental operations. For in meeting this challenge, Leibniz in effect said "I am not just going to *tell* you how, I am going to *show* you how." And at this point he switched from Leibniz the theorist to Leibniz the mechanician and embarked on some brilliant feats of engineering.

What, after all, are the quintessential powers and capacities of mind? Clearly they are *reasoning* and *linguistic communication*. And even as Leibniz's calculating machine joined with his "calculus of reasoning" (*calculus ratiocinatur*) to show vividly how reasoning could be mathematically automatized, so the cipher machine automated the process at issue with communication. For what, after all, is encoding a message but to translate it from one language to another—the former familiar and perspicuous, the latter obscure?[252]

Those Leibnizian machines accordingly represent devices that are deeply implicated in the operations of the mind. For he assimilated reasoning to procedures where the mind configures and reconfigures facts by calculation and its instrumentalities are numerical. And in communication the mind configures and reconfigures things by *information* and its instrumentalities are verbal. And here it was Leibniz's insight that numbers can be made to do the work of words and calculations to do the work of reasoning. (Kurt Gödel could not bring himself to believe that Leibniz had not contemplated the idea of Gödel numbering.)

On this basis, those machines of his are vivid illustrations of how Leibniz conceived mechanical processes as deployed to good effect with

regard to both the sorts of processes involved: both reasoning and communication. As he saw it, the calculating machine performs mind-like processes in relation to reasoning, the cipher machine performs mind-like processes in relation to communication.

What Leibniz envisioned here represents a tectonic shift in conceptual point of view. Confronted by the operations of a machine such as the windmill we can ask: "What is it doing?" and looking to answers of the format "It is Xing." Now with ordinary machines the appropriate X will be something mechanical: "it is grinding" or "it is cutting" or even "it is keeping time." But—so Leibniz believed—with those machines that he himself envisioned the answer is something very different because now we can reply: "it is adding" or "it is translating." That is, we can now fill in that X with something that is a cognitive and thereby mental operation. And at this point—so it appears—we have taken a large step towards an entirely new conceptual realm—the field of artificial intelligence.

And so, as such considerations indicate, Leibniz's ingenious machines were not *just* developed for their quite obvious utility in their own right. They also constituted integral parts of a larger philosophical program that implemented a deep-rooted and far-ranging framework of thought, providing a vivid illustration of Leibniz's amazing capacity to give a concrete embodiment to his abstract reflections.[253]

III

Pictographic Contextualization of Leibniz's Machina Deciphratoria of the 1670s

G. W. Leibniz (illustration A) displayed his characteristic ingenuity in contriving his cipher machine. Drawing on mechanisms used in constructing his amazing calculating machine (illustration B)—and exploiting the "Leibniz gear" or stepped drum (Staffelwalze) which he contrived especially for this apparatus (illustration C)—he designed the world's first cryptographic machine. Its capacity far outreached such cryptographic devices as Alberti's cipher disk (illustration D) or Jefferson's cipher cylinder (illustration E), instruments whose functioning yielded a polyalphabetic encoding in a way whose regularity of operation rendered them vulnerable to being broken.

Leibniz's cipher apparatus, devised in the early 1670s (illustration F), was centuries ahead of its time and marked the important transition from devices to machines. Not until the World-War-I-era machines of Hebern and Damm (illustrations G, H and I) did comparable coding machines emerge, some of them using the same principles as Leibniz's, namely

typed letter input → automated scrambling → display output

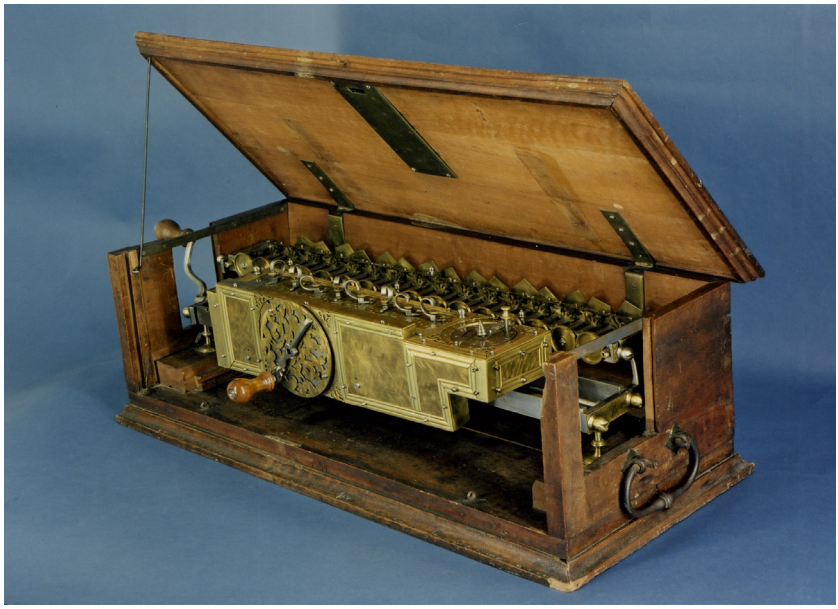
Only at this late date did cipher machines superior to that of Leibniz come into being.

Leibniz's machine was a milestone in a longer course of development. With Leibniz's machine the operator did not have to fiddle with wheels or slats: the apparatus worked in a fully automatic way that combined convenience of operation with reasonable cryptographic security.

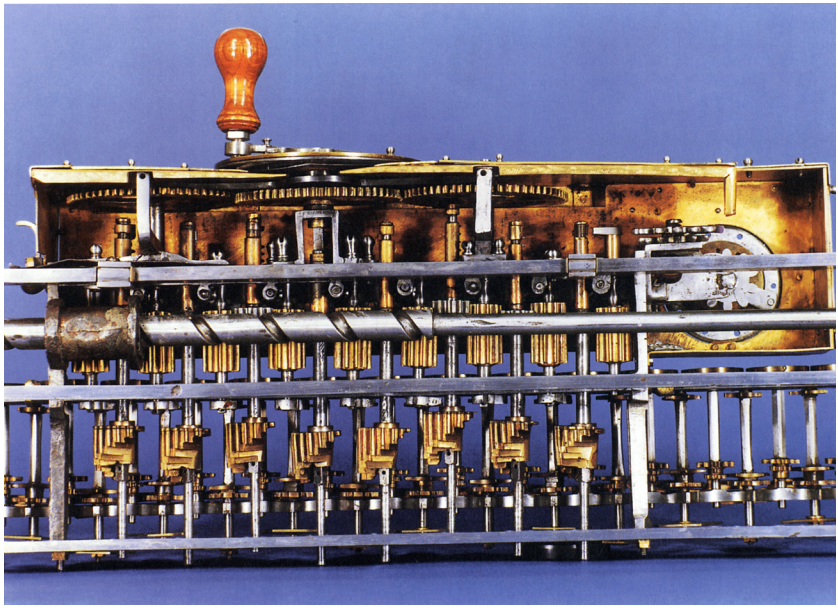
A major advance was the classic three-rotor Enigma (illustration J) which led via a four-rotor variant ("Fisch"—illustration K) to the twelve rotor "Tunny" (illustration L). Its German devisers were greatly mistaken in thinking these cipher machines un-breakable. However, coming to terms with these increasingly sophisticated machines itself demanded incredible ingenuity as well as massive innovation moving from card sorters (illustration M), to electronic pattern seekers like the so-called "Bombes" (illustration N), to full-fledged electronic computers like the "Colossus" devised by T. H. Flowers for Bletchley Park, in a phenomenal feat of electrical engineering (illustration O).

In the cleverness of its conceptualization and the sophistication of its operation Leibniz's *machina deciphratoria* of ca. 1670 was some 250 years ahead of its time.

A **G. W. Leibniz (1646-1716)**
Courtesy of Dr. Wolfgang Volk, http://www.monumath.de



B **Leibniz's Arithmetical Machine (ca. 1675)**
Courtesy of Gottfried Wilhelm Leibniz Bibliothek - Niedersächsische Landesbibliothek

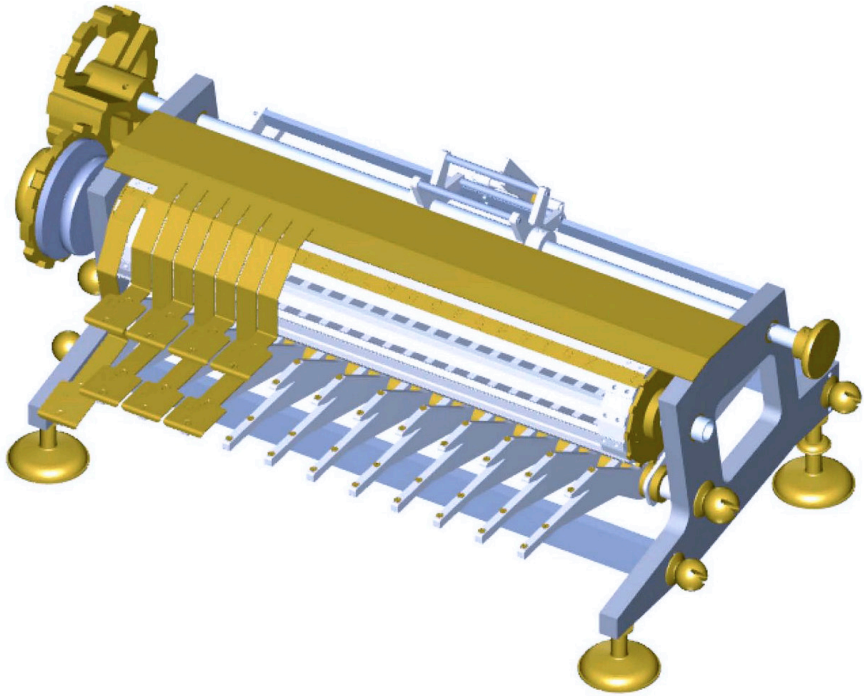


C **Leibniz's Arithmetical Machine (ca. 1675) – Close up of stepped drum (Staffelwalze)**
Courtesy of Gottfried Wilhelm Leibniz Bibliothek - Niedersächsische Landesbibliothek

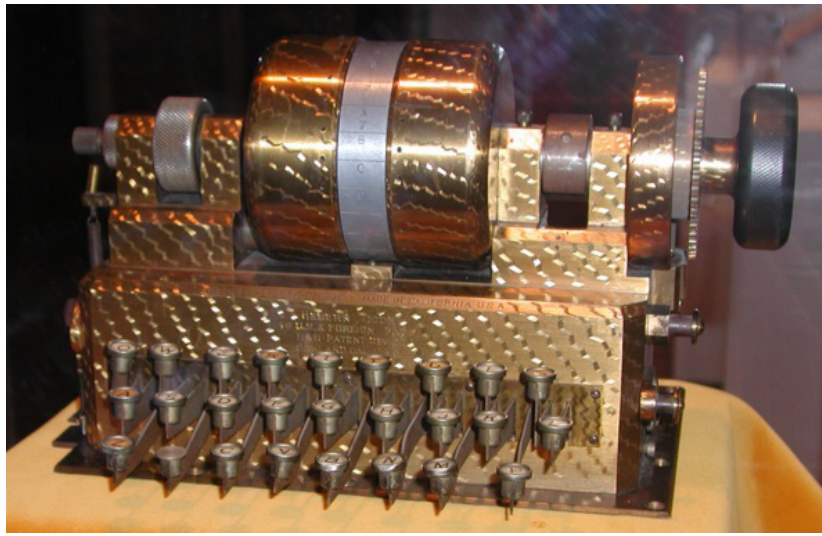
D **Leon Battista Alberti (1404-72) – Cipher disk**
De componendis cifris, 1467 – Image prepared on March 18, 2008 by Augusto Buonafalce, http://en.wikipedia.org/wiki/File:Alberti_cipher_disk.JPG. CC BY-SA-3.0.

E **Jefferson's Cipher Cylinder (ca. 1795)**
Courtesy of the National Security Agency

A variant of this design was the cryptographic device M94 (CSP-448) consisting of 25 aluminum discs arranged cylinderally on an axel. Each disc was lettered with a scrambled alphabet, and a message was encrypted by turning the discs until the plain text appeared in line. Sufficiently secure for tactical use this device remained in service until 1943.

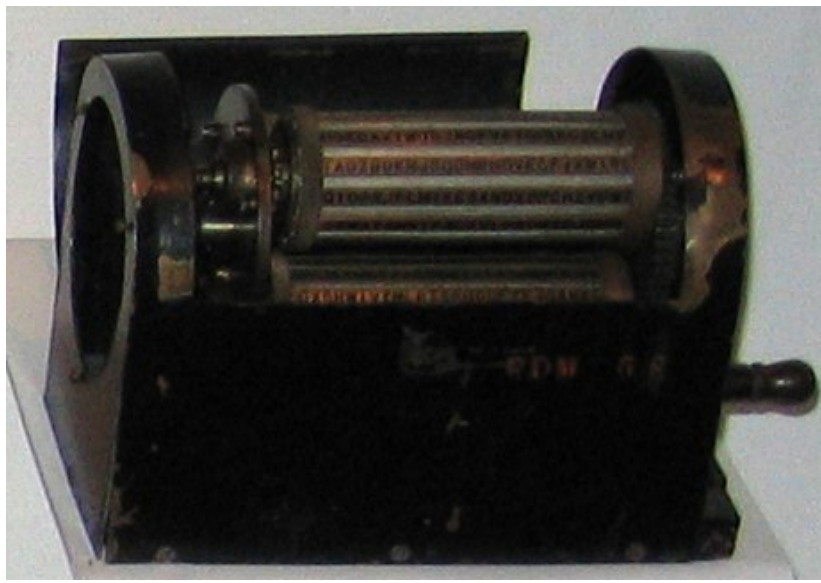


F **Leibniz's Cipher Machine (ca. 1670)**
Leibniz's machina deciphratoria under production by Klaus Badur and Wolfgang Rottstedt, using design suggestions by Richard Kotler to implement Nicholas Rescher's conceptual reconstruction of the device. (View from above.)

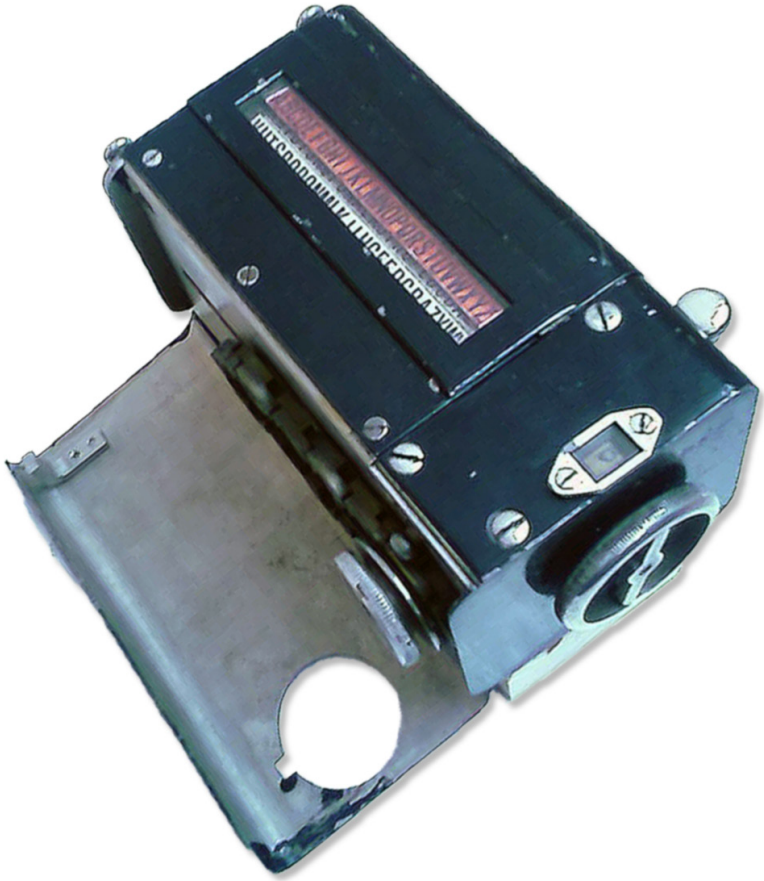


G **Hebern Cipher Machine (1918)**
Courtesy of the National Security Agency

This contrivance by Edward H. Hebern was the first of the rotor machines. Its rotor turned on each depressing of a key. Its limited cryptographic strength motivated further developments in its class.



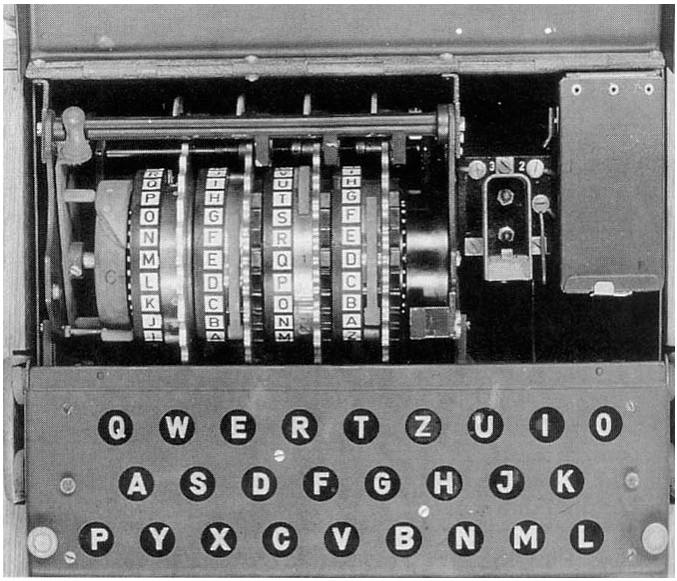
H **Arvid Gerhard Damm's Revolving Drum – Cipher Prototype from 1920s**
Courtesy of the National Security Agency



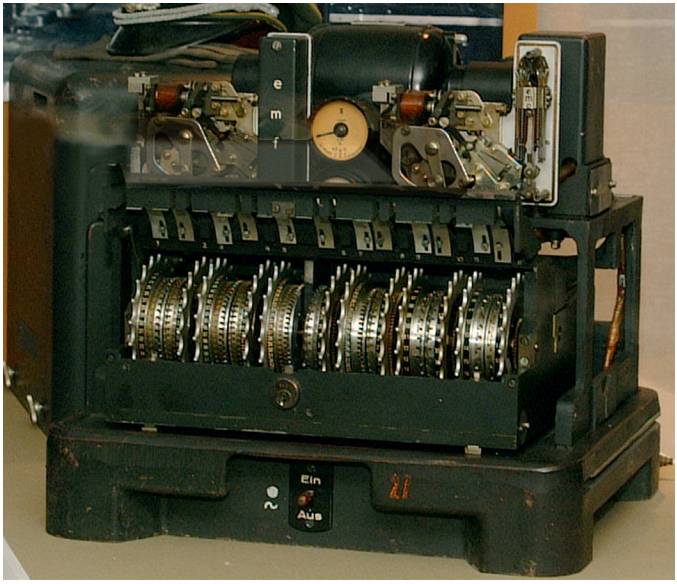
I **Arvid Gerhard Damm's A-21 of 1921**
Courtesy of John Alexander, http://www.enigmaandfriends.com via Jerry Proc, http://jproc.ca

Arvid Damm's A-21 of 1921 featured a revolving drum with 26 alphabet strips arrangeable in any order, forming a scrambled Vigniére square. For each encrypted letter the drum stepped one alphabet strip further, thereby sacrificing the variation afforded by Leibniz's use of a stepped drum (Staffelwalze).

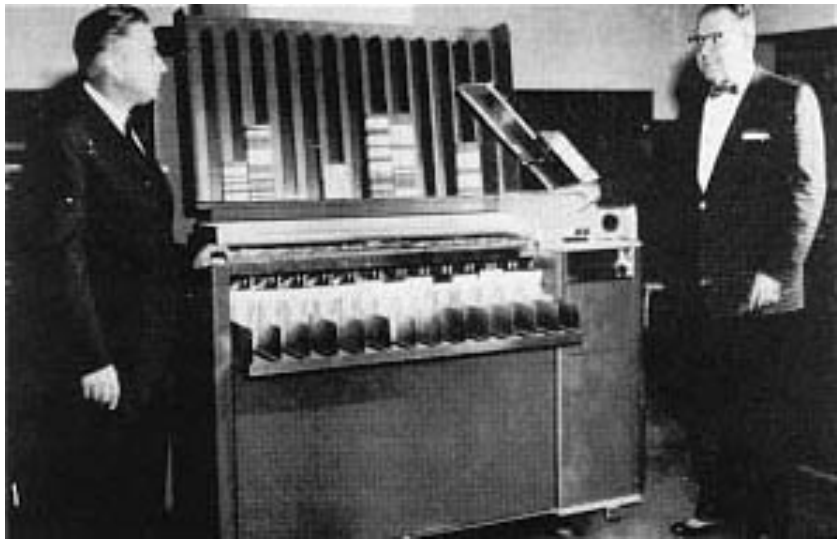
J **Classical WWII Enigma (1940s)**
Courtesy of the National Security Agency



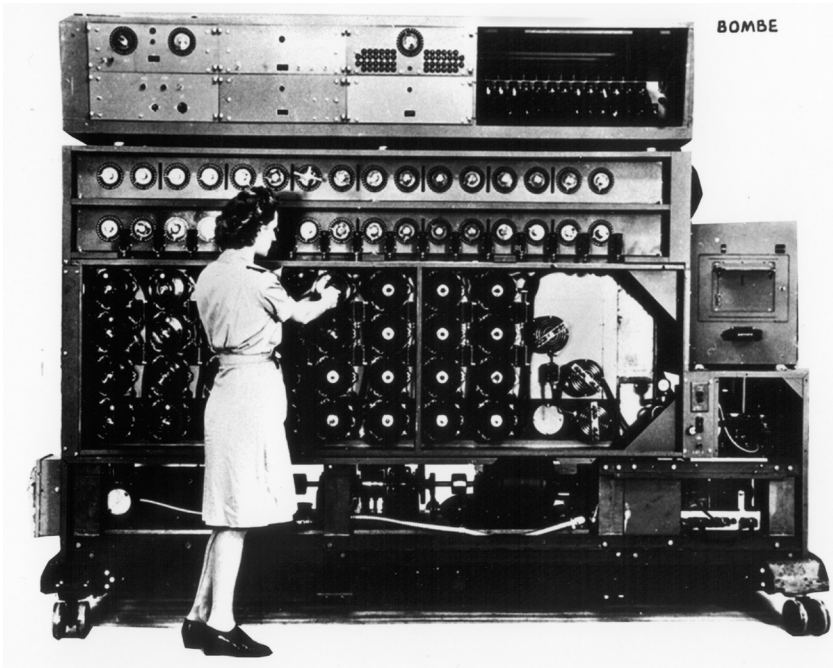
K **Four Rotor Naval Enigma (ca. 1944)**
Courtesy of the National Security Agency



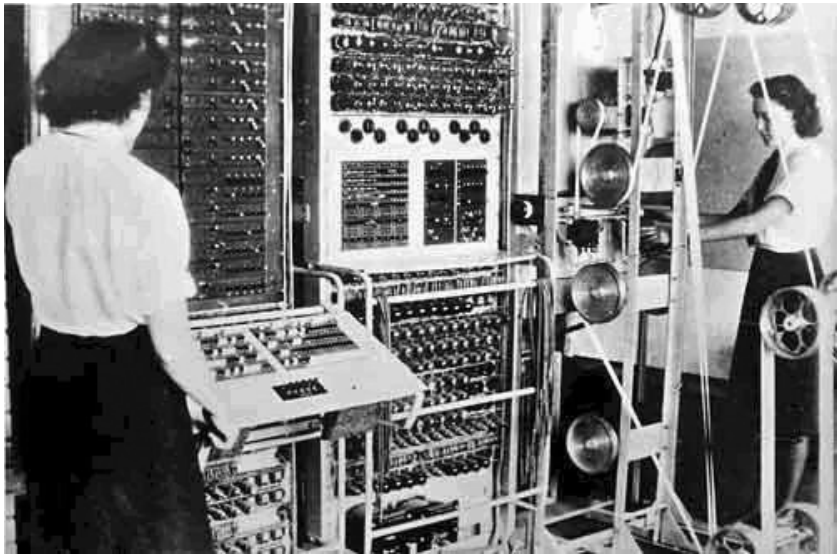
L **Twelve-rotor Tunny Machine (ca. 1944)**
Courtesy of the National Security Agency



M **IBM Card Sorter (ca. 1961)**
http://en.wikipedia.org/wiki/File:Cardsorter.fhwa.jpg



N **Bletchley Bombe**
Courtesy of the National Security Agency



O **Tommy Flowers' Colossus Mark 2 computer at Bletchley Park**
http://en.wikipedia.org/wiki/File:Colossus.jpg

IV

Leibniz's Own Work at Decipherment

The pages at issue are sheets (Blätter) 34-40 of Leibniz MS LH V VI 4, seven sheets effectively unique in the Leibniz corpus in dealing with technical issues in cryptography. [254]

In the interests of achieving a more "logical" order among this miscellaneous material I shall relabel the sheets at issue as A to G. Their substance is as follows:

Sheet A (Blatt 38)

The left side of this sheet presents a message written in a numerical code. It consists of 301 numbers of a range from 1 to 262. And scattered among the numbers are six French words. The text itself starts with 31.12.211.11 4.8.181.25.55.70.185.22.171.77.262.29. For unfathomable reasons Leibniz transposed this numeric next into an alphabetic form.[255]

Leibniz provides no information regarding the origin of this numerical text—the N-text as we shall here call it—apart from designating it as "the transmitted cipher". Was it a puzzle sent to him by one of his scientific correspondents? Did it come with a request for help from some cryptographer? Did some political official who came across the message seek help with it's decipherment? We just do not know.

The occasional occurrence of plaintext words within the numeric message is a near-to-certain sign that what is at hand is not a mere encipherment but a message written in a numeric code. However for unexplained reasons Leibniz proceeds to test—and ultimately reject—the hypothesis that a monoalphabetic encipherment is at issue.

In this context Leibniz observes that given an alphabet scrambling as per ♀ / ☽ it remains open whether LOUIS is to be rendered as ZYXUT or inversely as CNIFE.

Display 1

♉

⊙														☽	♀
a	1	23	45	67	89	111	133	155	177	199	221	243		z	L
b	2	24	46	68	90	112	134	156	178	200	222	244		y	O
c	3	25	47	69	91	113	135	157	179	201	223	245		x	U
d	4	26	48	70	92	114	136	158	180	202	224	246		u	I
e	5	27	49	71	93	115	137	159	181	203	225	247		t	S
f	6	28	50	72	94	116	138	160	182	204	226	248		s	E
g	7	29	51	73	95	117	139	161	183	205	227	249		r	G
h	8	30	52	74	96	118	140	162	184	206	228	250		q	R
i	9	31	53	75	97	119	141	163	185	207	229	251		p	A
l	10	32	54	76	98	120	142	164	186	208	230	252		o	N
m	11	33	55	77	99	121	143	165	187	209	231	253		n	D
n	12	34	56	78	100	122	144	166	188	210	232	254		m	B
o	13	35	57	79	101	123	145	167	189	211	233	255		l	C
p	14	36	58	80	102	124	146	168	190	212	234	256		i	F
q	15	37	59	81	103	125	147	169	191	213	235	257		h	H
r	16	38	60	82	104	126	148	170	192	214	236	258		g	M
s	17	39	61	83	105	127	149	171	193	215	237	259		f	P
t	18	40	62	84	106	128	150	172	194	216	238	260		e	Q
u	19	41	63	85	107	129	151	173	195	217	239	261		d	T
x	20	42	64	86	108	130	152	174	196	218	240	262		c	X
y	21	43	65	87	109	131	153	175	197	219	241	263		b	Y
z	22	44	66	88	110	132	154	176	198	220	242	264		a	Z

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

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

Alongside this numeric text there is a tabulation (marked ♉) which specifies three alternative ways (columns ☉, ☽, and ♀) for re-interpreting those numbers as letters of the alphabet. See Display 1. And now Leibniz proceeds to construe the N-text as a monoalphabetic encipherment.[256] Here Leibniz's discussion favors the ♀ enciperment, based on the key: LOUIS LE GRAND. In this way he arrives, to begin with, at the first line presented on the right-hand side of sheet A. We shall designate this ♀-decoded version of Sheet A's numeric message by its incipit: INODHEC. This alphabetized recasting of the N-text is presented on—

Sheet B (Blatt 36)

The left side of Sheet B presents the entire INODHEC decription, labeled # which recasts the numerical N-text into alphabetic form. (See Display 0.) The result is—unfortunately—a meaningless letter-array, presenting the problem of how the INODHEC message itself is to be deciphered.

Below the # text there is a mysterious long line that reads:

(1)cmasb.iface(3-4)mbahb(5)chaoa.zbaux(6)efaen(7)ugaif.lbaof(8)fyaeh.(9)xnnaxe.(10)fiael.sxano.flalpT(11)fhhadh

Note that all of these numerically labeled expressions occur in those indicated lines of the text. There is no indication here as to what this is all about. However sheet C does provide some commentary regarding this mysterious long line labeled A below the # text. It is observed that all of these are five letter configurations of the format - - a - - , with double letters are treated as singles. Apparently, an investigation of the a-contexts is at issue here.

The right side of sheet B is a work-sheet offering a discussion (in French) of some further issues regarding the decipherment of INODHEC. It concludes—with special attention to the occurrence of alphabetic doubles—that this does not seem to be possible in a coherent way. One of the ways in which Leibniz establishes this incoherence is as follows:

> By "lbb Monsieur," line 9, it follows that b is an end-letter. But there is no doubled end-letter in French save e. Hence b must be [i.e. stand for] e.
>
> By "ssbb," line 4, s cannot be a vowel if b is e.

Display 0

(1) i n o d h e c m d i z s m x g c m a s b o l t t e i f a c e h o g o o u n c h z d c m f

(2) l f l e m d s h d b z y b i o s e i d t h b i p q t u q m f x x p r l s q q b i p p o s x m u s i z s

(3) y s h b q i f e u o f h c x i z x f i r c h t x f f n b t m s h t p g d f d t u n p u p n m b a

(4) h b d t i n n u u s t n o d m r f g s s b b g **E** p u h f t e d g u y c l e f f h m o x l s i x d o u

(5) b t p s p g u x c h a o a z b a u x m c m d d f c f p o c c u r i h p s d s g n d h q g y

(6) b q t h g q z m b n t e f a e n h f u n y f s g c x c z u z u u p b g h o y h f b c s e c g o **P** e f s f c t m

(7) t x y r x c c y h i e i m o h h b i p q t h t r f q h n c f x z u g a i f b s i i b u s z h **S** y s l b a o f x b

(8) h o s y m b g t m u c s g r o x y b f u d t i g z n l d s i r f y a e h t c l o n t d d h r t h t p o h t r m d n

(9) t f q x i m x f r t x n n a x e h r l b b **M** i p c c e t g q e f n q m o c y t t h r o d m g x f y o n f y t

(10) i h n f i a e l q n t h x q b s x a n o d u m n n s u s n f f p q o p u r z d f q f x t e f g f l a l p T c c x

(11) r b y t h t x u h u r q g f h h a d h g d b t z f l f n u h o d s

E = epartement?
P = pendant
S = sufficament
M = Mr 22y
T = toursjours

> By "nnuu," line 4, it follows that one of the two letters n and u must be e. For one must be a vowel. But there is no double vowel with a neighboring double, except e.
>
> However we [already] have it that b is e. And now we find that n or u is e. But this is absurd if our alphabetic encryption hypothesis is true.
>
> Hence that hypothesis must be incorrect.

These considerations are taken to indicate that "the hypothesis" that the INDOHEC text constitutes a monoalphabetic encryption obtained via the ♉ tabulation is in trouble.

Sheet C (Blatt 37)

The left-side of D gives a statistical analysis (in German) of number-occurrence frequencies in the original numeric N-text. The right side (eventually switching to Latin) continues the frequency analysis, now addressing letters rather than numbers. It also searches the text for common French marker words like *le* or *est*. No useful entry into the message seems to be available here. Nor does a number-count of the letters help.

Moreover the right-hand side of this sheet also discusses the mysterious "long line" of Sheet B. Its observations regarding - - a - - groups have already been commented on above.

Sheet D (Blatt 39)

Sheet D is a work-sheet that begins in Latin but switches to French. It too stresses the untenability of that decipherment hypothesis, primarily because that INODHEC text contains a successive letter-double (viz. nnuu).

Sheet E (Blatt 35)

This is a work-sheet giving a German discussion of the INODHEC text in relation to its ☽-based and ♀-based variants. It too argues against the possibility of such decipherments.[257]

Leibniz reproduces the Display 1 table (incompletely) and observes that none of the ☉☽ ♀ based decipherments make any sense. Leibniz

notes that the decipherment rule here is to divide the number at issue by 22 and then determine its alphabetic counterpart via the first column and use the remainder to determine the alphabetic counterpart via the first column (but with 0 in place of 22).

Apart from the considerations adduced by Leibniz there is one further fact that looks to be significant here. The most common letter in French usage is E (with 15% frequency) which is almost twice as frequent as its next competitor S. Now in the first line of the INODHEC text (see Sheet B) one notes that of its 49 letters the most frequent are O and C (5 occurrences each) and M (four occurrences). Not only does this not come close to E's 15% occurrence rate, but also

- If O is E there will be an E-less string of *17* letters.
- If C is E there will be an E-less string of *12* letters.
- If M is E there will be an E-less string of *24* letters.

A single glance at virtually any page of text in French will suffice to indicate how implausible this is.

Again the discussion is inconclusive since none of the procedures he envisioned led to a meaningful decryption of the N-text.

* * *

Overall, the deliberations of Sheets A-E cryptography are indecisive in failing to shed any light on the meaning of the N-text—let alone its INHOTEC offspring.

Sheets F & G (Blätter 40-41)

This discussion given here stands apart from the others. Written out far more carefully, it is a single-page note entitled *Praecepta artis decyphratoriae* written ca. 1685 and published in A VI 4B. pp. 1703-06. It is devoted principally to the question of determining the language of an encrypted text and seems to be indebted to the *Mysterium artis steganographicae novissimum* (Ulm, 1682) of Lugwig Heinrich Hiller (ca. 1640).

The issue has little bearing on the present INODHEC cryptogram, whose text is obviously in French. The placement of this (far more finished) MS page with the presently relevant material is apparently based on thematic grounds alone.

* * *

A modicum of relevant material is available elsewhere. The manuscript pages of LH VI V, Blätter 30-33 are principally devoted to some notes regarding a shorthand-like steganography. However, one single Latin page, namely Blatt 32, moves in an entirely different direction. It deals with cryptology and focuses on Leibniz's favorite LABYRINTHUS cypher based on the monoalphabetic substitution:

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

Leibniz here begins by noting that periculosum would now be encrypted as frkhbpsempc. And he addresses the question of whether this item of decriptive information—this "crib" as cryptologists now call it—would enable the cypher to be broken.

The discussion accordingly moves on to the question of determining its key word. Leibniz begins by noting that we would now have:

a	b	c	d	e	F	g	h	i	k	l	M	n	o	p	q	r	s	t	U	v	x	y	z
		B		R				H		S	C		E	F		K	M		P				

And at this stage, sheer cleverness (with perhaps by some information about letter frequencies), would make it possible to conjecture the initial key word to be:

L A B Y R I N T H U S

Accordingly, the point of the discussion appears to be that realizing how even a single word is enciphered can open a doorway to overall description.

More generally, what apparently concerns Leibniz in this discussion is the cryptographic security of his much-favored LABYRINTHUS cypher.

* * *

FURTHER DISCUSSION

The first line on the right-hand side of Sheet A reads:

(1) i n o d h e c m d i z s m x g e m a s b o l t t e i f a r e h o g o o u n c h x d c m f l f l e m d s h d b z

And the next four lines read:

(2) f d n t h q x b t f l e b u m q b z e y n e s s q f p z x q h n m n n i d x h t t x b p c p c q b t e h t y l
(3) u o y n h s l g n u a t g c r
(4) p m l u q t x n u p a f n c g
(5) a b c i r s u d i a z p d x m

There then follows the numerical array given in Display 1.[258] And running alongside this numerical array there are three alphabet-correspondences:[259]

☉ a b c d e f g h i l m n o p q r s t u x y z
☽ z y x u t s r q p o n m l i h g f e d c b a
♀ l o u i s e g r a n d b c f h m p q t x y z

Applying these as substitution ciphers we find that ☽ → ♀ relettering takes (1) to (2) (and thus ♀→☽ takes (2) to (1)). So those first two lines are simply variant encryptions of the same text via a monoalphabetic substitution.

Moreover, we also have it that

- ☽→☉ takes (1) to (4) and so ☉→☽ relettering takes (4) to (1)
- ☉→☽ takes (1) to (4) and so ☽→☉ relettering takes (4) to (1)
- ☉→♀ takes (1) to (5) and so ♀→☉ relettering takes (5) to (1)
- ♀→☉ takes (2) to (4) and so ☉→♀ relettering takes (4) to (2)
- ♀→☽ takes (1) to (3) and so ☽→♀ relettering takes (3) to (1)
- ☽→♀ takes (4) to (5) and so ♀→☽ relettering takes (5) to (4)

Various transitivities are at work here. Thus since ☽→ ♀ takes (1) to (2) and ♀ → ☉ takes (2) to (4), we have it that ☽ → ☉ takes (1) to (4). And since ☉ → ♀ takes (1) to (5) and ♀ → ☽ takes (5) to (4), we again have ☉ → ☽ take (1) to (4). Other relationships will also obtain. Thus while ☉ → ☽, followed by ☉→♀ will take (1) to (2), and this same process will take (3) to (1). Unfortunately, however, it seems that no combination of these various reletterings will take (1) to anything that makes sense.

Nevertheless, several significant considerations emerge here

i. In effect, all of the texts at issue with (1)-(5) are variations on the same theme.

Display 1

♉

☉													☽	♀
A	1	23	45	67	89	111	133	155	177	199	221	243	Z	L
B	2	24	46	68	90	112	134	156	178	200	222	244	Y	O
C	3	25	47	69	91	113	135	157	179	201	223	245	X	U
D	4	26	48	70	92	114	136	158	180	202	224	246	U	I
E	5	27	49	71	93	115	137	159	181	203	225	247	T	S
F	6	28	50	72	94	116	138	160	182	204	226	248	S	E
G	7	29	51	73	95	117	139	161	183	205	227	249	R	G
H	8	30	52	74	96	118	140	162	184	206	228	250	Q	R
I	9	31	53	75	97	119	141	163	185	207	229	251	P	A
L	10	32	54	76	98	120	142	164	186	208	230	252	O	N
M	11	33	55	77	99	121	143	165	187	209	231	253	N	D
N	12	34	56	78	100	122	144	166	188	210	232	254	M	B
O	13	35	57	79	101	123	145	167	189	211	233	255	L	C
P	14	36	58	80	102	124	146	168	190	212	234	256	I	F
Q	15	37	59	81	103	125	147	169	191	213	235	257	H	H
R	16	38	60	82	104	126	148	170	192	214	236	258	G	M
S	17	39	61	83	105	127	149	171	193	215	237	259	F	P
T	18	40	62	84	106	128	150	172	194	216	238	260	E	Q
U	19	41	63	85	107	129	151	173	195	217	239	261	D	T
X	20	42	64	86	108	130	152.	174	196	218	240	262	C	X
Y	21	43	65	87	109	131	153	175	197	219	241	263	B	Y
Z	22	44	66	88	110	132	154	176	198	220	242	264	A	Z

ii. The cryptogram of line (1) is basic here. Each of those three monoalphabetic substitutions takes it to one of the four other letter-lines at issue.

iii. Two distinct reletterings lead from (1) to (4) one each from (1) to (2), (3) and (5).

iv. Inverted reletterings are symmetric. Thus ☽→☉ takes (4) to (1) and ☉→☽ takes (1) to (4). etc.

v. None of these monoalphabetic substitutions transform (1) into something that makes sense. Only ☉→♀ which leads to ABC . . . , begins to move in this direction. (As already mentioned, it seems possible that (1) is an anagram rather than a cryptogram.)

vi. A decipherment that begins to make sense—such as those two that lead from (1) to (5) with its initial abc—can break down in the sequel.

vii. Symmetric reletterings will lead to the same outcome. Thus both ☉→☽ and ☽→☉ change A B C D E etc. to Z Y X U T etc.

The salient point is that—as Leibniz rightly remarks on Sheet E—none of these decipherments yield a meaningful text ("nichts Verstaendliches heraus kommt").

* * *

In the rectangular array of Display 1 Leibniz contemplates a tabulation the 22 letters of the Latin alphabet which are then first assigned successive integers:

a	b	c	d	e	f	g	h	I	l	m	n	o	p	q	r	s	t	u	x	y	z
1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22

But then the letters of the alphabet are also assigned further numbers, twelve each as per:

$$i, i+22, i+44, i+66 \ldots i+242$$

The result is 12 x 22 number matrix that Leibniz labels ♉.

Thereupon in column ♀ each of the 22 rows (ranging from $i = 1$ to $i = 22$) is assigned a different letter of the alphabet, say in the order

1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22
l	o	u	i	s	e	g	r	a	n	d	b	c	f	g	m	p	q	t	x	y	z

as per the column Leibniz labels ♀.

On this basis the plaintext CAT could first be rendered via ☉→ ♀ as ulq, and this could then be recast numerically as

3.1.18.

However, as per the indications of the ♉ tabulation, this is not the only prospect, since each integer could be replaced by itself with *n* x 22 added—as per the 22 x 22 tabulation, so as to result in, say, 25.23.40.

To the right of the ♉ array Leibniz writes as follows:

> *Si la table ♉ est juste, et si elle exprime le veritable disposition des nombres equivalentes, le chifre est dechiphfrable quel que l'Alphabet des Lettres come ☽.☉.♀ puisse estre. Mais ayant choisi l'hypothese de cette table ♉, et ayant appliqué le chifre consecutivement dans une feuille à part marquée de #, je trouve des difficultes qui en empechent le succès. Je apprehende fort, que la véritable disposition des nombres ne soit sans ordre. Et alors que un chifre aussi petit que celuy est indecipherable, car it ne donne pas assez de conditions.*

The situation is that by using a square number array such as ♉ a clear text reading *inodhe* (as per line 1 at the top) could be encrypted as 119.149.101.224.206.247, which could then be decrypted readily by its recipient on the basis of that number array. But if a monoalphabetic substitution cypher were used then we could obtain:

1. In the case of ☽: *pmlugt* exactly as in line (4) at the top.
2. In the case of ♀: *abcirs* exactly as in line (5) at the top.

What Leibniz appears to be suggesting here is that (i) when a simple transposition cipher as per ☽ or ♀ is used, decipherment is easy. But (ii) with a regular number-square cipher such as ♉ it becomes difficult, while (iii) with an irregular reshuffling as replacement for ♉ it would be virtually impossible.

* * *

Next Leibniz adopts a different approach. He sets up a tabulation where each letter of the alphabet is assigned a group of twelve successive integers, A from 1 to 12, B from 13-24, C from 25 to 36, etc. (See Dis-

play 2 where Leibniz left the shaded part of the tabulation blank.) Here too each letter is no longer represented by a unique number, so that the encryption is all the more difficult to spot.

Thus CAT could be encripted not only as 25.1.205, but also (for example) as 33.9.216.

Display 2

a	b	c	d	e	f	g	h	i	l	m	N	o	p	q	r	s	t	u	x	y	z
1	13	25	37	49	61	73	85	97	109	121	133	145	157	169	181	193	205	217	229	241	253
2	14	26	38	50	62	74	86	98	110	122	134	146	158	170	182	194	206	218	230	242	254
3	15	27	39	51	63	75	87	99	111	123	135	147	159	171	183	195	207	219	231	243	255
4	16	28	40	52	64	76	88	100	112	124	136	148	160	172	184	195	208	220	232	244	256
5	17	29	41	53	65	77	89	101	113	125	137	149	161	173	185	197	209	221	233	245	257
6	18	30	42	54	66	78	90	102	114	126	138	150	162	174	186	198	210	222	234	246	258
7	19	31	43	55	67	79	91	103	115	127	139	151	163	175	187	199	211	223	235	247	259
8	20	32	44	56	68	80	92	104	116	128	140	152	164	176	188	200	212	224	236	248	260
9	21	33	45	57	69	81	93	105	117	129	141	153	165	177	189	201	213	225	237	249	261
10	22	34	46	58	70	82	94	106	118	130	142	154	166	178	190	202	214	226	238	250	262
11	23	35	47	59	71	83	95	107	119	131	143	155	167	179	191	203	215	227	239	251	263
12	24	36	48	60	72	84	96	108	120	132	144	156	168	180	192	204	216	228	240	252	264

Note: the darkened entries were left blank

Towards the bottom of that page Leibniz adds one further tabulation as per Display 3. Seemingly, Leibniz is here concerned with the possibility of certain combinations. Thus if 26.27.28.29 occurred relative to the Display 1 tabulation then 29 could not possibly be a or b or c since there must be three alphabetically prior letters. (However, this particular illustration does not fit Display 3.) Those numbers seem to be intended to divide the alphabet into two groups. But the rationale of this division remains entirely unclear thanks to the incompleteness of the available text.

At the very bottom of the page, Leibniz comments:

> Trois [[nombres]] lettres semblables ne se rencontrent ensemble que rarement. Quatre semblables jamais. C'est pourquoy trois ou

quatre [[nombres]] lettres qui se trouvent ensemble immediatement n'auront pas la meme valeur.

Leibniz is acutely aware that there is an inverse relationship between the decipherability of a body of encrypted text and its extent. It is a point he stressed again and again that with insufficient texts too many possibilities are left open:

> *In arte Cryptographiae . . . aliquando enim tam pauca verba alphabeto incognito scripta habentur, ut prorsus impossible sit humano ingenio clavem reperiri, imo ut fieri possit eadem verba occulte scriptamodis innumeris secundum diversas claves recte posse explicari.* (A VI 4A, pp. 371-72: mid-1679.)

The brief text at the top of the page seems to have been designed to drive home the very point.

The ciphers of the Displays 1 and 2 are interesting because while indeed monoalphabetic, they are not substitution ciphers because a single letter can be represented in many different ways. Conceivably, the numeric encipherment at issue with the numbers that underlay INODHEC could be of this sort. It is just that none of those given there could do the trick. It would be nice if one of those Display decodings enables one to make sense of this text, but this is unfortunately not the case. Neither Leibniz nor we ourselves could establish any sort of harmony between the numeric problem text before us and the decipherments afforded via Display 1 and its cognates.

The approach to monoalphabetic encipherment at issue in the Display 1 and Display 2 Tables—the use of multiple numbers to represent one single letter—contributes somewhat to enhancing cryptographic security, but runs counter to the then diplomatically universal mode of using nomenclators rather than (or additionally to) mere encipherment. This does not argue against Leibniz's mode of proceeding as such, but may well render it pointless in the face of the N-text's provenience.

Overall the sheets at issue yield the following result:

1. The numerical N-text of Sheet A lies at the basis of the discussion.
2. The tabulation of Sheet A provides for several different alphabetizations of this numeric text, in particular those based on ☉, ☽, and ♀

3. From a cryptological point of view these texts are simply monoalphabetic substitutions for one another.
4. Various rather straightforward analyses of the situation show that none of the [proposed descriptions] succeed in providing for a meaningful decipherment of the N-text.

Display 3

29	non est a . b . c . d . f . g . h . i . l . m . n . o . p . q . r . x . Ergo potest esse e . s . t . u . y . z
255	- -
118	- -
90	- -
102	- -
137	non est a . b . d . e . f . g . h . i . o . p . r . x . y . z . Ergo potest esse c . l . m . n . q . s . t [u omitted!]

On the other hand, Leibniz believes when the volume of text is sufficiently large, a decipherment should always be possible in principle. He repeatedly holds that there is no such thing as an unbreakable encipherment provided that sufficient text is available. *Haec* [viz. *deciphrare*] *semper possumus, quando est aliquod significationis alphabetum, et sufficientia sunt data.* (A VI 4B, p. 1203: ca. 1685.) However, it seems only too clear that in the present case the particulars of Leibniz's efforts is not due to an insufficiency of text but to an erroneous assumption that a monoalphabetic encipherment is at issue. For the most logical conclusion of Leibniz's elaborate cryptographic investigations of the N-text is simply that this is not the case. Granted, it is conceivable that some other alternative for letter-to-number assignments, different from those specified Displays could place a meaningful alphabetic construal upon that numerical message. But yet another prospect is even more promising, namely that what is at issue in the N-text is an encoding nomenclator that assigns words or brief expressions to those numbers (in the manner of the diplomatic text whose decipherment Wallis was shortly to publish in the *Acta Eruditorum*).[260]

What we do know is that Leibniz's investigation this text apparently convinced him that serious applied cryptographic work was not for him—that the time and application it demanded was better applied in other directions. For as best we can tell, Leibniz's defeat by the INODHEC challenge had the result that he never again made another effort at serious decryption.

It would seem that Leibniz found this close encounter with real-world cryptology frustrating, and applied it to his sage policy: "Mir gehet es wie mit dem tiegerthier, von dem man sagt; was es nicht im erste, andern, oder dritten sprung erreiche, das lasse es lauffen."[261]

Leibniz's unsuccessful encounter with the N-text seems to have had a double effect: On the one hand it convinced him of the difficulties of cryptanalysis in its application to coded communication in the real world, dissuading him from ever again devoting his own time and effort to so demanding a venture. On the other hand, it stimulated his admiration for so successful a practitioner of this arcane art as John Wallis. And it evoked a curiosity-driven determination to gain for the world of learning a fuller knowledge of the methods and processes involved. When Leibniz reviewed Wallis's Treatise of Algebra for the June 1686 issue of the *Acta Eruditorum* of Leipzig he expressed the wish that Wallis would publish more information about his cryptographic work. And when Wallis ultimately did so, Leibniz was genuinely amazed at the scale and scope of his achievement. It is clear from the Leibniz INODHEC effort that his own efforts at cryptology never contemplated the complexities at work in the diplomatic practice of his day.[262] And it is doubtless this circumstance that ultimately explains the disinterest with which his cipher machine was met in Hanover and Vienna.

Notes

I. LEIBNIZ AND CRYPTOGRAPHY

1. a *mathematico tractari meretur*. To John Bernoulli in March 1697 (GMath III, p. 377 and A III 7, p. 329). Leibniz had in view John Wallis as well as the *In artem analyticam isagoge* of Francois Viète (Tours: Jamet Mettayer, 1591), whom he often mentions with approbation. (See Kahn, pp. 116-18.)
2. A I 13, p. 551: February 1697 (to Burnett).
3. Leibniz to Tschirnhaus, June 1678: "*quod radix in Algebra, id clavis in Cryptographia.*"
4. A IV 3, p. 426. On Leibniz's project at large see Louis Couturat, *La logique de Leibniz* (Paris: Alcan, 1901).
5. GMath IV 460: May 1687.
6. GMath VII, p. 206: ca. 1685. Compare A VI 4, pp. 425, 465 (1680) and 543 (1689). See the related acterization in GPhil. VII, p. 298: mid-1680s.
7. A IV A4, pp. 80-81 (ca. 1678). It is also a component of the *ars invenienda* (or *topica*) in the *ars deciphratoria* or *ars divinatoria*. A IV A4, pp. 80-81 (ca. 16979). Compare also A VII 3, p. 406.
8. A VI 4, pp. 80-81 (1678?) cf. ibid. pp. 345 (1679) and 545 (mid-1680s). See also Couturat, *Opuscules*, p. 162 (ca. 1689).
9. See A VII 2, p. 806 and A VI 4, p. 545.
10. See GPhil VII, pp. 184-88 and 198-203.
11. See A IV 3, p. 462: Sept. 1674.
12. A IV 4, p. 200-1; ca. 1678.
13. A VI 6, pp. 454-55; NE IV 12 §13.
14. "An Introduction on the Value and Method of Natural Science," Tr. Loemker, p. 283. Compare A II 1: March 1678, to Hermann Conring.
15. See Kahn, p. 146.
16. A III 7, p. 214: December 1696. To l'Hospital. On the metaphor of "deciphering the book of nature" see Persic, pp. 685-88 and Ernst Robert Curtius *European Literature in the Latin Middle*

Ages, tr. W. R. Track (New York: Pantheon Books, 1953), pp. 319-26.

17. "On the Value and Method of Natural Science" (early 1680s). Loemker, p. 283.

18. GPhil IV, pp. 161-62; Loemker, pp. 129-30.

19. A II 1, p. 600; to Conring, March 1687; and also pp. 603-604. See also A VI 4, p. 1999 (ca. 1678).

20. See A VI 4, pp. 371-72; see also pp. 1203, and 1999. The close relationship between cryptography and probability was not something that eluded Leibniz. See de Leeuw 2007, pp. 331-32.

21. A VI 4, pp. 371-72; ca. 1679.

22. Couturat, *Opuscules*, p. 174. Already in 1674 he wrote: *Ars faciendi Hypotheses, sive Ars conjectandi diversi generis est, huc pertinent ars explicandi Cryptographemata quae pro maximo haberi debet specimine artis conjectanti purae et a materia abstractae, unde exempla regulae duci possunt quae postea etiam materiae applicare liceat*.

23. *New Essays* IV, xii, 13. This analogy of scientific inquiry to cryptography goes back to Descartes, *Rules for the Direction of the Mind* (Rule 10).

24. See Couturat, *Logique*, and also L. J. Cohen, "On the Project of a Universal Character," in *Mind*, vol. 63 (1954), pp. 49-63.

25. Caesar sent confidential messages in Greek. The U.S. Army used Navaho code-talkers in its world wars.

26. See Gerhardt's introduction to GPhil. VII.

27. See Louis Davillé, *Leibniz historien* (Paris: F. Alcan, 1909), especially pp. 500-501 and 607. His plans for library arrangements always allotted room to cryptology. (See for example A IV 5, p. 861.)

28. See A I 5, pp. 428-62 (See p. 444): Summer 1689.

29. On Jobst Dietrich Brandshagen see Bodemann, *Briefwechsel*, p. 25.

30. See A III 3, pp. 808-13. The lost letter is registered at A III 3, p. 799.

31. See also Leibniz's July 1680 letter to J. D. Crafft, A III 3, pp. 224-8.

32. A I 2, p. 319: February 1678.

33. A. VI 4B, pp. 1203-6: ca. 1685.

34. A I 9, pp. 43-44: May 1693. More on Haes below.

35. A III 4, p. 407: June 1688. Already in 1680 Leibniz observed in a letter drafted for Crafft that "eine Zipher ist zwischen uns nötig" and proposed using his LABYRINTHUS cipher. (A I 3, pp, 402-03: July (?) 1680.) On Leibniz's relations with Crafft see Rescher, 2012B.

36. On this book see Crafft's letter to Leibniz A III 4, pp. 490-96: April 1690. The encipherment consisted of the use of nonstandard lettering plus a repositioning the first letter of a word at its end. Crafft had a low opinion of this resource; he comments "Der clavis ist so leicht, dass man sich Schämen muss, denselben nicht primo intuitu gefunden zu haben" p. 492. In their own correspondence Leibniz and (especially Crafft) often used the LABYRINTHUS cypher. (See A I 3, p. 402: July (?) 1680; and pp. 341-43: February 1681, also A III 5, p. 579: June 1693, and A III 6, p. 79: May 1694, and 227: November 1694.) And again in a letter from Crafft of February 1681 touching on some alchemical matters, Leibniz appended a sketch of this. (A III 3, p. 343). He was committed to secrecy in much of his Crafft-involving business correspondence, urging "Man mus Namen und data nicht debey sezen" (III 3, p. 228). They also used the cipher based on the key JACOBUS—see A III 3, p. 466: May 1683, and cf. p. 811. See also III 3, p. 363.

37. A III 4, pp. 492-93: April 1690.

38. See A I 3, pp. 486: June 1681 and p. 493: August 1681. Breger, 2006 (p. 102) rightly suggests FORTUNA as the key word here.

39. A I 6, pp. 391-92: February 1691.

40. A III 4, p. 493: April 1690. Moreover, in a letter dealing with the reunion of the churches, Leibniz suggested to Christoph de Rojas y Spinola, Bishop of Tina, that they might mention sensitive matters in cipher, *scribenda arcaniora* (A I 3, p. 568: mid-April 1683). And in reply the bishop suggested a procedure that might serve. (Ibid., p, 577: 14 July 1683). Also in his extensive correspondence with Leibniz, Friedrich Wilhelm Leidenfrost, secretary to the Hanoverian chancery, often encrypted his reference to persons, (See A I 2, pp. 147-48, and frequently elsewhere.)

41. See the letter to Leibniz from J. D. Crafft of 25 November 1672 (A I 1, p. 406)

42. See the letter to John Bernoulli of March 1697, GMath III, p. 377.

43. Letter to Tschirnhaus of May 1678; GMath IV, p. 460. But compare G Math VII, p. 206. In his library arrangements Leibniz classed *Cryptologiae inter Mathematicos*. (See A IV 5, p. 681.) He Wrote: "*Hujus scientiae (viz. ars combinatoria) etiam portio est Cryptographia, quamquam in ea non tam componere quam resolvere composita et ut ita dicam radices investigare difficile sit. Nam quod radix in Algebra, id Clavis in Cryptographia Divinatoria*." (A II 1, p. 622.)

44. A I 11, p. 352: March 1695. On Rossignol see Kahn, pp. 157-65. St. Simon called Rossignol "the most skillful decipherer in Europe." (Persic 1997, p. 685.)

45. A VI B, pp. 1203-1206: ca. 1685. This particular text forms part of LH V VI 4 and is apparently extracted from L. H. Hiller's *Mysterium artes steganographicae novissemum* (Ulm, 1682). See Appendix 1.

46. See A I 1, passim.

47. A I 1, p. 489: 26 March 1673. Unterdessen, dafern E. Hochfürstliche Durchlaucht einiger erwehnten Dinge fernere enclärung, oder von andern meinen *desseinen* ausführlichen Bericht . . . begehren, . . . [bitte ich Sie mir] eine zipher zuzuschicken, und sowohl die weise zu *correspondiren* als sonst zu dienen, vorzuschreiben. Leibniz also employed encipherment in his early coprrespondence with Melchior Friedrich von Schönborn. See A I 1, pp. 312-320: March 1673.

48. See A I 3, p. 5 (1680) and following.

49. See, for example, A IV 7, p. 272 (1698).

50. See A IV 5, pp. 640, 646 and 654.

51. A VI 4, pp. 1203-6. See Breger 2006, p. 103.

52. J. S. Haes, *Steganographie nouvelle* (Kassel: Jean George Hüter, 1693).

53. A III 5, p. 251. Compare also pp. 542 and 204.

54. A III 5, p. 205: November 1691.

55. A III 5, p. 251: January 1692.

56. A III 5, p. 540: May 1693. Leibniz did as Haes asked. See I A 9, pp. 43-44: May 1693. Haes was not inadept at diplomacy. He wrote to Leibniz: "Vous me dites dans votre derniere en citant Viete et Wallis que Vous sonhaiteriés que quelque habile autheur traitast à fond l'art des chifres. Il s'y en a pas de plus habiles que Vous même Monsieur pour nous donner un tel ouvrage." (A III 5, p. 287: April 1692).

57. See A III 5, p. 551: May 1693; and also pp. 554-55: May 1693; pp. 556-68: May-June 1693; pp. 571-72; June 1693. This last letter virtually grovels off the page.

58. A I 9, pp. 44: May 1693.

59. See A III, p. 643: October 1693.

60. See Persic, p. 688 and Bauer, pp. 98-99.

61. A III 5, pp. 86-87: March 1691. Huygens here writes: "pour prevenir toute dispute, il est absolument necessaire qu'on se communique premierement les chifres, comme j'ai fait il y a longtemps" (p. 87). He then proceeds to set it out. Compare also A III 5, pp. 103-05: 21 April 1691. On the details of his encypherments see Huygens, Oeuvres, Vol. 10, pp. 63-71.

62. A III 5, p. 97: April 1691. Leibniz writes "ayant déja envoyé sa solution, je ne crois pas qu'il soit necessaire de luy envoyer un chifre."

63. A III 5, p. 104: April 1691 Huygens adds: "j'adjoutay mon Chifre second contenant quelque chose de plus que le premier." See also Huygens letter of March 1691, GMath II, pp. 85-88.

64. A III 5, p. 169: September 1691.

65. A III 5, p. 169: September 1691.

66. In his correspondence with Baron Boineburg—but also, and especially, in correspondence with his friend and business partner J. D. Crafft—Leibniz used not only a cypher (generally his favorite LABYRINTHUS) but also a compact codal nomenclator. See A I 1, pp. 262ff (correspondence with Boineburg).

67. On Leibniz's dealings with Spedazzi see notes 174 an 175 below.

68. A VII 3, p. 253 (August-September 1673). Wallis had discussed cryptography in his *Mathesis universalis* of 1657.

69. *Acta Eruditorum*, June 1696, pp. 249-59. In response, Wallis sent a letter to the editor of this publication, Otto Menke, in January 1697, and subsequently wrote Leibniz that he did not know its fate, but sent Leibniz a copy via Menke. Wallis' comments on the review were then published in a subsequent issue (June 1697, pp. 254-56). Compare Menke to Leibniz in A I 14, p. 245: June 1697. The original Wallis piece is reprinted in Vol. III of his Opera mathematica (Oxford, 1699), pp. 659-72. Leibniz had been in contact with Wallis since his London visit in the early 1670s. See his letter to Mariotte A II 1, p. 372: July 1673. On Wallis as a cryptographer see Kahn, pp. 167-72.

70. Leibniz had already made overtures to Wallis via Thomas Burnett in December 1695. (See A III 6, pp. 577-78.)

71. To GMath IV, p. 14: March 1697.

72. GMath IV, pp. 18-19: April 1697.

73. A III 7, p. 759: April 1698.

74. Ellis, p. 127.

75. GMath IV, p. 3. On Wallis and Leibniz's relation to him see J. E. Hoffman, "Leibniz und Wallis," *Studia Leibnitiana*, vol. 5 (1973), pp. 245-91, and also Beeley 2007.

76. See D. E. Smith, "John Wallis as a Cryptographer," *Bulletin of the American Mathematical Society*, vol. 24 (1917), pp. 82-96, where we are given a brief but vivid picture of Wallis' work as a decipherer.

77. Ibid., p. 87.

78. A VI 2, p. 129.

79. See A I 16, p. 250: to Ferdinand of Toscana, November 1689, and also A I 11, p. 432; to Thomas Burnett, April 1695. And again: "Je lui exhorterary [i.e., Wallis] de nous donner quelque chose sur l'art de dechifrer, où l'reussissoit merveilleusement [dejà] dans son jeunesse," A I 13, p. 551: February 1697.

80. Thomas Smith, *Vellem vir egregius [i.e., Wallis] aliquid nobis daret de Arte Solvendi aenigmata*

cryptographica, in qua vix quenquam sese habere ostendit. (A I 13, p. 300: 16 October 1696.) Compare A I 16, p. 250.

81. Extending from 1696 to 1700 this correspondence is printed in GMath IV pp. 1-82 as well as in A III 10-11. The Gerhardt edition is cited here.

82. Beeley, pp. 68 and 75 (note 58).

83. Leibniz to his secretary, Otto Menke, A I 14, p. 439: September1697.

84. Ibid.

85. Breger, 2007 (p. 104) characterizes it in these terms.

86. A I 6, p. 267: 20 October 1690. See also A III 5, p. 314: June 1692 (to Justel for Halley). On Justel see Bodemann, *Briefwechsel*, p. 107. He had moved to London in 1681 and eventually became the royal librarian there.

87. A III 5, p. 314: June 1692.

88. To Thomas Burnett in London (A I 11, pp. 430-34: April 1695); see also (A I 13, p. 551: February 1697). To Alexander Cunningham in London (A I 8, pp. 502-03: November 1692). To Henri Justel then in London (A I 6, p. 267: October 1690). To Thomas Smith in London (A I 13, p. 300: October 1696).

89. A I 13, p. 551 February 1697. Leibniz also asks about the identity of another English adept of whom he had heard, describing the craft as half-mathematical in nature. Burnett says nothing about the matter in later correspondence.

90. A I 8, p. 502: November 1692.

91. A I 13, p. 300: October 1696. To Thomas Smith.

92. AI 14, p. 245: 1 June 1697. (Otto Menke to Leibniz). Subsequently reprinted in Wallis' *Opera mathematica*, Vol. III (1699), pp. 659-67.

93. To Otto Menke, A I 14, p. 439: August/September 1697. On this issue compare A VI 4, pp. 371-72.

94. A III 7, p. 593: October 1697. See also GMath IV, pp. 42, 44-45, and 65.

95. The correspondence is printed in Vol. IV of GMath. For Leibniz's pleas see pp. 14, 27, 42, 55, 65, 75, and 82.

96. GMath. IV, p. 74: November 1699. Ego vero qui nollem pulcherrimos in hoc quoque genere labores Tuos intercidere, dudum mirificam illam a Te ostentatem artem preadicando Principis cujusdam eximii curiositatem accendere conatus sum.

97. GMath. IV, p. 14: March 1697.

98. See GPhil. VII, p. 298: ca. 1685.

99. See Couturat, *Opuscules*, pp. 174 and 348.

100. *Quod memoras de Arte divinandi Occulte Scripta, est ea res non certis regulis coercenda propter infinitam varietatem Ciphras ponendi (et quarum difficultas, jam satis ardua, quotidie crescit) quae a conjecturis principio positis inchoanda est, quae prout succedere vel non succedere deprehenduntur, vel prosequendae sunt vel mutandae, donec quid certi constat.* (GMath IV, pp. 18-19: April 1897.)

101. GMath. IV, p. 81: January 1689.

102. Kahn, p. 167.

103. GMath. IV, p. 55: December 1698.

104. GMath. IV, pp. 60-61; January 1699. In this regard it warrants stress that "Wallis' skill in inter-

pretation stood him in good stead in his work in deciphering, particularly when numerical cipers and nomenclators were involved, since there the decipherer is being confronted with line upon line of numbers in which he has to divine some kind of meaning." (Beeley, p. 66.)

105. GMath. IV, p. 27: May 1697 and compare p. 42.

106. GMath. IV, p. 27; to Wallis, June 1697.

107. GMath. IV, p. 27 and pp. 55-56, and also A I 16, pp. 577 and 726.

108. See A I 16, pp. 121, 639, and 662.

109. See A I 16, p. 726.

110. A VI 4, p. 425. Leibniz's own penchant for labyrinths (e.g., of the free will or of the continuum) affords an example here.

111. Davillé, pp. 501-502.

112. GMath IV, p. 19. For the paper see See also Wallis, *Opera mathematica*, Vol. III (1699), pp. 659-67.

113. GMath IV, p. 76: March 1700.

114. See A I 16, p. 121: 17 March 1699.

115. GMath. IV, p. 82: late 1700.

116. Müller & Krönert, pp. 99, 117.

117. A I 16, pp. 249-51; November 1698.

118. A I 16, pp. 309-10: December 1698. The individual was not named.

119. A I 16, pp. 505-06: January 1699.

120. A I 16, p. 552: February 1699.

121. A I 18, pp. 686-87: May 1700.

122. A I 18, p. 723: June 1700.

123. A I 16, pp. 577-78: February 1699.

124. A I 16, pp. 639: March 1699. See also A I 16, p. 662: March 1699. Schmidt was a versatile scholar and antiquarian with whom Leibniz carried on an extensive correspondence after ca. 1690. See Bodemann, Briefwechsel, p. 261.

125. A I 16, pp. 656-57: March 1699. They returned to the matter in further correspondence, without any definite result. See A I 16, pp. 694-95: April 1699, to Schmidt. See A I 18, p. 722, June 1700, and A I 18, p. 783: August 1700. See also Schmidt to Leibniz in A I 18, p. 744: July 1700 where he mentions *Hoffmanii Professoris olim Jenensis nepos*, who is doubtless the young man at issue.

126. A III 7, pp. 969-71: 2 December 1698 (see p. 969).

127. A I 16, pp. 120-21: March 1699.

128. A I 16, pp. 120-21: March 1699. Substantial funding is necessary, so Leibniz thinks, because Wallis "durch hoffnung eines anständigen recompens zu einer zulaenglichen apertur animiert werden müste".

129. A I 16, pp. 726-27: April 1699 and compare p. 418. Magnus Gabriel Block (d. 1722) was for a time the "secretaria di camera" to Cosimo de Medici, the grand duke of Tuscany. His correspondence with Leibniz is also printed in J. Nordström, *Leibniz ach Magnus Gabriel Block* Lychnos 1695-66 (Stockholm, 1697). On Sparwenfeld see Bodemann, *Briefwechsel*, pp. 295-301, and on Block see ibid., p. 18.

130. A I 17, p. 142: May 1699. Leibniz's letter to him is not available.

131. A III 7, pp. 802 and 811-16: July 1698. On Bodenhausen—the tutor of Ferdinand of Tuscany—see Bodemann, *Breifwechsel*, p. 19.

132. Leibniz wrote Block that "J'approuve fort le choix que vous avez fait, Monsieur, de la profession de le médicine" (p. 844). I would surmise Block to be related to the Hanoverian Hofrat and diplomat Johann Heinrich Block.

133. See A III 4, p. 526: July 1690, and also p. 551: August 1690.

134. A I 18, pp. 742-43: July 1700. Also in December of 1698 Leibniz pressed M. G. Block for particulars regarding a young Swedish calculating prodigy, doubtless with a view to his Wallis project. (A III 7, pp. 969-71: 2 December 1698).

135. A I 18, pp. 742-46: July 1700. Christian L. Cibrovius was matriculated as a student in Königsberg since 1699. On Vignoles see Bodemann, *Briefwechsel*, pp. 361-62.

136. GMath IV, p. 76.

137. Kahn, p. 169.

138. See Smith, p. 84 and also Beeley p. 75 and 81 (note 97).

139. De Leeuw 1999, p. 143. Blencowe was the son of Sir John Blencow(e) (b. 1642) who married Wallis' daughter in 1675. Like Wallis, he also became a fellow of All Souls in Oxford, but died quite young.

140. See Kahn, p. 171 and De Leeuw, p. 134.

141. His pay as such was £500 that year. See Ellis, p. 129.

142. On Bode see Kahn, p. 171.

143. His pay as such was £200 in 1742. See Ellis p. 129.

144. See Ellis, pp. 63, 65, 66, 69, 71, 76, 81, 95, 105.The Neubourgs then passed the torch to the Todd family which continued in the service until the Decipherment office was closed down in 1844, when a descendent of Bode's was the last head of the office. P. H. Zollman's history is particularly interesting. See note 198 below.

145. Ellis, p. 75.

146. See K. L. Ellis, "*British Communications and Diplomacy in the Eighteenth Century,*" in Bulletin of the Institution of Historical Research (London University), vol. 31 (November 1958) pp. 159-67, esp. p. 163.

147. Leibniz "hätte ihn [Wallis] noch in dessem höchsten Alter gern als Ausbilder für junge Hanoverische Dechiffreure gewonnen." Schnath II, p. 355. In support Schnath cites the Engensen memorandum discussed above. This, however, represents only one effort among many—most aimed in other directions. As already noted, the mistaken idea that Leibniz was acting solely for Hanover's benefit goes back to Wallis himself. It was perpetuated by Eduard Vehse, *Geschichte der Höfe des Hauses Braunschweig* (Hamburg: Hoffmann und Campe, 1853), Vol. I, p. 167, and in nowadays generally, if erroneously, behind.

148. See also Beeley, p. 75.

149. GPhil VII, p. 456 (October 1697). In January of 1712 Leibniz wrote Peter the Great: "I am not someone devoted solely to his native country or to one particular nation; on the contrary, I pursue the interests of the whole human race because I regard heaven as my fatherkind and the well-meaning people as fellow citizens . . . to this end I have for a long time been conducting a voluminous correspondence in Europe and even as far as China . . ." See Vladimir Ivanovich Guerrier, *Leibniz in seinen Beziehungen zu Russland und Peter dem Grossen* (St. Petersburg and Leipzig: Commissionäre der Kaiserlichen Akademie der Wissenschaften, 1873), pp. 206-7 (Tr. in Antognazzi, p. 471).

150. Beeley, p. 75.

151. Herbert Breger suggests (Breger 2006, p. 104) that Leibniz saw his Wallis project as a means of ingratiating himself with an otherwise unsympathetic George Louis, who was clearly interested if not in cryptography as such, then in its results. I myself regard this as somewhat implausible—as well as failing to do justice to Leibniz's intellectual curiosity in a vastly challenging domain of inquiry.

152. From the short tract *de demonstrationibus* (1690), Phil. VII, pp. 198-203. (See p. 201.)

153. A I Transkription 1716, p. 165.

154. See, for example, the various letters of 1672 given in A I 1, pp. 267ff and esp. pp. 289-92. Leibniz also uses a few encipherments in a long 1673 political letter to M. F. von Schönborn. (See A I 1, pp. 312-320.) The monoalphabetic cipher used here was based on the Latin tag given on p. 312.

155. A I 1, pp. 333-35 and 338-40; April 1673. Münch's encipherment was based on the key word IAKOB, i.e. his own first name.

156. A I 1, pp. 387-94: February 1674.

157. See, for example, his 1672 draft of the Egyptian project (A IV 1, pp. 383-99: Autumn 1672). He also occasionally concealed names by speaking of someone as Mr. Nxxx. (See, for example, A I 19, pp. 342 and 379.)

158. Grote to Leibniz. A I 8, pp. 59-61: September 1690. Leibniz occasionally made a mis-decoding.

159. Schnath IV, p. 63. On Falaiseau see the Index to Schnath (many references), and Bodemann, *Briefwechsel*, p. 54 (very sparse). Leibniz passed Falaiseua's letters on to the Electress Sophia who asked him to decipher them first to save her the trouble. (See A I 21, p. 68: September 1702).

160. Schnath IV, pp. 661-64. In a letter of October 1705 to Falaiseau in London Leibniz addressed him as Ministre d'état. (Ibid, p. 647.) For other references to encrypted messages from Falaiseau see A I 21, pp. 68 and 74 to Sophia 1702. The electress expected Leibniz to provide her with transcripts *en clair*. The cipher he used is available in Leibniz's Nachlass. Some extracts by Leibniz of decoded letters from Falaiseau to Electress Sophia have survived, as has the key to the encipherment. See A I 21, p. 568 and note 1 there.

161. "Quant aux letters de Falesau (sic) je suis surprise qu'il n'a pas reseu les nostres et qu'il demande tousjour si nous n'avons pas reseu son chiffre ce que nous lui avons fait scavoir il y a longtems, et je ne crois pas que ses letters ayent esté perdues, aussi je n'y trouve pas grand chose." (A I 21, pp. 82-83: October 1702; see n. 1 there.)

162. In his letters to Sophia, Falaiseau encrypted some salient words and many proper names in a simple monoalphabetic substitution. A typical example is printed in Schnath IV, pp. 601-11, giving —and correcting—the decipherments of Leibniz.

163. A III 7, p. 329: 8 March 1697. Cf. note 35 above.

164. A I 1, pp. 406-09: November-December 1762 and also ibid. pp. 413-15: March 1673. Their correspondence only encrypted words and phrases—never entire communications.

165. A I 1, pp. 421-422: July 1674. As presented the cipher involves errors—as per the missing I between H and K.

166. A III 3, p. 294: December 1680; and see also *ibid*. pp. 304ff, 343, 401-02, 421-22, 460-62, 470-75, etc. and 489-94 as well as A I 3, p. 403.

167. See A IV 3, pp. 37-38.

168. A I 13, pp. 515-528: (February 1697). On Leibniz's contacts with Grimaldi see D. J. Cook and Henry Rosemont, Jr., *Leibniz: Writings on China* (Open Court: Chicago & La Sale, Ill., 1994).

169. Leibniz makes various practical suggestions here. He urges that encipherment be used spar-

ingly, since with less text decipherment becomes more difficult. He also shrewdly suggests that occasional errors in encypherment are advantageous in creating obstacles to decipherment. He also recommends not separating words and singularizing double letters (as per *leters*). A I 13, pp. 527-28).

170. Thus in a letter to J. D. Crafft Leibniz—then enroute to Wolffenbüttel—writes: "Will M.h.H. Mir etwas part von der persönlichen unterredung geben, so dient unser ehemaliger Labyrinthus." (A III 5, p. 579: June 1693. See also A III 3, p. 343. In a later letter to Crafft Leibniz reiterates the cipher, along with a brief (8-item) nomenclature. (A III 6, p. 79: May 1694.) And he later repeats this more elaborately, (A III 6, pp. 227-28: November 1694). The secrecy relates to Leibniz's project of collaborating with Crafft in the production of brandy (*lapis potabilis*)—one among many entrepreneurial collaborations contemplated between them over three decades (1670-1700). See Bodemann, *Breifwechsel*, p. 121.

171. See L. H. V, VI, 3 Blatt 32 recto. Even Wallis viewed monoalphabetic substitution as suffering from most personal use. See Smith 1917, p. 95.

172. Beeley, p. 72.

173. Breger, 2006, p. 102.

174. See Chapter IV below.

175. A IV 4, pp. 371-72: ca. 1679.

176. Kahn, p. 156.

177. To Count Platen ca. 1700; cited in Beeley, p. 80, n. 78. Cf. Schnath II, p. 355. In his lively account of what he calls *Descartes' Secret Notebook* (New York: Broadway Books, 2005), in dramatizing Leibniz's construal of a bit of solid geometry that was somewhat obscurely formulated by Descartes, Amir D. Aczel writes that Leibniz "had the tools for breaking codes—he was an expert on combinations and decoding" (p. 214). The last contention is only half right.

178. In a letter from Hanover of 1715 Leibniz addressed Spedazzi as "Secretaise des Chifres de l'Emperear" (A I, *Transkriptionen, 1715*, p. 628). However their correspondence related mainly to matters of banking and public finance. (See A I, *Transkriptionen, Januar-December 1715*, pp. 46-47 and 302.)

179. A I, *Transkriptionen, Januar-November 1716*, p. 65 (No. 60): 6 February 1716 (see also ibid. pp. 165, 196, 226, and 278). For Leibniz's efforts to be of use to Spedazzi see ibid. p. 337. Schöttel, a trusted friend, is one of the very few correspondents with whom Leibniz signs himself *von* Leibniz and Schöttel even addressed Leibniz as "Freiherr". Leibniz's extensive correspondence with Schöttel dealt with issues of payment from the Imperial treasury for Leibniz's service as an Imperial Hofrath (see A I, *Transkriptionen, Januar-December 1715*, especially pp. 155-60, 225-26, and 346-47).

180. Schlemm (1677-1733) also served as *secrétaire des dépeches*. For details see Schnath, Vol. II, pp. 354-55 and passim as well as S. P. Oakley, "The Interception of Posts in Celle 1699-1705" in R. Hatton and J. S. Bromley (eds.), *William III and Louis XIV: Essays* 1680-1720 *by and for Mark A. Thomsen* (Liverpool: Liverpool University Press, 1968, pp. 95-116).

181. In the reign of duke John Frederick, Zachariae was a principal draftsman of official foreign correspondence and also provided service as a decipherer. The duke found his work indispensable and brought him along on his Venetian visit of 1679. In 1688 he became vice-secretary of the Kammer, Ernest August's personal secretariat. See Schnath I, pp. 308-10 and passim as well as II, pp. 318-19. (On the Hanoverian Kammer see Schnath I 307 (51)). Zachariae was one of the few personal beneficiaries named in Ernest August's will (with 3000 taler).

182. In his capacity as Hanoverian postal expeditor, Schlemm was sometimes reluctant to accommodate Leibniz's Hanoverian correspondence. (See A I 21, pp. 100, 110-11: November 1702). On his complaints against Schelmann see also Leibniz's letter to Lorenz Hertel of 27 November

1715 (A I, *Transkriptionen, Januar-December 1715*, p. 591). One letter from Leibniz to Schlemm survives. See Bodemann, *Briefwechsel*, p. 456.

183. Schnath II, p. 355.

184. Schnath II, p. 318, and III, p. 60. See also below, towards the end of this section.

185. See for example A I 5, p, 467. Zahariae was apparently in charge of the move of the ducal library (and Leibniz's quarters) from the palace to the Anderten house in 1688)

186. See I A 21, pp. 110-11.

187. *The Historical Journal*, vol. 42 (1999), pp. 133-56. See p. 140.

188. Cp. GPhil. IV, p. 25.

189. On Augusts II in relation to cryptography see Strasser 1988 and 2007, and also Kahn, p. 154, and especially Gerhard F. Strasser, "Herzog Augusts Handbuch der Kryptographie" in *Wolfenbüttler Beiträge*, vol. 8 (1988), pp. 99-120. The duke was the uncle of Hanover's John Frederick who brought Leibniz there.

190. For Leibniz's correspondence with him see A I 3, nos. 63-65, A I 4, no. 38, A I 5, nos. 216, 226, 253, 293, and 303. All of these relate to Leibniz's dealings with him as an official of the ducal chancery (*Kammer*) outside the sphere of his cryptographic work.

191. For these officials see Schnath II, pp. 355 and 358.

192. Schnath II, p. 358.

193. Schnath III, p. 61. The average annual wage of a baker at the Hanoverian court came to some 75 taler.

194. De Leuw, p. 146.

195. See Kahn, p. 172.

196. See Ellis, pp. 71-73.

197. Ellis, pp. 63-73 gives an informative picture of the whole business.

198. See Ellis, pp. 127-31

199. To Count Platen ca. 1700; cited in Beeley, p. 80, no. 78. Cf. Schnath II, p. 355.

200. Schnath II, p. 355.

201. Schnath III, p. 61. Leibniz wrote his recommendation to Bernstorff on 11 May 1713.

202. The younger Zollmann (ca. 1685-1748) deserves attention in this own right as a scholar of impressive versatility. His father, a privy counselor in Zeitz and a regular Leibniz correspondent, made oft-repeated efforts to enlist Leibniz's aid on his behalf. Highly capable he rose rapidly in Hanoverian officialdom, and transferred to London in 1714. Initially the name was spelled Zollmann, but in England he dropped the second n. He died in 1748. (See Bodemann, *Briefwechsel*, p. 399, and especially Ellis.) In the late 1710s Zollmann regularly sent Leibniz reports from London regarding books and publications as well as political and cultural developments. (See especially A I, *Transkriptionen, Januar-November 1716*, passim and also A I, *Transkriptionen, Januar-December 1715*, pp. 142 and 545-46.) He had studied law in Leipzig and early on produced the first hydrographic map of Germany. (See Hans Rohde, "Phillip Heinrich Zollmann und seine Karte *Hydrographica Germaniae* von 1712" in *Hydrologie und Wasserbewirtschaftung*, vol. 6 (1999), pp. 310-12.) In 1715 he went to London as guardian Hofmeister to Baron von Bothmer's son, apparently on Leibniz's recommendation. There he came into the service of the Secret Office and in 1723 was subsequently appointed Secretary for Foreign Languages to the Royal Society on Robert Walpole's recommendation owing to "his skill in many languages". (See Derek Mossarelle, "P. H. Zollmann, First Assistant Secretary

for 'Foreign Correspondence," *Notes and Records of the Royal Society of London*, vol. 46 (1992), pp. 219-34.) In 1727 he was elected a Fellow of the Royal Society. As of the early 1730s he was a secretary in the British legation in Paris, where his scientific work doubtless provided a convenient cover for more covert tasks. His literary estate consisting of many letters has found its way into the Bodleian library.

203. Herbert Breger has proposed that "Wir werden auch nicht von vornehin auschliessen können dass Leibniz . . . mit Blick auf eine mitlesende Hannoversche Geheimkanzlei geschrieben haben könnte." (Breger, 2006, p. 101) While this is perfectly true, it is still unlikely that Leibniz realized the extent to which this was probably the case.

204. Schnath II, p. 355.

205. The monumental novel triptich, *The Baroque Cycle* by Neal Stephenson (*Quicksilver, The Confusion, the System of the World* (New York, William Morrow, 2003-2004), assigns to Leibniz the role as a master cryptographer who used his discovery of binary arithmetic in coding. But in this particular regard any relation to the historical actualities is purely coincidental.

206. Trithemius projected a *magia naturalis* developed in such works as his *Steganographia* (1500 but first published in 1606) and *Polygraphia* (1507 but first published in 1518). For him see W. Schneegans, *Abt Johannes Trithemius und Kloster Sponheim* (Kreuznach: R. Schmithals, 1882) and Wayne Schumaker, " *Johannes Trithemius and Cryptography*," *Renaissance curiosa: John Dee's conversations with angels, Girolamo Cardano's horoscope of Christ, Johannes Trithemius and cryptography, George Dalgarno's Universal language* (Binghamton, NY: Center for Medieval and Early Renaissance Studies, 1982). The mystification which Trithemius cast over his discussion led to its being placed on Rome's index of prohibited books.

207. A I 2, p. 125: February (?) 1679. The only Leibniz biography even merely to mention this remarkable machine is Erke Christian Hirsch, *Der berühmte Herr Leibniz* (Munchen; C. H. Beck, 2000), p. 227.

208. A IV 4, p. 27: August/September 1688.

209. A IV 4, p. 27, notes. In his memorandum for Duke John Frederick of October 1679 (A I 2, p. 223) Leibniz says that he will "an der *Machina Arithmetica* eifrig arbeiten lassen" and then makes the marginal addendum "item die Machina zum dechiffrieren." "Ob Leibniz . . . die Absicht, eine solche Maschine zu konstruiren, weiter verfolgt oder sogar in die Tat umgesetzt hat, ist noch nicht bekannt." Given his commitment to secrecy, I see this as very unlikely before this idea found princely reciprocity.

210. A. IV 4, p. 44

211. A IV 4, P. 29.

212. On Zollmann's projected visit see A I, *Transkriptionen, Januar-November 1716*, p. 35: 31 July 1716. In his memorandum for Duke John Friedrich of October 1679 (A I 2, p. 223) Leibniz says that he will "an der *Machina Arithmetica* eifrig arbeiten lassen" and then makes the marginal addendum: "item die Machina zum dechiffrieren." However, we have no indications that he did so.

213. See the article "Staffelwalze" and "Stepped Reckoner" in the Wikipedia's internet article of this name.

214. Ibid. and see also A IV 4, p. 45, but see also pp. 27 and 68.

215. Müller & Krönert p. 260.

216. See note 202.

217. For a good account of Leibniz's calculating machine and its potential see Stein 2006. All in all Leibniz spent roughly 20,000 gulden of his own money in the fabrication of his machine—well over a million dollars in present-day purchasing power.

218. Persic, p. 678.

II. LEIBNIZ'S MACHINA DECIPHATORIA

219. An original copy of Leibniz's calculating machine has survived and ample information—and excellent pictures—are available in the internet. Leibniz celebrated his calculating machine with the proud motto *supra hominem*.

220. A I 2, p. 125. (Here A stands for the Akademie edition cited in the References, with a Roman numeral for the series (here I) and an Arabic numeral for the volume (here 2).) For a general overview of Leibniz's dealings with cryptography see Breger 2006.

221. A I 2, p. 223: October 1679. On Leibniz's ongoing struggles to produce a proper working model of his calculating machine see Hirsch 2000. Phillip Beeley has stated that "Leibniz already in his youth spoke of the construction of an arithmetical machine for encipherment and deciphering letters" (Beeley, p. 72) But there is considerable inaccuracy here. Granted, his arithmetical machine goes back to ca. 1774 in Leibniz's Paris period (aet 26). But his *cipher* machine is something quite different—an after-thought that was never mentioned until the letter to John Frederick of 1679 (aet 33).

222. Mueller-Kroenert, p. 92. On Leibniz's long-aspired audience with Leopold I see Hirsch 2000, pp. 225-30. In the middle of 1688 Leibniz formally petitioned to have an audience with Leopold, partly to thank him for access to the royal library, but primarily to publicize his own past and projected activities for the public good. (A IV 4, pp. 3-4: summer 1688). This audience was granted him late that October.

223. A IV 4, pp. 15-40: August/September 1688.

224. For the former of these see A IV 4, pp. 78-90, and for the latter see ibid. pp. 50-78 (late Sept. 1688).

225. A IV 4, p. 27: August/September 1688.

226. A IV 4, p. 45: August/September 1688.

227. A IV 4, p. 68: August/September 1688.

228. On Vienna's later (1695-8) disinterest in secret intelligence from Hanover see Schnath II, pp. 75 and 357. The administration of Leopold I clearly felt confident in the sufficiency of its own resources. In the days of the War of the Spanish Succession, the Imperial black chamber—the Geheime Kabinets-Kanzlei—was the best in all Europe. (Kahn 1967, p. 163.) On its history see Stix 1937.

229. However, this possibility only came to light in 2001 with the publication of A IV 4. In its wake I have been able to devise a conceptual reconstruction of the apparatus with the assistance of my engineer friend Richard Kotler. Arrangements are under way for a physical model of the machine to be fashioned by Messers Klaus Badur and Wolfgang Rottstet of Hanover who have expertise with the construction and operation of Leibniz's calculating machine.

230. Trithemius projected a *magia naturalis* developed in such works as his *Steganographia* (1500 but first published in 1506) and *Polygraphia* (1507 but first published in 1518). For him see W. Schneegans, *Abt Johannes Trithemius und Kloster Sponheim* (Kreuznach: R. Schmithals, 1882) and Wayne Schumaker, " J*ohannes Trithemius and Cryptography," Renaissance curiosa: John Dee's conversations with angels, Girolamo Cardano's horoscope of Christ, Johannes Trithemius and cryptography, George Dalgarno's Universal language* (Binghamton, NY: Center for Medieval and Early Renaissance Studies, 1982). The mystification which Trithemius cast over his discussion led to its being placed on Rome's index of prohibited books.

231. For an animated illustration of this mechanism see the article "stepped reckoner" in Wikipedia (English version), as well as the article "Staffelwalze." Leibniz's calculating machine has nine

of these; the cypher machine needs only one.

232. The constant change of encryption-alphabets responds to the fact that encipherment variation impedes decipherment (*facilius est cryptographemata solvere, si plures literas occultandu sensu secundum eandem clavem scriptas*) (A IV 4, p. 2001).

233. The slat-count of six is an artifact of reconstructive convenience. Leibniz's original plan might well have been 10 with the decimalized calculating machine in view.

234. See De Leeuw, 2007, p. 361 and Strasser 2007, 315. On Kircher see Kahn, pp. 904-5 as well as the *Catholic Encyclopedia*.

235. On issues of antecedence See David Kahn, "On the Origin of Polyalphabetic Substitution," *Isis*, vol. 71 (1980), pp. 122-27.

236. With a *device*, the linkage of input to output is effected entirely by the operator; in a *machine* it is mediated by a series of operations performed by the apparatus itself. Thus a pencil is a device for writing but a typewriter a machine; a sundial is a device for telling time, a clock is a machine.

237. I am grateful to an anonymous reviewer for *Cryptologia* for drawing my attention to these later analogues of Leibniz's apparatus. The operation of the Leibniz machine is readily simulated on modern computers and I am grateful to Anastas Stoyanovsky for realizing this for my Apple desktop.

238. For details see Bengt Beckmann, "An Early Cypher Device: Fredrik Gripenstierna's Machine," *Cryptologia*, Volume 26, (2002), pp.113-123.

239. See B. C. W. Hagelin and David Kahn, "The Story of the Hagelin Cryptos," Cryptologia, vol. 18 (1994), pp. 204-242 as well as Bauer 1997 and Kahn 1967, pp. 422-25.

240. A I 2, p. 319: 28 February 1678.

241. While some early Enigma models provided for a printed output, the German military Enigma used during WWII was a glow-lamp version where the encripted letter was lit up. In this respect, it was closer to Leibniz's machine, for here also the output letters were mechanically indicated for copying by hand. Thus while in point of cryptographic operation Leibniz's machine is closer to that of A. G. Damm's aforementioned A-21, its mode of use is precisely that of the WWII Enigma. Enigma was usually operated by a three-person team: an input typer, a reader, and a recorder. The same arrangement would make for a highly efficient operation of the Leibniz machine. There are, however, some significant cryptographic differences between the Leibniz machine and Enigma. Unlike Enigma, the Leibniz machine is reflexive in allowing that a letter can be encrypted by itself. Moreover, Enigma has "reciprocity" in that whenever letter X is encrypted by another Y, then Y is encrypted by X, so that a given encypherment is self-decoding. The Leibniz machine does not have this feature.

242. A IV 4, p. 27.

243. In his memorandum for Duke John Friedrich of October 1679 (A I 2, p. 223) Leibniz says that he will "*an der Machina Arithmetica eifrig arbeiten lassen*" and then makes the marginal addendum, "and also the cipher machine" (item die Machina zum dechiffrieren)." However, we have no indications that he did so.

244. A IV 4, p. 27, notes. (This volume appeared in 2001.)

245. A I 2, p. 223

246. GPhil. IV 391 (Loemker, p. 409.)

247. *Monadology*, sect. 17.

248. For the details of Leibniz's position see J. E. H., Smith, *Divine Machines: Leibniz and the Sciences of Life* (Princeton: Princeton University Press, 2011).

249. *Monadology* sect. 64.

250. *Monadology* sect's. 78-79.

251. See Gilbert Ryle, *The Concept of Mind* (London; New York: Hutchinson's University Library, 1949).

252. Leibniz envisions a fundamental analogy between inference, calculation and encipherment (A II 1, p. 681: February 1679). See also A VI 4 A, p. 65-68

253. The paper has profited from constructive suggestions made by two anonymous referees for the journal *Cryptologia*. I am much indebted to Dr. Breger for constructive comments on this essay.

IV. LEIBNIZ'S OWN WORK AT DECIPHERMENT

254. Bodemann (*Handschriften*) registers them simply as *De Arte deciphratoria*, without any further commentary. I am grateful to Heinrich Schepers for transcribing some of this material from its often near-illegible manuscript text.

255. Analogously, in a May 1715 letter to the Imperial chamberlain Theobald Schöttel about personal matters Leibniz suggests using letters in lieu of numbers. (See I, *Transkriptionen, Januar-December 1715*, p. 221-2. His cipher machine doubtless resorted to this device. This practice, which goes back to ancient Greece, can of course serve with encipherment as well.

256. This tabulation is depicted in Philip Beeley, "Un de mes amis: On Leibniz's Relation to the English Mathematician and Theologian John Wallis" in P. Phemister and S. Brown (eds.), *Leibniz and the English-Speaking World* (Dordrecht: Springer, 2007), pp. 63-81. For the text at issue see Figure 3 on page 73.

257. I am grateful to Heinrich Schepers for providing me with a transcription of this manuscript page.

258. Note that Leibniz's alphabet omits the letters not needed in Latin, viz. j, k, y, and w.

259. Leibniz often used the astronomical/alchemical symbols ☉, ☽, and ♀ to indicate groupings. Compare, for example A VII 3, p. 361.

260. See Beeley 2007, pp. 70-71.

261. To Rudolf Ch. von Bodenhausen 30 December, 1693, III 7 oder 8.

262. Breger (2007) is entirely right when he writes: "Der Code [of the N-text] ist weit schwieriger als alle Geheimschriften die Leibniz oder seine Korrespondenten (soveil wir das zur Zeit wissen) benutzt haben . . . Nur nach wenige Stunden [Arbeit] erklärt er die Geheimschrift für nicht dechifrierbar, da nicht genug Material zur Verfügung steht (LH V VI, 4, Bl. 38 recto). Dies duerfte richtig sein, aber im Grunde haben seine Schlüsse nur gezeigt das es sich nicht um eine monoalphabetische Chiffre handelt." (Breger 2007, pp. 103-04).

References

Leibniz's writings will primarily be cited after the monumental Leibniz edition of the Deutsche Akademie der Wissenschaften in the manner of: Series + volume + page(s).

Other cited Leibniz editions include:

GPhil: C. I Gerhardt (ed.), *Die philosophischen Schriften von G. W. Leibniz*, 7 vol's (Berlin: Weidmann, 1875-90).

GMath: C. I Gerhardt (ed.), *Leibnizens Mathematische Schriften*, 7 vol's (Berlin and Halle [[with E]]: A. Asher, 1849-63).

Couturat, Opuscules: Louis Couturat (ed.), *Opuscules er fragments inédits de Leibniz* (Paris: F. Alcan, 1903).

The secondary references cited here include:

Bauer: Friedrich L Bauer, *Decrypted Secrets: Methods and Maxims of Cryptology* (Berlin: Springer, 1997). 3rd ed. 2002.

Beckmann, Bengt, "An Early Cypher Device: Fredrik Gripenstierna's Machine," *Cryptologia*, Volume 26, (2002), pp.113-123.

Beeley: Philip Beeley, "Un des mes amis: On Leibniz's Relation to the English Mathematician and Theologian John Wallis," in P. Themister and S. Brown (eds.), *Leibniz and the English Speaking World* (Dordrecht: Springer, 2007.

Breger: Herbert, "Leibniz und die Kyptographie," in H. Breger, J. Herbst, & S. Erdner (eds.), *Einheit in der Vielheit: Akten des VIII. Internationalen Leibniz Congress* (Hanover, 2006), pp. 101-05.

Couturat, *Logique*: Louis Couturat, *Le Logique de Leibniz* (Paris: F. Alcan, 1901).

Davillé: Louis Davillé, *Leibniz Historien* (Paris: F. Alcan, 1907).

de Leeuw (1999): Karl de Leeuw. "The Black Chamber in the Dutch Republic during the War of the Spanish Succession and its Aftermath, 1707-1715," *The Historical Journal*, vol. 42 (1999), pp. 133-156.

de Leeuw (2007). Karl de Leeuw, "Cryptology in the Dutch Republic," in de Leeuw and Bergstra, pp. 327-67.

de Leeuw and Bergstra: Karl de Leeuw and Jan Bergstra (eds.), *The History of Information Secrecy* (Amsterdam: Elsevier, 2007).

Ellis: Kenneth Ellis, *The Post Office in the Eighteenth Century* (London: Oxford University Press, 1958).

Hagelin, B. C. W. and David Kahn, "The Story of the Hagelin Cryptos," *Cryptologia*, vol. 18 (1994), pp. 204-242.

Hirsch, E. C, *Der Berühmte Herr Leibniz* (Muenchen: Beck, 2000).

Hoffman: J. E. Hoffman. "Leibniz und Wallis," *Studia Leibnitiana*, vol. 5 (1973), pp. 245-81. [Focuses on issues related to the calculus and contains no mention of cryptanalysis.]

Kahn, 1980. David Kahn, "On the Origin of Polyalphabetic Substitution," *Isis*, vol. 71 (1980), pp. 122-27.

Kahn: David Kahn, *The Codebreakers* (New York: Macmillan, 1967).

Leary: Thomas (Penn) Leary, "Cryptology in the 16th and 17th Centuries," *Cryptologia*, vol. 20 (1966), pp. 223–242.

Müller & Krönert: Kurt Müller and Gisela Krönert, *Leben und Werk von G. W. Leibniz: Eine Chronik* (Frankfurt am Main: Vittorio Klosterman, 1969).

Oakley, S. P., "The Interception of Posts in Celle: 1694-1700." Mark A. Thomson (ed.), William II and Louis XIV (Liverpool: University Press, 1968), pp. 95-116.

Persic: Peter Persic, "Secrets, Symbols, and Systems: Parallels between Cryptanalysis and Algebra, 1580-1700," *Isis*, vol. 88 (1997), pp. 674-92.

Rescher, Nicholas, "Leibniz's Machina Deciphratoria: A Proto-Enigma Machine," *Cryptologia*, vol. 36 (2012): A.

Rescher, Nicholas. *On Leibniz* (Pittsburgh: University of Pittsburgh Press, 2012). B.

Schnath: Georg Schnath, *Geschichte Hannovers im Zeitalter der neunten Kur und der englischen Sukzession: 1674-1714*, 4 vol's (Hildesheim & Leipzig: August Lax, 1938-82).

Schneegans, W., *Abt Johannes Trithemius und Kloster Sponheim* (Kreuznach: R. Schmithals, 1882).

Schumaker, Wayne, " *Johannes Trithemius and Cryptography*," Renaissance curiosa: John Dee's conversations with angels, Girolamo Cardano's horoscope of Christ, Johannes Trithemius and cryptography, George Dalgarno's Universal language (Binghamton, NY: Center for Medieval and Early Renaissance Studies, 1982).

Smith, Justin E. H., *Divine Machines: Leibniz and the Sciences of Life* (Princeton: Princeton University Press, 2011).

Smith: D. E. Smith, "John Wallis as a Cryptographer," *Bulletin of the American Mathematical Society*, vol. 24 (1917), pp. ???

Snyder, Laura J., *The Philosophical Breakfast Club* (N.Y.: Broadway Books, 2011). [Chapter 12 gives an account of Babbages work on codes.]

Stein, Erwin, *Die Leibniz-Dauerausstellung der Gottfried Wilhelm Leibniz Universität* (Hanover, 2006) [Exhibit catalogue available on the internet at http://www.uni-hannover.de/de/universitaet/leibniz/leibnizausstellung.]

Stephenson, Neal, The Baroque Cycle, 3 vols: *Quicksilver*, 2003, *The Confusion*, 2004, *The System of the World*, 2004 (New York: William Morrow).

Stix, Franz, "Zur Geschichte und Organisation der Wiener Geheimen Ziffernkanzlei," *Mitteilungen des Österreichischen Instituts für Geschichtsforschung*, vol. 51 (1937), pp. 132-60.

Strasser (1988): Gerhard F. Strasser, *Lingua Universalis: Kryptologie und Theorie der Universalsprachen im 16. und 17. Jahrhundert* (Wiesbaden: Otto Harrasowitz, 1988).

Strasser (1992): Gerhard F. Strasser, "Diplomatic Cryptology and Universal Languages in the Sixteenth and Seventeenth Centuries," in K. Neilson and B. J. C. McKerchen (eds.), *Go Spy the Land: Military Intelligence in History* (Westport, Conn: Praeger 1992), pp. 73–97.

Strasser (2007): Gerhard F. Strasser, "The Rise of Cryptology in the European Renaissance," in de Leeuw and Bergstra; pp. 277-325.

Türkel, Siegfried, *Chiffrieren mit Geräten und Maschinen* (Graz: Moser, 1927).

Vehse: Eduard Vehse, *Geschichte der Höfe des Hauses Braunschweig in Deutschland und England*, 5 vol's (Hamburg: Hoffmann und Campe, 1853).

About the Author

Born in Hagen, Germany in 1928, Nicholas Rescher came to the United States of America at the age of ten. He has been at the University of Pittsburgh since 1961 and is Distinguished University Professor of Philosophy. He has also served as Chairman of the Philosophy Department and a Director (and currently Chairman) of the Center for Philosophy of Science. In the course of a productive research career extending over six decades he has served as a President of the American Philosophical Association, of the American Catholic Philosophy Association, of the American G. W. Leibniz Society, of the C. S. Peirce Society, and of the American Metaphysical Society as well as Secretary General of the International Union of History and Philosophy of Science. He was the founding editor of the American Philosophical Quarterly. An honorary member of Corpus Christi College, Oxford, he has been elected to membership in the American Academy of Arts and Sciences, the Royal Asiatic Society of Great Britain, the European Academy of Arts and Sciences (Academia Europaea), the Royal Society of Canada, the Institut International de Philosophie, and several other learned academies. Having held visiting lectureships at Oxford, Constance, Salamanca, Munich, and Marburg, he has been awarded fellowships by the Ford, Guggenheim, and National Science Foundations. Author of some hundred books ranging over many areas of philosophy, he is the recipient of eight honorary degrees from universities on three continents. He was awarded the Alexander von Humboldt prize for Humanistic Scholarship in 1984, the Belgian Prix Mercier in 2005, and the Aquinas Medal of the American Catholic Philosophical Association in 2007. In 2011 he was awarded the premier cross

of the Order of Merit (Bundesdienstkreuz Erster Klasse) of the Federal Republic of Germany in recognition of contributions to philosophy and to German-American cooperation in this domain.

To acknowledge some extensive gifting and to recognize his fifty years of service to the institution, the University of Pittsburgh established in 2010 the substantial Nicholas Rescher Prize for Contributions to Systematic Philosophy.

Dr. Nicholas Rescher
Distinguished University Professor of Philosophy, University of Pittsburgh