Nicholas Rescher, *Leibniz and Cryptography: An account on the occasion of the initial exhibition of the reconstruction of Leibniz's cipher machine*. Pittsburgh: University Library, 2012. Pp. xiv + 96.

Reviewed by Philip Beeley, University of Oxford

Among the extensive array of letters and papers which constitute G. W. Leibniz's intellectual legacy, it is seldom that one finds items which provide an overview of the various philosophical, scientific, and technical interests which consumed his restless mind at any particular time. The most notable exceptions are the memoranda which he drew up in preparation for meetings with those who employed him or whose patronage he sought. In one such memorandum, drafted in the summer of 1688 in preparation of his audience with Emperor Leopold I in Vienna, Leibniz refers to what he calls his "Machina deciphratoria", a cipher machine which would enable a great ruler "to correspond concurrently with many ministers, using many virtually unsolvable ciphers".[1] As he tells us in an earlier version of the same document, the machine would be easy to use, being operated "much like using a musical instrument or clavicord, so that the text appears by touching the keys and only needs to be copied".[2]

The 1688 audience is one of only two known occasions on which Leibniz mentions his cipher machine in any detail, the other being some nine years earlier in a letter written to duke Johann Friedrich of Hanover in February 1679. After outlining various other achievements and projects, Leibniz discusses first the significance and usefulness of his calculating machine, his machina arithmetica, and then turns to "another beautiful machine" which, he says, "will serve to transform letters into ciphers and also to decipher them".[3] He adds that it will also carry out these operations "with great quickness and in a manner which is indecipherable to others". But perhaps the most important reason for developing the machine is that it will encourage the use of high level enciphering by those concerned with affairs of state:

> "For I note that most ciphers which one is accustomed to employ are easy to decipher; while those which are difficult to decipher are usually difficult to write; which has led to them being abandoned by persons who are busy. But by means of this machine an entire letter will be almost as easily transformed into ciphers and deciphered by him that has the machine, as it would be copied."[4]

However, in a memorandum for duke Johann Friedrich, written some six or seven

months later, the cipher machine is at first completely forgotten and only gets added – almost as an afterthought – as a marginal addition to notes containing his short progress report on the machina arithmetica.[5]

It is no mere coincidence that Leibniz spoke of both machines at the same time, for they were based on a common component, the Staffelwalze or stepped drum, otherwise known as the "Leibniz wheel". While the 1679 notes do not go into any technical detail on machina deciphratoria and therefore do not make the fundamental relationship clear, things are quite different in the 1688 memorandum. There, he reveals that the stepped drum conducts a carrying function, as it does in the calculating machine, but instead of effecting a shift to the next decimal it brings about a shift to the next alphabetic slide. The cipher machine, as presented, was revolutionary in another way, too. As Leibniz had already indicated to duke Johann Friedrich in 1679, his machina deciphratoria was operated not by means of discs, as in the case of Leon Battista Alberti's apparatus, nor by means of slats, as Athanasius Kircher had used, but rather it was to bring about polyalphabetical substitution with the utmost ease, employing a kind of keyboard "just as when one plays on a clavicord or instrument".[6] In a word, the task of encoding or decoding was to become almost fully automated. But there was another advantage, too: by means of mechanization, the whole process of enciphering and deciphering was to become fail-proof.

Leibniz's interest in cryptography went well beyond the conception of his machina deciphratoria. There was, for instance, also a strong mathematical motivation, for as he wrote on one occasion to his friend Thomas Burnett of Kemney, he considered the art of deciphering to be a "semi-mathematical" subject matter.[7] Already during his stay in Paris 1672-6, we find Leibniz convinced that the search for the rule of a series or of an array or "table" is to be compared with the search for the key of a cipher. Noting that one series might be part of another, and that in such cases it is necessary to choose that which is simplest and best accommodates the data, he recognizes an apparent relationship between the doctrine of discovery or hypothesis on the one hand and the practice of constructing or solving ciphers on the other hand. At that time he notes, too, that the Oxford mathematician and cryptographer John Wallis is likely to be man most suited to elucidate the relationship.[8] On other occasions, Leibniz draws a comparison between finding the key to a cipher and finding the solution to an algebraic equation.[9] Numerous remarks to this effect are to be found in his philosophical and scientific oeuvre. In notes written on Jean Prestet's *Elemens des mathematiques* (1675), for instance, he tells us that algebra

is like a game of chess and that the method one employs in both is similar to that used in deciphering.[10]

There is also a strong philosophical component to Leibniz's interest in cryptography, partly deriving from its mathematical significance. Thus, in his *Nouveaux essais sur l'entendement humain*, Leibniz also compares the discovery of the causes of natural phenomena, and that is to say, the discovery of explanatory hypotheses, with the the art of deciphering.[11] Furthermore, he describes the ars deciphrandi as being an integral part of his project of a general science (scientia generalis) and, at the same time, as representing an important part of the combinatorial art (ars combinatoria).[12] Above all, however, Leibniz believes the art of deciphering is able to throw light on and to contribute to the art of invention (ars inveniendi). As he explains in a note probably written in the summer or autumn of 1678, the ars deciphrandi constitutes in his eyes an area of discovery where analysis alone does not suffice.[13]

Alongside Leibniz's intellectual motivation there were also good political reasons for his being concerned in matters cryptographical. Of all the German principalities, duchies, and kingdoms, Brunswick-Lüneburg was transversed by undoubtedly the most significant postal routes for diplomatic and military affairs – at a time when only in a few regions of the Empire there was anything so much as could be described as an established infrastructure for epistolary communication. To facilitate the passage of letters along the routes, and particularly at crossover points, post-houses had been set up. But that was not all that was facilitated. In order that the state be well apprised of potentially useful information of political or military character, black chambers were also instituted, where letters, often written in cipher, could be opened, and their contents copied. Generally, such letters would then be re-sealed carefully and returned to the post house where they had been intercepted so that they could continue their journey: ideally, the recipient would be completely unaware that anything untoward had happened. To this end of intelligence gathering, the Brunswick dukedoms of Callenberg and Celle worked together. Under Hanoverian control they ran an elaborate and efficient cryptographic service. Indeed, the black chambers at Gifhorn and Nienburg were among the best in Europe and could rely on the experience of such noted code-breakers as Johann Albrecht Zachariae or his brilliant pupil Ludwig Ernst Neubourg.[14]

Some four years ago, the renowned philosopher and Leibniz scholar Nicholas Rescher began to occupy himself with Leibniz's work on cryptography. Working through the widely dispersed original sources on the topic, he was struck in particular by the accounts of the machina deciphratoria which are to be found in the 1679 letter to duke Johann Friedrich and the 1688 memorandum for his audience with the Holy Roman Emperor. Fascinated by Leibniz's sparse comments on his machine, and particularly by its asserted relation to the machina arithmetica, Rescher began to conceive how it might have functioned. He did not stop there. On the basis of his conceptualization, he elicited the help of engineer friends in producing a model of the cipher machine, in function if not in appearance. That machine was subsequently put on display in Pittsburgh as part of an exhibition on cryptography aimed at drawing attention to Leibniz's important contribution to that subject. The essay under review was published to coincide with the Pittsburgh exhibition.

Rescher's essay comprises four sections. In the first of these (3-34), he provides a broad overview of the place of cryptography in Leibniz's thought, drawing on the whole breadth of his surviving letters and papers. In this context, he also considers Leibniz's own work on cryptography as well as his relations (or rather absence thereof) to practicing code-breakers in the state of Brunswick-Lüneburg. The second section (35-48) contains in substance Rescher's conceptual reconstruction of Leibniz's machina deciphratoria.[15] In this section, he puts forward the thesis that Leibniz's cipher machine was some two hundred and fifty years ahead of its time and that it can in many ways be seen to anticipate the technology employed in the Enigma, famously used by the German Abwehr (counter-intelligence) during Second World War. In the third section (49-60), Rescher presents what he calls "a photographic contextualization" of Leibniz's machina deciphratoria of the 1670s, in which in its reconstructed form it takes its place alongside other cryptographical devices, ranging from Alberti's cipher disc to the mark II Colossus at Bletchley Park. Finally, in the fourth section of his essay (61-75), Rescher devotes fifteen pages to analysing Leibniz's most extensive manuscript on deciphering as a means to providing the reader with some insight on Leibniz's abilities as a cryptographer. Fittingly, Rescher calls this section "Leibniz's own work at decipherment".

Of the four sections, the first is by far the most useful. Rescher leads his readers to many of the significant places in Leibniz's oeuvre where cryptographical matters are discussed. He elucidates Leibniz's comparison of the deciphering of a cryptogram with the method of forming a hypothesis, just as he describes and

explains the role played by ciphers in the correspondence with Johann Daniel Crafft, Johann Sebastian Haes (Haas), and Jobst Dietrich Brandshagen. He also provides a useful account of Leibniz's dealings with John Wallis on cryptography, the salient points of which are summarized in what he calls "The chronology of Leibniz's Wallis project" (20).

However, even in this section, where Rescher is on relatively solid, if not exactly new ground, all is not well. The author asserts that Leibniz's fascination in cryptography was engendered by his reading works of the English virtuoso and founder member of the Royal Society John Wilkins, such as the *Essay towards a Real Character, and a Philosophical Language* (1668) and his earlier *Mercury: or the Secret and Swift Messenger* (1641), and he also suggests that Wilkins "evoked much contemporary interest in cryptography" (6). He provides no evidence for these bold claims, nor would he be able to do so, for there is absolutely no historical foundation to either of them. Not for the last time in his essay, Rescher reveals an astonishing lack of understanding of the political and intellectual tradition in which the practice of cryptography in the early modern world was situated. The suggestion that Wilkins evoked an interest in cryptography is absurd when viewed against the background of the widespread use of ciphers in private, political, and military correspondence throughout the seventeenth century. During the English Civil Wars, for instance, popular gazettes of various political hues regularly published deciphered letters as a means to revealing the supposedly true (and sometimes truly fictional) aims of opposite parties. Ciphers and deciphering were part of daily political life.[16] On another occasion, Rescher fails to take account of the rich history of concealment in early modern scientific discourse. For example, he cites Christiaan Huygens's employment of an anagram in order to conceal core features of his solution to Johann I Bernoulli's catenary problem, posed to contemporary mathematicians in 1696. While this is certainly correct, Rescher does not recognize that some twenty-five years earlier Huygens had proposed to the Royal Society that ciphers be used in intellectual commerce in order to protect scientific discoveries until such time as they were ready to be published.[17] The background to that proposal was of course the increasing number of disputes over priority in discovery which threatened to harm the open exchange of ideas in the wider Republic of Letters.

Unfortunately, as a record of Leibniz's deliberations on cryptography and his intellectual commerce with contemporaries on the topic, Rescher's account is marred by far too many historical inaccuracies. For instance, he tells his readers that Wallis in order to keep Leibniz at bay in his persistent demands to be supplied

with information on his methods of deciphering "sent him a copy of his paper in the *Acta Eruditorum*" (16; repeated 75). No such article was ever printed. Wallis did send Otto Mencke an example of his deciphering work, namely a French numerical substitution cipher with various stages of its solution, but the editor of the German ephemerides refused to print the material in his journal and sent it to Leibniz instead. Elsewhere, Rescher states that Wallis's grandson, William Blencowe, succeeded him in 1702 (21). This is also not correct. Wallis and Blencowe were jointly appointed to the post of decipherer in the office of the Secretary of State in the year of the accession of Queen Anne. Moreover, this was the first time at which an official post of that nature was created.[18] After Wallis's death in 1703, Blencowe continued working alone before committing suicide in 1712. Rescher is therefore also wrong when he writes that Blencowe was England's "first official decipherer" (30). That honour accrues equally to the Oxford mathematician and to his grandson.

In many ways, Rescher's essay appears to have been hastily written. Too little of the historical narrative is based on sound readings of original sources, and the overall quality of the presentation leaves much to be desired. Basic editorial mistakes abound and are far too numerous to be listed in their entirety here. For example, Leibniz's short paper entitled *Praecepta artis deciphratoriae*, written in the mid-1680s, is introduced and summarized on page 8, despite this having already been done, although admittedly in somewhat different wording, a page earlier. It is re-introduced yet again on page 10, and for a fourth time on page 66. Nor is this an isolated case of repetition. On page 32, Rescher introduces the Benedictine polymath Johannes Trithemius and describes his pioneering work on polyalphabetical encipherment, only to do the same thing again, and in almost identical words, on page 37. On page 32, the important passage on the cipher machine in Leibniz's letter to duke Johann Friedrich of February 1679 (incorrectly cited as the memorandum of the same year) is quoted in extenso in French. Three pages later, on page 36, precisely the same passage is quoted again, but this time in English translation. A passage on cyclic alternation on page 42 is repeated verbatim on page 43, and so on.

It is not at all clear what kind of audience Rescher is seeking to address. On the face of it, his essay has been produced to accompany the exhibition, at which Leibniz's reconstructed cipher machine was first presented to the public. Indeed, all of the illustrations in the small volume are given their corresponding display numbers from that exhibition. This fact would suggest that the essay is intended to

reach an educated general audience, but if that is the case it is hard to understand why Rescher does not translate all the passages from Leibniz's letters and papers which he quotes in French or Latin. More to the point, one wonders why he does not explain or so much as provide a glossary for the many technical terms from the practice of cryptography and the construction of cryptographical machines which he employs. The long section on Leibniz's mechanistic philosophy, well written as it is, also appears out of place (44-8).

When the editors of the political series (IV) of the Academy Edition of Leibniz's *Sämtliche Schriften und Briefe* weighed up all the available evidence, they reached the conclusion that it is not known whether Leibniz's cipher machine was ever completed or constructed.[19] Rescher is not so prudent. Instead, he uses his conceptual reconstruction, and the model built on the basis of this, as a vehicle in order to evaluate Leibniz's supposed achievements in the field of cryptography. Of course, there is a certain interest in witnessing the result of this reconstruction, but like the reviewer, many of those reading Rescher's essay will no doubt question the extent to which the machine before their eyes can justifiably be called Leibniz's cipher machine or ponder how much of its design has benefitted from hindsight.

At times, Rescher speaks in relatively moderate terms of the nature of the achievement constituted by the machina deciphratoria, telling his readers that it "effects" – more appropriately, he should say "would effect" – a polyalphabetical substitution of the same sort as Alberti's disc or Kircher's cipher slides, but eliminating "all the laborious (and error-inviting) physical letter-matching" (41). In this sense, the main benefit provided by Leibniz's cipher machine over its antecedents would be that it renders the entire process of encipherment "automatic and fail-proof by mechanization". Thus, as Rescher with some justification suggests, Leibniz marks the transition from cryptographical devices to cryptographical machines (41). Unfortunately, he does not stop here, but proceeds to compare his reconstruction with cipher machines used during the First World War, and ultimately throws all caution to the wind by comparing it with the Enigma machine. Of course, "there are differences", but in their basic conception, he tells us, "the two machines are kinsmen" (43-4). Rescher therefore has no compunction in describing Leibniz's cryptographical machine as "a proto-Enigma in its generic modus operandi" (44). This is quite a claim, given how little Leibniz actually writes about his conception.

One is reminded by Rescher's claims, based as they are on sketchy ideas contained in two short passages in Leibniz's oeuvre, of the heroic age in the history of science, when it was always important to show how "great men" were ahead of

their time. How little such approaches have in common with the contextual richness of good intellectual history nowadays.

In contrast to the prudence of the editors of the Academy Edition, Rescher is convinced that Leibniz's machina deciphratoria was at some time constructed and he even goes so far as to call it Leibniz's "most closely guarded secret" (44). Of course, Rescher has no evidence to back up this bold assertion. Moreover, one wonders why the machine should have been kept so well concealed if it was able to fulfil all the potential which Rescher ascribes to it. There is no plausible reason, and Rescher certainly does not supply one, why Leibniz should not have sought to have a working model built and presented at court, assuming of course that its conception had been as well developed as Rescher evidently assumes it to have been. Would such a machine not have enhanced Leibniz's standing immeasurably in Hanover in the late 1670s, or at the imperial court in Vienna nearly a decade later? Tellingly, Rescher neither raises this question, nor does he attempt to answer it.

As Rescher recognizes, all the available evidence suggests that Leibniz was only marginally involved in the practice of cryptography (24). The few examples which exist are entirely in his correspondence. In the already mentioned epistolary exchanges with Johann Daniel Crafft, we find that his well-travelled friend proposes employing a monoalphabetical cipher based on the keyword LEIBNYZ already early on, in May 1672.[20] However, in their correspondence only individual words or phrases were encrypted, never entire communications (25). In later years, Leibniz used his own LABYRINTHUS code in letters to Crafft to the same purpose.[21]

Similarly, in his epistolary commerce with the Jesuit missionary Claudio Filippo Grimaldi in Beijing, Leibniz encouraged the use of the LABYRINTHUS code in view of the ever-present danger of their letters being intercepted during the long journey they had to take both over land and across open seas.[22] Interestingly, Leibniz recommends using ciphers only sparingly, since as he knew from his own experience decipherment becomes the more difficult the less cipher text one has to work with. He also points out to Grimaldi that occasional errors in enciphering could be advantageous, as such mistakes created additional barriers to code-breaking.

Rescher is to be applauded for the considerable pains he takes to elucidate the significance of Leibniz's only known work on deciphering of significant length, namely the Hanover manuscript LH V 6, 4, of which up to now only one folio has been edited in the Academy Edition.[23] Part of the manuscript is concerned with a complex numerical code, which Rescher calls the N-text, whose origin is unknown.

Possibly it was sent to him by one of his many correspondents, but Leibniz gives us no clues. Be that as it may, despite making a considerable effort to solve the cipher, and no doubt also expending considerable time in this attempt, Leibniz was unable to break the code. Was this experience typical of Leibniz's ventures into the world of deciphering? Rescher believes it was and furthermore surmises that these failures might well have persuaded Leibniz that he had insufficient skill to succeed in the discipline of code-breaking. Conversely, such experience would have only served to increase his admiration for Wallis, who had demonstrated on numerous occasions his prodigious ability to solve even the most difficult numerical substitution ciphers which the French court had to offer (75). However, here again, Rescher falls into error. He claims, namely, that Wallis eventually fulfilled Leibniz's often expressed wish that he divulge something of the cryptographical methods he employed. He did no such thing. As Wallis recognized, he would have been foolhardy indeed if he had made his deciphering techniques widely known, for such knowledge would inevitably have helped those whose task it was to foil him. A good decipherer never gives away the tricks of his trade.

It is surely a clear reflection of Leibniz's awareness of his own limitations as a cryptographer that so few of his surviving letters and papers are devoted to its practice. But how is this fact to be squared with the cipher machine, the machina deciphratoria which according to Rescher was Leibniz's great secret, firmly kept under wraps for most of his life? The obvious answer is of course that it cannot be squared at all: the Leibnizian machine for all its theoretical brilliance, in all probability never proceeded beyond its incomplete conception. For Rescher, having built up the machine to be a proto-Enigma, such a conclusion is not available. Instead, he is forced to conclude that Leibniz's apparatus was unsuccessful because he "underestimated the complexities at work in the diplomatic practice of his day" (75). Does he mean the skilled cryptographers already at work in Hanover's black chambers? Surely not, for their task was essentially one of code-breaking, not of creating ciphers, the prime function of the cipher machine. The complexities Rescher refers to were perhaps the sophisticated codes produced by French cryptographers working in the tradition of the legendary Antoine Rossignol in Paris; the kind of ciphers with which Wallis was confronted, sometimes almost on a daily basis. But Rescher cannot have it both ways. If Leibniz's machina deciphratoria was all he makes it out to be, a proto-Enigma indeed, why should this have been a problem? It would after all have provided an easy and efficient way of constructing impenetrable ciphers.

Nicholas Rescher's essay is the most ambitious attempt yet to provide a comprehensive account of Leibniz's interest in and creative work on questions of cryptography. Moreover, it is the first scholarly investigation devoted entirely to that topic. Rescher is to be congratulated particularly on his efforts to conceptualize and recreate Leibniz's cipher machine. Undoubtedly, if that machine had been realized in the form in which Rescher exhibited it in Pittsburgh, it would have represented a ground-breaking achievement. But can the apparatus described in *Leibniz and Cryptography* justifiably be called Leibniz's machine? The numerous inconsistencies which Rescher's account entails tend to confirm the reviewer's belief that his speculation on the nature of that machine and its capabilities is fundamentally flawed.

Philip Beeley
Faculty of History
University of Oxford
George Street
Oxford OX1 2RL
United Kingdom
philip.beeley@history.ox.ac.uk

Notes

[1] Leibniz, *Ausführliche Aufzeichnung für den Vortrag bei Kaiser Leopold I* (second half of September 1688), A IV, 4, 68: "Aus gleichen principio [sc. as the Machina Arithmetica] wiewohl viel leichter, habe ich eine Machinam deciphratoriam vor hohe Personen ausgefunden. Ist eine kleine Machinula die leicht bey sich zu führen. Darauff kan ein großer herr viele fast unauflößliche Ciphern zugleich haben, und mit vielen Ministris correspondiren; weilen aber sowohl die stellung in Ziphern als das deciphriren mühsam, so bestehet die facilitat darinn, daß man die gegebene Ziphern oder buchstaben nur greiffen darff als wenn man auff einem clavicordio oder Instrument spielte, so kommen die begehrten augenblicklich herauß und stehen da; durffen denn nur abgeschrieben werden."
[2] Leibniz, *Aufzeichnung für die Audienz bei Kaiser Leopold I* (August/September 1688), A IV, 4, 27: "Dergleichen sind meine Machina Deciphratoria damit ein potentat mit vielen ministris, in unterschiedenen ziphern gleich correspondiren, und ohne einige muhe entweder die zipher die er schreiben will, und den verstand

deßen so ihm in zipher zugeschickt wird gleichsam wie auff einem musicalischen instrument oder clavicordio greiffen könne, also daß es gleich mit berührung der clavir darstehe, und nur abcopiert werden dürffe."

[3] Leibniz to Johann Friedrich, February (?) 1679, A I, 2, 125: "Cette machine d'Arithmetique m'a fait songer à une autre belle machine qui serviroit à mettre les lettres en chiffres, et à les dechifrer: et cela avec une tres grande promtitude et d'une façon indechiffrable aux autres."

[4] ibid: "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 lettre entiere seroit presque aussi aisément mise en chiffres et dechiffrée par celuy qui a la machine, que copiée."

[5] Leibniz for Johann Friedrich, October 1679, A I, 2, 223.

[6] Leibniz, *Ausführliche Aufzeichnung für den Vortrag bei Kaiser Leopold I* (second half of September 1688), A IV, 4, 68. See also Leibniz, *Kurzfassung einiger Ausführungen vor Kaiser Leopold I* (August/September 1688), A IV, 4, 45.

[7] Leibniz to Burnett, 1/11 February 1697, A I, 13, 551: "Car c'est [sc. le déchiffrement] une matiere encor demy-mathematique."

[8] See Leibniz, *De methodo quadraturarum usu in seriebus*, A VII, 3, 253, and the reviewer's 'Un de mes amis. On Leibniz's relation to the English mathematician and theologian John Wallis' in: *Leibniz and the English-Speaking World*, ed. P. Phemister and S. Brown, Dordrecht: Springer 2007, 63-81, especially 68-9, 72-5.

[9] Leibniz to Tschirnhaus, June 1678, A III, 2, 412: "Nam quod radix in Algebra, id Clavis in Cryptographia Divinatoria."

[10] Leibniz, *Zu Prestets Elemens des mathematiques* (December 1675-January 1676), A VII, 2, 806: "L'algebre est comme le jeu des echecs: il y faut mettre en usage mille adresses, aussi bien que dans l'art de dechiffrer."

[11] Leibniz, *Nouveaux essais sur l'entendement humain* IV, 12, §13, A VI, 6, 454-56.

[12] Leibniz, *De synthesi et analysi universali seu arte inveniendi et judicandi* (summer 1683-beginning of 1685), A VI, 4, 545.

[13] Leibniz, *De arte inveniendi in genere* (summer-autumn 1678?), A VI, 4, 80-1: "Exemplum ubi Analytica sola exitum reperire non potest, in arte deciphrandi, aliisque casibus ubi condendae sunt Tabulae et percurrendae, cum scire volumus an datus numerus sit primus; et examinamus divisores possibiles ordine."

[14] See S. P. Oakley, 'The interception of posts in Celle, 1694-1700', in: *William III and Louis XIV. Essays 1680-1720 by and for Mark A. Thomson*, ed. R. Hatton and

J. S. Bromley, Liverpool: Liverpool University Press 1968, 95-116; G. Schnath, *Geschichte Hannovers im Zeitalter der neunten Kur und der englischen Sukzession 1674-1714*, 4 vols, Hildesheim and Leipzig: August Lax, 1938-82, II, 354-5

[15] The subtitle 'A Seventeenth Century Photo-Enigma' (35) should of course read 'A Seventeenth Century Proto-Enigma'.

[16] See the reviewer's 'Breaking the code: John Wallis and the politics of concealment' (forthcoming).

[17] See Huygens to Oldenburg, [27 January 1668/9]/6 February 1669, in: *The Correspondence of Henry Oldenburg*, ed. A. R. Hall and M. B. Hall, 13 vols, Madison, Milwaukee, and London: University of Wisconsin Press et al. 1965-86, V, 360-1.

[18] See *Officials of the Secretaries of State 1660-1782*, ed. J. C. Sainty, London: Athlone Press 1973, 59, 66, 114.

[19] See the editors' notes on Leibniz, *Aufzeichnung für die Audienz bei Kaiser Leopold I* (August/September 1688), A IV, 4, 27: "Ob Leibniz [...] die Absicht, eine solche Maschine zu konstruieren, weiter verfolgt oder sogar in die Tat umgesetzt hat, ist noch nicht bekannt."

[20] See Crafft to Leibniz, Crafft to Leibniz, 6/16 May 1672, A I, 1, 405-6. Crafft introduces the LEIBNYZ code in his letter to Leibniz of 25 November/[5 December] 1672, A I, 1, 406. See also his letter to Crafft of 4/[14] July 1674, A I, 1, 421-3.

[21] See for example Leibniz to Crafft, 5/[15] May 1694, A III, 6, 79.

[22] Leibniz to Grimaldi, mid-January/beginning of February 1697, A I, 13, 527-8.

[23] Leibniz, *Praecepta artis deciphratoriae*, A VI, 4, 1203-6.