

Eric Sams

Cryptanalysis and Historical Research

© *Archiviaria* 21, Winter 1985-86 (pp. 87-97)

In 1641 John Wilkins, a young chaplain later to be Bishop of Chester and a founder of the Royal Society, published the first English textbook on cryptography, *Mercury, or the Secret and Swift Messenger, showing how a Man may with Privacy and Speed communicate his Thoughts to a Friend at any Distance*. Most of his proposals were more ingenious than usable; but his book was timely. Within months of its publication the Civil War broke out and enciphered writing was used on a more extensive scale than ever before. Wherever the keys to these ciphers have been lost or mislaid, modern historical research may be frustrated.

Some fitful progress has proved possible: for example, where a contemporary decipherment yields a key which is also found to fit other texts in the same cipher which have not survived *en clair* (as with some of the letters of Queen Henrietta Maria published by M. Green in 1857). Similarly, access to one text *en clair* may permit the decipherment of a whole correspondence, a possibility to which contemporaries themselves were alive. Thus when the Parliamentary forces captured the drafts of some Royalist cipher letters, they were soon able to publish the most discreditable passages from other such correspondence. There is now, however, little likelihood that the archives will yield similar windfalls for the modern researcher.

But the spread of cryptography stimulated its countermeasure – cryptanalysis, that is, the methodical application of techniques which permit decipherment without the key. In modern times this has become first mechanized and then computerized in ways well beyond the technical or financial resources of the average historian. But far simpler methods can yield effective and even impressive results. Thus in the nineteenth century a few dedicated full-time cryptanalysts made important contributions to the elucidation of state papers. But historical cryptanalysts are today a rare if not extinct species; and there is evidence that historians both in Europe and in America have now dug down in the archives to an apparently impenetrable bedrock of documents in cipher.

So the answer to the problem of unsolved ciphers still left in the archives is for research workers to acquire the relevant skills and to do it themselves. Uninstructed personal endeavour in this field must often have led to total frustration, or at best to disproportionate delay. A recent example is the cipher diary kept by Beatrix Potter between 1881 and 1897, left unstudied until 1952 and not solved until 1958 (by Leslie Linder) - although a competent cryptanalyst could have broken the system in about half an hour.

This article offers general advice on the compilation of the basic equipment which the historian will need should he set out to elucidate an enciphered document. It takes a whole library to encompass the history and practice of cryptography. But it happens that one particular cipher-system dominated European diplomatic and military correspondence for several centuries. The reason for its dominance is itself instructive. In *The Advancement of Learning* Francis Bacon defined the main virtues of ciphers "whereby they are to be preferred" thus: "that they be not laborious to write and read" and "that they be impossible to decipher." But these aims were already antithetical; and it was precisely the fruitful tensions between convenience on the one hand and security on the other that gave rise to the use of number-cipher throughout Europe from the sixteenth century onwards.

Ciphers operate by obscuring the most easily recognizable characteristics of the written word. Decryption (i.e., decipherment without the key) relies on using those patterns of language which the encipherer has not destroyed to provide the foundation for a reconstruction of the plain text. Convenience of encipherment favours the method of substitution, in which each letter of the message loses its usual identity and is regularly replaced by another symbol. Classically the method may be simple and formulaic, e.g., for A write D, for B write E, and so on.

Suetonius said that such alphabetical displacements were used by Julius Caesar, and whatever the truth of this story the results are still known as "Caesars." During the Middle Ages substitution more often involved the use of specially invented symbols; and the more cabalistic these looked the better. But such systems were soon seen to be insecure because all letters in all languages behave in predictable and hence identifiable ways. Thus the most frequent symbol used would be that representing E, since this letter is commonest not only in English (and especially in *olde Englishe*) but also in French, German, Italian, and Spanish.

To render this substitution less vulnerable the encipherer has to go further than merely disguising the identity of the plain text letters. So extra obscurity may be added by: the allocation of more than one equivalent to each letter; what Bacon calls "intermixtures of nulls and non-significants;" additional symbols for two or three-letter groups or common words or proper names; the avoidance of division into separate words. While such devices are well designed to camouflage linguistic patterns, and particularly the letter frequencies, they require more symbols than the alphabet provides.

The practical alternative first adopted (for example in the diplomatic ciphers associated with the name of Sir Francis Walsingham) was to supplement the alphabet with a plethora of invented signs. Their often arcane appearance endeared them to nineteenth-century romancers, and variations were used by Poe, who employed a selection of printer's signs in *The Gold Bug*, and Conan Doyle, who adopted arbitrary patterns in *The Dancing Men*. But in real life the labour of inventing and writing unfamiliar symbols soon rendered Walsingham's picturesque systems obsolete. The only set of equivalents that can provide sufficient variety and yet is familiar enough to be conveniently written is the series of integers; hence the dominance of number-ciphers.

These systems may be made as simple and formular as "Caesars" for the sake of convenience (e.g., E may be 30, 31, and 32), or else randomized for the sake of security (e.g., E may be 3, 29, 45, 61, and 89). In either case, by the late sixteenth century it is usual (but by no means invariable) for a one or two-figure number to represent single letters while three-figure numbers stand for syllables, common words, or proper names. This three-figure usage, properly called code rather than cipher, is often arranged in alphabetical order and is to that extent vulnerable to analysis.

The cipher component (i.e., replacement of letters by substitutes) is in principle entirely vulnerable, given a sufficient length of message. As a rule of thumb, the convenient minimum length may be calculated as about twelve times the number of different symbols used; but texts where the ratio is much smaller will be accessible to the skilled analyst. Very few, if any, of these ciphers are, technically speaking, indecipherable - although insufficient material may render them so for practical purposes - and Poe's dictum applies to them as it does not to some modern systems: "It may well be doubted, whether human ingenuity can construct an enigma of the kind which human ingenuity may not, by proper application, resolve."

A wish to exercise such ingenuity is the prime qualification of the amateur cryptanalyst. All researchers have the powerful incentive of contributing to knowledge by being the first solver ever, with added bonuses of possibly significant discovery and personal satisfaction. Second (but only second) comes the right cast of mind. The latter was defined more than thirty years ago by the psychologists who advised on recruitment to the British cryptographic service, which played so vital a part in the Second World War. The selection system was designed to identify general linguistic and problem-solving ability enhanced by special aptitudes for, *inter alia*, mathematics, chess, crosswords, and orchestral score-reading.

All such skills can be acquired in some degree. Cryptography is essentially a discipline, despite its important intuitive aspects. Its basic principles have been lucidly set out in elementary and advanced cipher manuals. The first essential is to know the cipher's background and provenance. Here the research worker has a clear advantage over the cryptanalyst because of his knowledge of the sources, including the prime clue of the probable subject-matter of the text in question. But he will need suppleness of mind to avoid the frustration of the *idée fixe*. As he becomes more familiar with material from one source, the researcher will be able to recognize and employ to his own advantage the foibles of the encipherer - his preference for certain systems, say, or his penchant for protecting the beginning and end of his messages with many nulls, perhaps leaving the main body of the text comparatively vulnerable.

The next step is to identify the language used. This knowledge can offer unexpected insights. Thus a number-cipher in the hand of Abraham Cowley was used for two letters to Charles I, one from Baron Jermyn and the other from Henrietta Maria. (The cipher was not one of those elucidated in the standard edition of her correspondence.) The frequency and pattern of the numerals used in the two texts differed in such a way as to suggest that the same cipher-system, probably designed for use in English, was being used to convey messages in two different languages - English and French. One significant clue was an apparent affinity between several cipher numerals that could only have arisen from the need to encipher the letters Q and U. A French cipher system could be expected to disguise this common (in French) digraph; but it is rare in English and the system available to Cowley accordingly did not provide any special camouflage. The tentative identification of these letters began the chain of reasoning that led to the recovery en clair of the French text, the much less accessible English text, and to the discovery of a key which has been found to fit other unsolved cipher correspondence of the period.

To identify such patterns and combinations it is always essential to count and analyse the whole cipher-text, as one of the preliminary steps, in as much detail as possible. Index cards provide a serviceable method.

Take as an example of analysis a phrase from a letter of the exiled Charles II intercepted by agents of the Commonwealth and published in the papers of Thurloe, Cromwell's chef de cabinet (State Papers, Volume 111, page 76): "Upon the whole matter let me heare from you 114.20.28.41.66.25.63.30.32.68.31.44.167, in such a manner as may at least fully instruct me of what I may looke for." Divide each index card notionally into a grid suitable for entering the numbers used (10 x 10 for the two-figure cipher, with space for three-figure groups as necessary, is a suitable framework). On the card headed 1 14 write 20 in the appropriate cell; on the card headed 20 write 28; and so on (using dots for repetitions) throughout the whole message. With increasing experience the practitioner can readily devise more complex and informative systems for intractable texts. The emerging patterns of frequency and juxtaposition, though no doubt obscured by the devices already described, are nevertheless likely to permit certain inferences – for example that two or more different numbers throw up patterns sufficiently analogous to suggest that they represent one and the same letter.

The card index system will suggest letter relationships which may then themselves be the subject of further close analysis, and the most unpromising looking feature can in this way become the fulcrum for a solution of resistant material. At a crisis in his career, during a quarrel with Charles I, Prince Rupert wrote an often quoted letter, the greater part of which is in cipher, to his trusted friend Will Legge, the governor of the Royalist stronghold Oxford. Rupert seems to have been at pains to keep most of his meaning secret and used his cipher system skilfully to break up the texture of his message to an exceptional degree. The systematic analysis of such letter relationships as repetitions and reversals has, however, recently led to the decryptment of the text.

There are many other examples of detailed analysis. As with Rupert's cipher, their general rules will need to be modified or supplemented (in ways far too detailed and varied to be dealt with here, even in summary) by experience and practice with the cryptography of a given country and period. In these circumstances the researcher is well placed to supplement analytical methods by inference from extant plain texts, for example, to try to find the "probable word" hidden beneath the cipher.

Thus the cipher letter from Henrietta Maria to Charles I referred to earlier was found to include her customary and touching salutation "mon cher coeur," which usefully confirmed some tentative identities between cipher and plain text. In all contexts the process of inference, hypothesis, and test by cross-checking is crucial.

In the example from Thurloe's papers cited above, the reasoning (much simplified for the sake of brevity and cogency) might run thus: "Let the language be English. The look of the frequency count strongly suggests a formular cipher, with consecutive groups of numbers representing letters in alphabetical order. Most frequent are the early 30s; try them as E. Hence E E 68 E. So 68 is probably a consonant. T seems plausible in itself and about the right distance down the alphabet. Then 63 and 66 might well be R and S; which would give S 25 R E E T E. So 25 looks like C; try D I S C R E E T E. That yields D for 28, which assorts well with 25 as C. Then 20 looks like A; and if 41 is I, then 44 suggests K (bearing in mind that in the English seventeenth century I and J are, like U and V, identical). Then the request must be for 'a discrete key,' making 167 = EY; so the three-figure groups are probably also in alphabetical order and 114 will be BY (rather than IN or WITH)."

In practice, this process was reinforced and counter-checked at every stage by the substitution of proposed equivalents into the main body of cipher text, with encouraging results. So the request was in fact an indiscreet betrayal of the key actually used. That degree of naivety in cipher and encipherer alike, together with the failure of the interceptors to decipher the text, may suggest a certain lack of awareness of security and its techniques both in Charles II's court and Thurloe's cabinet; and the study of historical cryptography might permissibly include analogous inference from the type and use of cipher-systems.

Similar analysis, and "probable word" formulae such as dates and subscriptions, can also provide vital points of entry into the unread shorthand systems which lie in the archives alongside cipher. For example, the shorthand used by William Clarke as secretary to Cromwell and his generals in Scotland has been declared by stenographic experts to be unreadable. But a cryptanalytic approach proved more fruitful; a frequency count and other analyses enabled some 300 equivalents to be identified, so that the whole system is now in principle readable wherever it is legible. It turns out to be similar to shorthand used by Pepys; Shelton's *Tachygraphia* (six editions were published between 1620 and 1641) was no doubt the common source book.

The disciplines of cryptanalysis can be taxing, and the tasks arduous, but the expenditure of time and effort is hardly greater than that required by the more cryptic of crosswords, and there is always the possible bonus of genuine and fruitful discovery. Such results are surely well within the competence of the average historical researcher, who already possesses the background knowledge and has only to acquire some relevant technique and dispel some irrelevant mystique. The only other needs are photocopied holographs (never transcriptions), plenty of cards and paper, sharpened pencils and wits,

technical information or experience, reasonable confidence, plenty of patience, and a modicum of good fortune.

Of course some archives are likely to remain dark and impenetrable. William Friedman, one of the world's greatest cryptanalysts, spent many a fruitless hour on the Voynich manuscript, attributed to Roger Bacon, which is fluently written in a natural-looking yet wholly unintelligible language. The British Library has a photocopy, and also owns an original volume of equally obscure manuscript which begins by saying in plain English that no one will ever unravel the meaning of what follows. So be it; many tracks lead into such caves. but none ever come out. The true treasure-chests are much more likely to be those which clearly once had real keys, later lost or mislaid. Such cases can often be opened by the simplest tools of cryptanalysis, such as counting and classification. Thus Archbishop Laud in a letter of September 1636, also in the British Library, uses substitution cipher in an artless way. He writes *en clair* "Pray God some have not a hand in this that you little suspect, for I hear there is," and he then concludes in cipher, "a successor designed." The sample word 71 54 33 32 14 72 71 49 70 ("successor") illustrates both his system and its basic simplicity.

State ciphers were more sophisticated, but essentially similar and hence vulnerable to systematic scrutiny. The longwindedness of Henrietta Maria and Charles I proved very helpful in breaking their cipher letters. Hers to him of January 1646, now in the Public Record Office, is eloquent of their confusion and despair on the personal as well as the political plane. Her customary and touching salutation remains "mon cher coeur;" but she threatens to retire to a convent if her efforts on her husband's behalf are not received more appreciatively. His letter of January 1643, now in the British Library, turns out to be a fervent appeal to his envoy in Paris for "ten thousand good armes such as wee shall chuse there to be brought and provided for our use forthwith freely and without any hinderance lett or trouble to be brought over hither to such a place in this our kingdom as wee shall direct," and so forth. However, these negotiations seem to have moved at an even more deliberate pace than the royal prose.

In later centuries private diarists continued to devise their own personal cipher-systems, which provided effective cover then and later. Thus the National Library of Scotland has a diary with previously unread cipher-entries alluding to, for example, the Duke of Newcastle's appointment to the Treasury in 1754 and the disquieting rumour that "Mr Fox wanted to have some of the secret service money and to see the plans of the elections." Both applications were rejected. So were the amorous appeals of the London worthy Henry Kirk, whose secret journal ca. 1818 has long remained untranscribed in the British Library, though its cipher is none too demanding and the excerpts I have decrypted are by no means barren of human or historical interest.

Both these journals, as it happens, use cipher-symbols akin to those of contemporary shorthand, perhaps with the aim of baffling any interceptor. Conversely, the early shorthands themselves were quite like some contemporary cipher-systems. One main difficulty in gaining access to the former lies not in the absence of keys but in the presence of a huge and jangling bunch of them. In the last four centuries, at least 350 different shorthands have been published in England alone, and many others will have circulated in manuscript form. Further, each such system could be altered or adapted at will by each user. Even the printed manuals were often revised by their authors in later editions, or plagiarized by others. So it is usually impossible to begin by identifying the system and consulting the source-book.

It is however entirely feasible, given enough shorthand text, to decrypt the system by means of analysis and induction, without ever seeing the published manual or indeed knowing of its existence. The greatest triumph of that approach, namely the elucidation of the Pepys shorthand diaries by William Wyndham, Lord Grenville, in 1818, has still not had its full due, even in the magisterial Latham edition. Credit is often wrongly assigned, for instance, to Grenville's brother Thomas, who was merely an intermediary, or to the otherwise unknown John Smith, who was clearly the transcriber not the solver of a shorthand writing which had long been obsolete and required reconstruction from first principles.

That same procedure enabled me to decrypt the shorthand system used by William Clarke as secretary to Cromwell's army. It too had been left unread, and indeed shelved as unreadable. Yet some of its entries are as lively as anything in Pepys, in a style equally formed by the fluent and familiar brevity of shorthand writing.

Leith, 25 February 1651/2. This day one Wragge who was formerly a sutler in the army having a wife in England and since his coming in Scotland married another here which being discovered with was this day sentenced by a court-martial to be tied down to the gallows and after that to have twenty stripes from the main guard to the sand port and so turned out of town which sentence was executed this day accordingly.

Here is a vivid glimpse of the disciplines of a Puritan army. The Clarke journals have now been published complete on microfilm, and their extensive shorthand passages await transcription.

There are many more such discoveries still to be made. Success requires only the skills of the cryptic crossword solver; there is no need for any stenographic or historical expertise. The background story is straightforward enough. A book of so-called *Characterie* by Timothy Bright appeared in 1588; and this retains an honoured place as the precursor not only of shorthand, with the rudiments of phonetic spelling and contractions, but also of basic English, thesaurus classification, and artificial language. But it depends first on the memorization of some 500 separate symbols for individual words, and then on the use of a laborious and ambiguous method for recording their synonyms or antonyms. It seems manifestly impracticable, despite contemporary claims, as a method of taking dictation.

This applies also to the *Writing Schoolmaster* of 1590 by Peter Bales, which is essentially the Bright system simplified. Some Shakespeare scholars have contended that the "stolne and surreptitious copies" of which the First Folio complains were procured by such means. But if plays were indeed pirated by shorthand, a far more likely method is that of John Willis, whose *Art of Stenography* in 1602 introduced that word into the language as well as the art itself into the modern world. All later systems are much indebted to its basic principles, which include an alphabet of letter-symbols and the idea of showing internal vowels by position only. Although still primitive and unwieldy, this shorthand was both viable and durable, as evidenced by its use in a diary ca. 1625, which is now being transcribed. Its successor, the *Brachigraphy* of Edmund Willis, 1618, was apparently more widespread and certainly more serviceable. It figures, in fluently cursive use, in a Bodleian manuscript of the period and also as marginalia on a privately owned copy of the *Eikon Basilike: The Portraiture of His Sacred Majesty in His Solitudes and Sufferings*, 1648.

That thirty-year gap between source and sample is not uncommon. The shorthand manuals were no doubt handed down within a family; not only the convenience but the commercial advantages of the new idea were readily recognized. Thomas Shelton's *Short Writing*, ca. 1630 was popular enough to go through several editions over three decades; it was used by both Pepys and Clarke, as well as by unknown hands in literary and poetic manuscripts now in the Bodleian Library. One of these includes several verses of Milton's *Ode on the Morning of Christ's Nativity*, together with less familiar works.

Other mid-seventeenth-century shorthands to survive the test of practical usage include the *Brachigraphy* of Henry Dix, in British Library manuscript correspondence about the marriage of Richard Cromwell, while Shelton's second invention, the *Zeiglographia*, and the *Stenography* of Thomas Metcalfe, occur as marginalia on printed books. The *Charactery* of Jeremiah Rich figures in an interesting undated manuscript now in private hands. It contains the royal monogram of Charles I, together with details of a secret cipher which he is known to have used in correspondence. But it consists mainly of agonized and self-abasing prayers written in the Rich system. Their text is largely formulaic and unrevealing; but occasional phrases such as "my people," "my duty," and "my danger" suggest that the voice of the king himself may perhaps be recorded here, just as it later was (by William Clarke among others) on the scaffold.

As the practice of shorthand grew and spread down the centuries and across the world, its infinitely variable symbols registered the same constant themes. Prayer and pious meditation are recurring keynotes. When the preacher James Humphreys left his Massachusetts home in 1776 to fight for American independence, he took with him his knowledge of James Weston's *Stenography Completed*, 1727. That method enabled him to chronicle his devotions as well as his campaigns, in a manuscript now preserved by the New York Historical Society. A journal kept in the 1780s by the Reverend Alexander Ewing, once a rector in Devonshire, has emigrated into the archives of Bermuda; there too, personal prayers are couched in the intimacy of stenography, this time that of John Byrom's *Universal English Shorthand*, 1767.

Again, the Reverend James Hawkes in a Bodleian manuscript of the early nineteenth-century notes his homilies and sermons in the *Shorthand Unmask'd* of Henry Barmby, ca. 1780. In general, the early systems served especially to express the writer's most intense and inward thoughts, whether of religion, politics, or love. So shorthand writing is predictably used for concealment as well as convenience. Thus in 1851 the once renowned phrenologist George Combe examined the bumps of Charles Bray, close friend and mentor of George Eliot, and diagnosed "Vigorous Amativeness." Bray's supporting testimony is discreetly recorded in a shorthand note, which begins, "At twelve years of age he was seduced by his father's cook." The Combe journals are now in the National Library of Scotland; their occasional passages in the *Universal Stenography* of William Mavor, 1800, may well reveal further vignettes of contemporary life.

The best advertisement yet available in favour of the analytical methods advocated here is in Professor Peter Waite's recent biography of Sir John Thompson, Prime Minister of Canada 1892-94 entitled *The Man from Halifax*. It combines many of these typical features. Its chief topics are politics and love; its method indicates that J. Dodge's *Complete System of Stenography* (1823) was still being put to everyday use nearly seventy years later. No doubt both the Dodge source-book and Thompson's skill had

been acquired from his father, a practised shorthand writer. A document written originally in shorthand in December 1892, and now in the Manuscript Division of the Public Archives of Canada begins with exemplary suavity: "I have always felt that the most disagreeable part of the duties falling upon one who should choose a new Cabinet was the horrible task of parting with former colleagues for whom feelings of respect and confidence had grown up the stronger by years of mutual confidence ..." and so on. In other words, you're sacked! (The same flowing hand pens the tenderest of love-letters with a limpid readability clearly much indebted to the shorthand system itself.)









This decryptment was much facilitated by the writer and the system used. The look of the hand on the page was exceptionally appealing. Graphology, though it can be impressively effective in its practical applications, is very far from an exact science; and brachygraphology, or whatever we may elect to call the process of drawing inferences about the psychological characteristics of the shorthand writer, will no doubt remain further still. Nevertheless one cannot help noticing the vigour and fluency of the Thompson style. It is the hand, surely, of an unusually intelligent and complex personality, a highly private individual who is also a born communicator. Despite all the differences of system and penmanship, its attributes are entirely Pepysian in their combination of easy self-expressive flow and detached business-like practicality. It looks like the effective symbolisation of fluent and forthright yet thoughtful speech. It wants to address, not to say harangue, the reader; it is clearly designed far more for the despatch of public affairs than for private concealment, though it happens to serve both purposes.

A salient feature is the appearance *en clair* of certain words, such as "Cabinet," and the abbreviated name Sir I (or J)McD. In many an earlier document such expressions would certainly have been enciphered or otherwise disguised, whatever else remained directly readable. The fact that potential points of entry have been thus left unguarded strongly suggested that the entire system was in principle penetrable. I had been sent a specimen page, which in the ordinary course would hardly have sufficed. It was dated 1892, by which time some 350 separate shorthand systems had been published in England alone. Even after eliminating the superseded and obsolete sources and also making due allowance for plagiarisms and repetitions, there would still be little practical possibility of direct identification save by an actual expert practitioner of the particular shorthand in question. In any event the only rational methodology is the commonplace cryptanalytical procedure of counting and classification. However, a preliminary inspection can often prove rewarding. It is always worthwhile to pay special attention to dates, for example, whether in shorthand or cipher writings; the name or abbreviation of a day or month can often provide a decisive clue. No such pointer appeared on the Thompson page. But certain revealing features were readily discernible. First, there was no trace of what might be called diacritic signs such as the dots or dashes (formerly known as jots or tittles respectively, hence that expression) generally used from the early seventeenth century onwards to differentiate various vowel sounds by position around a central stem.

The Thompson shorthand was clearly consonantal only, which eliminated several possibilities straightaway. It also permitted the inference that the words "I" or "a" would either be omitted or written *en clair*. The very first symbol of the text in fact corresponds exactly with the "I" (or "J," then often the same letter) already noted in the abbreviated name. So *prima facie* the draft begins with the word "I" in the writer's ordinary hand. Next comes a symbol with two components, presumably standing for a verb such as "have," "was," "met," "came," or the like (but not for example "want" or "cannot," which would entail three components, or "am" which needs only one) and representing such concepts as "hv," "ws," "mt," or "cm" respectively. Later on the word "a" also duly appears *en clair*, separated from "Cabinet" by actual symbol which presumably stands for an adjective beginning with a consonant and containing only one other. We also find the word "anew" *en clair*, which offers interesting confirmation that this is indeed a consonantal shorthand unapt to distinguish between "anew" and "new," both of which would be written as the symbol for n joined to the symbol for w. However, the analyst must resist the impulse to pursue such inferences and should proceed instead systematically with the more mundane tasks of computation.

Here experience helps by predicting what shapes the basic alphabetical symbols are most likely to assume, and how their combinations probably subdivide into separate letter-equivalents. After the ubiquitous e, the commonest letters in written English are t, next a and o, then n and i, then s and r, and so on in descending sequence through h, l, d, c, down to z. Counts vary in detail, but the general pattern persists. Each language has its own different and identifiable structure, including valid rules about the likeliest initial final letters of words; the detailed data are readily available in published manuals. There are, unsurprisingly, no corresponding works on shorthand analysis; and for that purpose all normal linguistic rules require radical reappraisal, in terms of phonetics as well as orthography. Almost all historical systems are basically consonantal; vowels may thus be conveniently disregarded for computational purposes. The consonantal frequency will itself fluctuate with the system adopted. For example the letter c is in principle also dispensable, since it can in practice be replaced by the symbol standing for k or s. Again, the more sophisticated shorthands of any period use one symbol only for the sound-diagrams sh, ch, th, and wh. All these features and others, such as abbreviations and conventional signs, affect the frequency-count. But there are still some good general rules. Thus the

symbol for the letter t, also often used for it, at, and to will probably stand highest, followed by the symbols for r, s, and n grouped at about the same level; next come l and d, at some remove. Letters h and c, however, tend to be comparatively rarely represented, for the reasons already adumbrated.

The following additional data may also be found useful. In the thirty best-known and most widely used shorthand systems 1602-1750, the symbols resembling h, p, q, r, v, y, and z are most likely to represent those letters. In over half of those same systems  signifies k (or hard c),  l,  m,  n and  t. These are always worth a trial. By 1750-1850, however, this prevailing pattern had shifted, partly because of increasing sophistication. Thus during that period the aspirate h is very rarely represented by any character resembling that letter; similarly the other analogues listed above also gradually disappear. On the other hand x is often used for that letter, and  increasingly stands for hard c or k;  is more likely to mean m and  n, while t is more usually represented by a short vertical than a slanting stroke. There are no special reasons or logical justifications for this evolution, so far as I can elicit; in this sphere as elsewhere the successive generations of inventors and adaptors are far more strongly influenced by the vicissitudes of custom and fashion than they realise or are prepared to acknowledge.

These changing styles are conveniently set out in columnar tabulation, showing the alphabetical letter-equivalents of successive shorthand systems from 1602 to 1882 in Isaac Pitman's *History of Shorthand* (first published in 1847 and reprinted with additions and corrections to 1884). This is an essential work of reference for the analyst; so is Thomas Anderson's *A History of Shorthand* (1882), though its similar listings arranged by alphabetical order of author are less helpful in practice. It will be rare for any system to resist patient siege by an investigator armed with all these data. The source-book when identified will also of course offer valuable additional information for the transcriber; but the original decrypter hardly ever needs it. A shorthand has only to be legible to be in principle readable, given enough manuscript material to work on. Since the solution proceeds on the trial and error programme familiar to us all from crossword puzzles, it offers the same degree of certainty on the same basis of interlocking and cross-checking. The 1823 Dodge shorthand as used by Sir John Thompson certainly has some elements of built-in ambiguity or obscurity, despite its clarity of structure and presentation. It is essentially a system of symbolised speed-words. Thus the letter cited by Professor Waite on p. 26 of *The Man from Halifax* begins, in transliteration, "ystrdy mrng the frst thng ftr brkfst (l) wnt p t the (Way Office) t s f the ml hd cm," with the underlined letter-groups represented by a single arbitrary symbol and the bracketed words written *en clair* (otherwise "wy ffs" would be unclear). Such usage in effect ensures that what stands in the shorthand is not only reasonably self-evident but in practice, on any common sense evaluation, basically reliable. When (as in this same letter) a young man addresses his fiancée as his "dr bby" we are entitled to assume that he does not mean "dire booby" for example, though the Dodge shorthand could not have rendered those words in any different way. Professor Waite is accordingly justified in interpreting the phrase "yr gly cwrđ by" as "your ugly coward boy," and adducing further inferences and insights from the shorthand as the sole source of these and other such revealing comments. It will always be the historian or the biographer who will best be able thus to elucidate the factual data and to whom therefore any decrypted material really belongs. It is a special satisfaction for the cryptanalyst when the personal pleasures of diversion and discovery also arrive at results which can prove to be of some service to such scholarship as Professor Waite's work on Sir John Thompson.