

RARE BOOK

Z

104

.B5

1807

1960

*1960*

CIPHER.

w/0100

C

# National Oceanic and Atmospheric Administration

## Rare Books from 1600-1800

### ERRATA NOTICE

One or more conditions of the original document may affect the quality of the image, such as:

Discolored pages  
Faded or light ink  
Biding intrudes into text

This has been a co-operative project between NOAA central library, the Climate Database Modernization Program, National Climate Data Center (NCDC) and the NOAA 200th Celebration. To view the original document, please contact the NOAA Central Library in Silver Spring, MD at (301) 713-2607 x 124 or at [Library.Reference@noaa.gov](mailto:Library.Reference@noaa.gov)

HOV Services  
Imaging Contractor  
12200 Kiln Court  
Beltsville, MD 20704-1387  
April 8, 2009

LIBRARY  
WEATHER BUREAU

No. 17298

Class \_\_\_\_\_



# CIPHER.

---

CIPHER, or ΣΥΦΗΡ, in *arithmetic*, one of the numeral characters called figures, and formed thus, 0. The word cipher is probably derived from the Hebrew ספח, *saphar*, to number. By the Italians it is written *zifra*, by the French, *chiffre*, and by the Low Latins *ciplra*. It is, therefore, more properly spelled cipher than cypher.

The arithmetical cipher by itself implies a privation of value, or nothing; but when disposed with other figures situated on its left, in common arithmetic, it seems to augment each of their values by tens; and in decimal arithmetic it lessens the value of each figure to the right thereof in the same proportion. See the article ΑΡΙΘΜΗΤΙΚΟ, “Rees’ Cyclopædia.”

A cipher also denotes a kind of enigmatical character, composed of several letters interwoven together fancifully; which represent the initial letters of persons’ names, and are frequently used on seals, coaches, and articles of plate, or other movables.

Formerly, when merchants and tradesmen were not allowed to use armorial bearings, they had ciphers thus artfully composed in their stead, which mostly consisted of the first letters of their names, curiously intertwined about a cross, etc., of which many instances remain on ancient tombs; but the

custom still obtains among persons of various ranks in life, as an ornamental device, especially on seals or carriages. This practice has, indeed, been increased of late, to avoid the annual tax of two guineas imposed in Great Britain on those who paint their family arms upon carriages. See HERALDRY, "Rees' Cyclopædia."

CIPHER in *diplomatic affairs*, signifies an occult manner of writing, legible to those only who possess the key or secret, and hence the term *deciphering*, which signifies to explain what is written in *cipher*. We believe this art was so called from the early custom of using arithmetical characters or figures for the purpose of secret correspondence; a practice still common in the courts of princes, and for the skilful management of which a decipherer is attached to the office of the Secretary of State for Foreign Affairs.

This art has been so much cultivated by the moderns, as to have acquired the importance of a distinct science, and is called *cryptology*, *cryptography*, *polygraphy*, *steganography*, &c.

In the present article we shall touch upon all the parts of this science, by whatever names they have been distinguished, although it must be allowed that the term *cipher* is only applicable to private writing. When we consider the noble and pre-eminent advantages of alphabetical writing, an art which so peculiarly distinguishes civilized society from uncultivated barbarians, and the very gradual progress it is likely to have made toward a state of perfection, we cannot reasonably suppose the practice of writing in cipher was common in the remotest ages of antiquity. To communicate our thoughts at a distance by means of arbitrary and visible marks was, in its rudest form, a vast effort of the human mind; and we must imagine that many centuries would elapse before writing was so perfect and universal as to render it necessary to adopt any more abstruse modes of concealment. See LETTERS, CHARACTER, and WRITING, "Rees' Cyclopædia."

A general sentiment has, indeed, prevailed among the literati, that the Egyptians invented hieroglyphics in order to hide and secrete their wisdom from the vulgar; a mistake, which the very learned Bishop Warburton ("Divine Legation," b. iv, § 4), has sufficiently confuted. Nay, we might with as good reason fancy the ancient picture-writing of the Mexicans, or the more refined hieroglyphical characters of the Chinese, to have been contrived for the purposes of secrecy, and not for the diffusion of knowledge. See the article **HIEROGLYPHICS**, "Rees' Cyclopædia."

Letters were undoubtedly a much later invention than emblematical or symbolical writing; and, in their infancy, they must have been so puzzling as to appear endowed with an almost miraculous faculty. But when this exquisite contrivance had become familiar to the vulgar eye, and would no longer serve to conceal the mysteries of statesmen or the intrigues of designing subjects, the use of ciphers began to be foreseen. The want of them was at first supplied by artifices of different kinds, but chiefly newly-constructed alphabets, which, being intended only for the use of princes, ambassadors, generals, and other public personages, were not disclosed to the world at large. Even so late as the time of Lord Chancellor Bacon, and in this free country, it was considered as an aggravation of Earl Somerset's crime to employ secret writing. "They made play," says Lord Bacon, "of all the world besides themselves; so as they had ciphers and jargons for the king, queen, and all the great men, things seldom used but either by princes, and their ambassadors and ministers, or by such as work and practise against, or at least upon, princes."—*Bacon's Remains: Charge against the Earl of Somerset.*

It is, too, much to be lamented, that, on some occasions, disaffected, treacherous, and ill-designing men have greatly abused this curious department of science, by applying it to the basest and most mischievous purposes; but, we ask, is this a reason

against using or divulging it? Is it a sufficient plea for suppressing all we know on the subject, and endeavoring to stifle our knowledge lest it should chance to be perverted? Would not a similar argument hold good for preventing the use of the press itself, and even for destroying books altogether? What useful thing has not been abused? And if this art should be turned to any purpose subversive of society, we have laws and magistrates to punish the offenders. It has been well observed by Bishop Wilkins (in his "Mercury, or the Secret and Swift Messenger"), that "nothing hath occasioned more troubles and contention than the art of writing, which is the reason why the inventor of it is fabled to have sown serpents' teeth; and yet it was but a barbarous act of Shamus, the Egyptian king, therefore, to forbid the learning of letters. We may as well cut out our tongues because that member is a world of wickedness! If all those useful inventions that are liable to abuse, should on that account be concealed, there is not any art or science which might lawfully be professed."

The authors who have written either formally or incidentally on the subject of secret writing are by no means few in number; but they are not often consulted, nor always very easy to be met with; and it is surprising to find how seldom they are quoted by writers on bibliography and general literature. In the last edition of the Encyclopædia Britannica, and in the article *Chiffres* of the large French Encyclopédie (Département Diplomatique, tome i., part ii., p. 538), mention is made of only three or four (and these not the principal) authors; so that we conceive that it may be interesting to point out those who have most distinguished themselves in this science at different periods and in various nations. We shall, however, attempt to compress our historical remarks into as narrow a compass as possible.

The art of corresponding by visible signs may be supposed

to have existed before the introduction of writing, and might have been practised by gestures or motions of the body; since infants are able to express themselves in this way before they have acquired the faculty of speaking; but whether or not the practice of holding secret information by signs of this nature, was carried to any great extent by the ancients, we are unable to say. Ovid takes notice of the art of discoursing thus in the lines following:

“Verba superciliis sine voce loquentia dicam,  
Verba leges digitis, verbaque vultus habet.”

And again:

“Sæpe tacens vocem, verbaque vultus habet.”

Schottus, in his “Steganographia,” exhibits an arthrollogical alphabet in Latin and German; also Mr. Falconer, in his “Cryptomenysis Patefacta,” and Bishop Wilkins, in his “Mercury,” chap. xiv., have given us a similar one in English.

As to the art of discoursing with the fingers, named dactylogy and cheirology, it has often been commended for its antiquity; since the ancients used to express any number under one hundred by the fingers of the left hand, and above one hundred and under one thousand, by those of the right hand. Moreover, Pierius has practically described their methods of reckoning from one to nine thousand; and hence Juvenal says:

“Rex Pylus, magno si quicquam credis Homero,  
Exemplum vitæ fuit à cornice secundæ,  
Felix nimirum, qui tot per sæcula vitam  
Distulet, atque suos jam dextra computat annos.”

To employ this manœuvre for the purposes of secrecy, Schottus has afforded us another alphabet; and so likewise has the celebrated George Dalgarno, in his “Didascalocophus,” p. 74, who distinguished himself in the reign of Charles II, by an endeavor to introduce an universal character and philosophical language.

Among the signs for nightly information at a distance, those by fire are extremely common, and have been used by the Chinese, Persians, and other nations, in the remotest times. This species of communication is affirmed by Diodorus Siculus to have been practised by Medea in her conspiracy with Jason, which carries us back three thousand and seventy years; and although there must be some uncertainty on this question, Pliny, in his "History," liber vii., cap. lvi., says it originated with Sinon. "Specularem significationem Trojano bello Sinon invenit." This was the signal upon which Sinon agreed to unlock the wooden horse, in the siege of Troy, about 1184 years before Christ :

" \* \* \* Flammas cum regia puppis  
Extulerat \* \* \* \* ."

*Virgil, Æn., lib. ii., 256.*

And after the taking of Troy, Æschylus relates, that Agamemnon immediately apprised his queen, Clytemnestra, of that event by a similar method, which, we suppose, must have been done either by men placed at certain distances with lighted torches, which they held up in succession, or by a considerable number of fires on the tops of hills, denoting the simple fact previously agreed between the parties. See Onosander's "Strategicus," cap. xxv, where this practice is described.

The fire-signals of the Greeks and Romans are also slightly mentioned by Quintus Curtius, Livy, Cæsar, Herodotus, Homer, and Thucydides; likewise by Vegetius and Frontinus; but still more in detail by Polybius, and Æneas Tacitus, the latter of whom was contemporary with Aristotle, and has left a valuable fragment on the duties of a general (translated into Latin by Casaubon), wherein are many curious remarks on the subject of secret correspondence. The Greek signals were much improved by Polybius, who, in his history, (liber x, cap. xlv., p. 296, tome iii., Leipsic, 1790, edited by John Schweighæuser), attributes the invention to Cleomenes and Democlitus, or

(more correctly) to Cleoxenes and Democlitus, in words thus rendered: "Postrema ratio, cujus auctores sunt Cleöxenes "et Democlitus, sed quam nos correximus, certa definitaque "est, adeo ut quidquid exortum fuerit negotii, id possis certo "facere notum." Prior to that period, the information communicated by torches, flags, smoke, or otherwise, was very limited, and it was requisite to settle beforehand, what each signal should mean; whereas Polybius showed how to correspond alphabetically, and to give or receive any species of intelligence without this previous concert. The plans of Æneas Tacitus had never arrived at such perfection, and were therefore of comparatively small use; though, without doubt, he at least equalled any of his predecessors in the facility of his telegraphic communications. *Vide* "Polybius," liber x., sub. finem.

Polybius has detailed the peculiar invention of Æneas, which consisted of a narrow earthen vessel filled with water, and having a tube or aperture to let off the fluid; a piece of stick is then to be thrust through a cork, so as to float above the surface when it is put in the water; and the upper part of this stick is to be marked by subdivisions of three inches each, upon which are to be written such common events as happen in war. Where the water is drawn off from any of these vessels, which must agree exactly in size, &c., it is evident the sticks will sink lower as the vessel becomes empty; so that on observing the space through which the sticks descend, the correspondents may (by the help of a similar apparatus) tell which of the expected events has occurred. But Polybius, finding this contrivance adapted only for those few occurrences which had been previously written on the sticks, describes his own method, which was far superior.

We are told, however, that Æneas Tacitus collected together about twenty different modes of writing, which could only be understood by persons who were in the secret; part whereof

were his own, and part of them invented by others; so that this author seems to have been well versed in the art of secret correspondence, as it then existed among the ancients.

We shall hereafter have occasion to notice some of the secret modes of writing recorded by Æneas; but it will first be proper to explain and illustrate the telegraphic invention of Polybius himself, which is as follows:

Divide the letters of the Greek alphabet into five parts, each of which will consist of five letters, except the last division, which will have only four. Let these be fixed on a board in five columns. The man who is to give the signals is then to begin by holding up two torches, which he is to keep aloft till the other party has shown two. This is only to show that both sides are ready. These first torches are then withdrawn. Both parties are provided with boards on which the letters are disposed as formerly described. The person then who gives the signal is to hold up torches on the left to point out to the other party from what column he shall take the letters as they are pointed out to him. If it is to be from the first column, he holds up one torch; if from the second, two, and so on for the others. He is next to hold up torches on the right to denote the particular letter of the column that is to be taken. All this must have been agreed on beforehand. The man who gives the signals must have a dioptrical instrument (*διοπτρον*), consisting of two tables, and so placed as that, by looking through one of them, he can see only the right side, and through the other only the left, of him who is to answer. The board must be set up near this instrument; and the station on the right and left must be surrounded with a wall (*παραπεφραχθαι*) two feet broad, and about the height of a man, that the torches raised above it may give a clear and strong light, and that when taken down they may be completely concealed. Let us now suppose that this information is to be communicated: *A number of auxiliaries, about a hundred, have gone over to the enemy.* In the first place, words must be chosen that will

convey the information in the fewest letters possible, as: *A hundred Cretans have deserted*—*Κρητες εκατον αφ' ημων ηντομολησαν*. Having written down this sentence, it is conveyed in this manner. The first letter is a *κ*, which is in the second column; two torches are therefore to be raised on the left hand to inform the person who receives the signals to look into that particular column. Then five torches are to be held up on the right to mark the letter *κ*, which is the last in the column. Then four torches are to be held up on the left to point out the *ρ* (*r*), which is in the fourth column, and two on the right to show that it is the second letter of that column. The other letters are pointed out in the same manner. Such were the *Φρύχτοι* or *Πυρσεια* recommended by Polybius.

As this contrivance deserves particular attention, and throws great light on a common mode of writing by cipher, we shall here attempt to give a further elucidation of it, by another example and a diagram.

Dispose the letters into five rows or columns; place a figure over each of them, and another by the side of the five lines; but instead of Q let K be its substitute. Thus:

	1	2	3	4	5	
	a	f	k	p	v	1
	b	g	l	r	w	2
	c	h	m	s	x	3
	d	i	n	t	y	4
	e	j	o	u	z	5

Provide ten torches, and let so many be held up toward the right hand as may denote the row in which the letter required is to be found; likewise so many on the left hand as shall point out the place of the same letter, reckoning from above. Proceed in this operation till you have completed the word or sentence to be communicated, as in the underwritten example; where the first figure in each pair shows the row, and the second denotes the order of the letter, which being duly performed, the spectator will receive the following information:

52. 15. 41. 15. 42. 24. 43. 23. 12. 54. 21. 11. 33. 24.  
 w e p e r i s h b y f a m i  
 34. 15. 11. 34. 14. 14. 24. 43. 15. 11. 43. 15.  
 n e a n d d i s e a s e.

An intelligent reader will perceive that five lights might do for the purpose of representing these five differences, as well as the ten; nay, better, only taking care to pause sufficiently after every separate elevation of the torches, whether to the right or the left hand. It is worthy of remark that this very principle of distant communication has been recently adopted in the construction of a day-telegraph at the Admiralty! Although in the latter there are six signs for the purpose of representing figures as well as letters. (See the articles SIGNALS and TELEGRAPH, "Rees' Cyclopædia.") But we have advanced enough to show that the ancients, two thousand years ago, knew how to maintain secret correspondence by signals. We shall next prove that they were also acquainted with several means of *writing by cipher*; although it must be confessed, that the moderns have greatly improved upon their inventions of this kind.

Le Sieur Guillet de la Guilletiere, in his "Ancient and Modern Lacedæmon," endeavors to show that the Spartans were the inventors of writing in cipher; and that their *scyta'æ* were the first rudiments of this art. We suppose he has taken

his account of the *σκυτάλη* from Plutarch; but as several modes of secret writing mentioned by Æneas Tacitus are entirely different from this, it by no means follows that those of Æneas were suggested by the former; nay, we are disposed to think, with Scaliger, that a little attention might have developed this cipher with ease.

The nature and use of the *scytala*, according to Plutarch, in his "Life of Lysander," was this: When the Grecian magistrates sent out an admiral or a general, they prepared two cylindrical pieces of wood with so much exactness that they were perfectly equal both in length and thickness. One of these they kept themselves, and the other was given to the military officer then employed. When they had any secret and important orders to communicate to him, they took a long narrow slip of parchment, and rolled it round their own staff, in a spiral form, one fold close to another, and then wrote their communication upon the edges of the parchment. This done, they took off the scroll and sent it to the commander; who, on receiving it, applied it to his staff, so that the broken and imperfect characters now became legible. The parchment, as well as the staff, was called *σκυτάλη*. As this contrivance was had recourse to by the Athenians and Lacedæmonians, in the time of Alcibiades, Pharnabazus, and Lysander, we are certain it was invented at least four centuries earlier than the birth of Christ.

Although this confused sort of writing, as it would appear upon the unrolled slip of parchment, is not a sufficient security against detection in the present sharp-sighted age, there are other means of secret writing which even Scaliger's eyes (as Bishop Wilkins observes in his "Mercury"), could not discover; "and therefore it was too inconsiderate and magisterial a sentence of him, thence to conclude all this kind of learning to be vain and useless. It is certain," adds the bishop, "that some occasions may require the exactest privacy, and it is as

“certain that there may be some ways of secrecy which it were “madness for a man to think he could unfold;” in which opinion he is supported by Vegetius, Baptista Porta, and Lord Bacon, as well as by several more recent judges; so that Scaliger showed greater self-confidence than skill in pretending he could decipher any writing that might be invented. The author of the present article (who has only taken up this subject as an amusement) challenges all the Scaligers in Europe to explain various kinds of cipher he has recently contrived, and which elude every rule laid down by his predecessors.

The learned Mr. Falconer, and some earlier writers on cryptography, have attributed the invention of the Lacedæmonian *scytalæ* to Archimedes, the mathematician; but we have already afforded the reader evidence of its use in the days of Alcibiades, Pharnabazus, and Lysander, who lived nearly two centuries prior to the time of Archimedes; and Plutarch does not speak of this invention as *new*, or as being used by the Greeks alone, at that early period. See Plutarch in his Lives of Alcibiades and Lysander.

We next descend to the age of Aristotle, about 350 years before Christ, when the art of secret writing seemed to have assumed a more regular and systematic form; but the authors of that age and those following, whose works have descended to posterity, are so few and imperfect as to throw only a faint light on the object of our inquiry. We are ignorant of what was done by Julius Africanus, Laertius, and Philo-Mechanicus, three ancient Grecians, who treated on this subject. Æneas Tacitus and Polybius are our principal guides; the former of whom was contemporary with Aristotle. (*Vide* “*Æneæ Vetusissimi Sæctici Commentarius, de tolerandâ Obsidione, Casaubono interprete,*” 1610, 8vo.)

Æneas is said by Polybius to have collected and invented a great number of secret modes of corresponding; and among them, we imagine, are included those few which are briefly

recited in the above-named work. He seems to have approved especially of affixing small dots to the letters of any book or epistle, written upon a common subject, in such a way as only to denote the characters expressive of the secret sentiment, all the rest being non-significant. He also recommends the substitution of points instead of vowels, and gives the two following short specimens :

D :: :: N :: : S : : : SP :: . LCH . . R ; which signifies  
DIONYSIUS PULCHER. H . . R . CL : . D . . SV . . N : .  
T : : ; which stands for the words HERACLIDES VENITO.

This mode may be varied indefinitely ; for it is of no importance what arrangement or number of points is substituted for the vowels ; and although we cannot say this is very difficult to decipher, it nevertheless demonstrates the fact of secret writing being employed in those remote ages. The same author likewise mentions the artifice of passing a thread through holes in a board or tablet corresponding with the twenty-four Greek letters, which Gustavus Selenus, (an assumed name of the Duke of Brunswick and Luneburg,) who published a folio book on cryptography, A. D. 1624, has therein described more at large. The order of the threads expressing the alphabetical characters, previously settled by compact, will represent any words we please.

There is great affinity between this method and that of tying knots upon a string at various distances from each other, so as to agree with a determinate measure, graduated for the purpose. Few people would suspect any private news or treachery to be hidden in a piece of knotted thread. Bishop Wilkins has further illustrated this device in the fifth and eleventh chapters of his "Secret and Swift Messenger," and we have given a representation upon *Plate II, Fig. 1*, of the gradual measure alluded to, with knots tied upon the threads opposite to the letters F, L, Y, from which any person may learn how to put this plan into execution.

The same effect will be produced if, in lieu of the knots, the thread be marked with ink at the proper intervals opposite each letter; or if the tablet, or the measure, be applied to paper, and dots are impressed upon it under the holes or subdivisions which stand for the respective letters. The ancients have laid down the principle which is thus easily varied in practice; but the merit of this invention belongs to them rather than to the moderns.

Æneas was acquainted with many other modes of occult writing besides these, some of which are alluded to in his "Poliorecticus," § xxxi, but the greater number are wholly lost. And it is truly surprising that these methods of correspondence should not have been more universally carried into effect by succeeding generations, so as to have prevented the loss of them. Surely the telegraphic apparatus of Polybius, with five or ten flambeaux, might have been employed and improved upon for the most important military or national purposes; and yet the moderns scarcely have dreamed of using any such means of alphabetical communication till the present age. How obvious it seems that this contrivance of Polybius, with some variation in the materials, should be deemed at least as applicable for daily use as it was found to be for nightly observations. And how numerous are the species of ciphers which a man of common ingenuity would extract from the principles suggested for secret writing in Æneas' little treatise.

He likewise describes several ways of fraudulently conveying intelligence into a besieged town, etc. For example, by the application of a manuscript to a sore leg instead of a plaster or bandage; by sewing up an epistle within the sole of a person's shoe, or hiding it under the arm-pit; rolling thin leaves of lead into the form of ear-rings, etc., after having written thereon; putting a bladder into a bottle of oil, first inscribing upon it, and inflating it, so as to fill the bottle completely; or

writing on a tablet and afterward covering it over with melted wax; to which are added some other singular proposals, showing the fertility of invention exercised by the ancients on such occasions.

But the strangest contrivance was that of Hystiaëus, mentioned by Herodotus; who, while at the Persian Court, sent to Aristagoras in Greece a servant affected with bad eyes, pretending that his hair must first be shorn and his head scarified; in performing which, Hystiaëus imprinted his secret intention, in legible characters, upon the servant's head, and kept him in close confinement till the hair grew, when he desired him to travel to Aristagoras for a perfect cure, who, on the man's arrival, repeated the shaving, and thus obtained the secret information transmitted by means of the ignorant messenger.

As a message may be concealed by adopting any arbitrary marks (for instance the dots of Æneas), instead of letters, so likewise, by changing their powers and substituting one character for another, which is said to have been practised in that kind of cabalism which the Jewish rabbis call קריס, or combination. Bishop Wilkins has cited examples of this sort among the Romans, as Suetonius relates of Julius Cæsar and Octavius Augustus; the former of whom wrote the fourth letter instead of the first, *i. e.*, D for A, the fifth for the second, the sixth for the third, &c.; and Augustus wrote after the same method, only by putting the second for the first, and the third for the second, *i. e.*, B for A, C for B, D for C; which confounds the general appearance of the writing, but is not sufficiently intricate to escape the scrutinizing eye of a modern decipherer. However imperfect and inadequate this ancient mode may be, it is quite as good as three fourths of those ciphers which the principal courts of Europe trusted to until after the sixteenth century. It is a matter of indifference whether we change the powers of the letters, or invent a new-

formed alphabet for secret writing, as the same rules for deciphering one of them will equally well apply to the other. And yet we find, for many centuries after the Augustan age, that kings and ambassadors contented themselves with only changing the form of their alphabets, as if this were any security against detection. It demonstrates how little men addicted themselves to this subject as a SCIENCE, while they felt an indispensable necessity for having recourse to it as an ART.

We do not indeed affirm that there is so much reason now to complain of the negligence of princes and statesman in this respect as there was formerly; but we are in possession of certain facts which show that the words of Lord Chancellor Bacon are not entirely inapplicable to our own times, viz. :  
 “ If the ciphers in use were good and trusty, several of them  
 “ would absolutely elude the labor of the decipherer, and yet  
 “ remain commodious enough so as to be readily wrote and  
 “ read; but through the ignorance and unskilfulness of secretaries and clerks in the courts of princes, the most important  
 “ affairs are generally committed to weak and treacherous  
 “ ciphers.” We have much cause to doubt whether any court in Europe, even at this time (1807), can lay claim to a cipher having the three essential properties required by Lord Bacon :  
 “ 1st. That it be easy to write and read; 2d. That it be trusty  
 “ and undecipherable; 3d. That it be clear of suspicion.”  
 But we refrain from divulging all we believe on this delicate topic—*verbum sapienti sat est*. It may be said that no individual ought to disclose an inscrutable cipher unless he is compelled by imperious circumstances.

The practice of transposing the ordinary letters of the alphabet, to perplex the reader, was not only resorted to by the Romans, but also by the Greeks, Syracusans, Carthaginians, and perhaps by other nations. The ancient Gauls, Saxons, Normans, &c., used more commonly to employ new and uncouth alphabetical characters for secret writing; many exam-

ples of which were collected by Trithemius, and the other systematic authors on polygraphy in the fifteenth and sixteenth centuries.

But the method of representing whole words or syllables by arbitrary marks, said to have been first introduced by the old poet Ennius, was much more perplexing, and was encouraged by Mæcenas, Cicero, Seneca, the elder, Philargirus, Fannius, Aquila, and Tyro. Thousands of these syllabic characters may be seen in Valerius Probus, Paulus Diaconus, Goltzius, and (in 200 folio pages) at the end of Gruter's "Inscriptions."

Although those Tyronian characters, as they are usually named, were not alphabetical, we observe among them a great many bearing a considerable resemblance to each other, when they denoted words beginning or ending with the same Latin particles; so that this kind of *ταχυγραφια* or *βραχυγραφια* was not composed entirely at random, but according to some preconceived system.

The Tyronian *notæ*, we are told by literary persons, were augmented in the time of Seneca to the number of thirteen thousand! And so completely did they answer the purpose of secret writing during the monkish ages, that an old copy of a psalter, found inscribed with these characters, was ignorantly entitled "Psalterium in Lingua Armenica." Nay, Pope Julius II. employed learned men, without success, to decipher them.

Herman Hugo, in his work "De Origine Scribendi," maintains an opinion of this writing having been used among the ancient Hebrews, and that it is alluded to in Psalm xlv: 1, and Daniel v: 25; but this needs further evidence, and is no better supported than the opinion some men hold of English short-hand, which is alphabetical, having originated from the Tyronian characters, which are not alphabetical.

Another ancient sort of writing employed among the Romans more than any nation besides, was that of abbreviating words

or syllables by omitting the final letters, and sometimes placing points or dashes in their stead. These *siglæ*, as they were called, from the word *sigilla*, used be chiefly inscribed on statues, arms, coins, public records, monuments, &c., for the sake of brevity, rather than of secrecy ; and, therefore, do not particularly come under our consideration in the present article, although most authors upon cryptography have taken notice of the *siglæ*. (*Vide* Waltheri “*Lexicon Diplomaticum*,” 1752, and Gerrard’s “*Siglarium Romanum*,” 1792.)

To bring these historical remarks toward a conclusion, we shall now refer to the chief modern writers on the subject of *ciphers*, whose names have come to our knowledge ; some of whom, indeed, have treated more formally and copiously on the art of secret writing than others, but all of whom deserve mention, and may be consulted with advantage. We prefix an asterisk \* to the names of a few authors who, in our judgment, have principally distinguished themselves, and merit an attentive examination.

The first writer among the moderns, and the man who may be said to have led the way in secret writing, for we have no work of any importance before his time, was the \*Abbé Trithemius, a Benedictine, whose erudition and acumen were such that he was suspected of magical practices in the exercise of his art. He composed two extensive treatises ; one of which, entitled “*Polygraphia*,” was published in the year 1499, but the other, called “*Stenographia*,” was not printed during his life. He also made some progress toward the completion of a third work at the instigation of the Emperor Maximilian. His “*Polygraphia*” was translated into the French language by Gabriel de Collange during the year 1561 ; but prior to its appearance, three other authors had written on this subject, viz., Palatino, in 1540, Bellaso, in 1553, and Glauburg, in 1560 ; and in the year 1563 the public were presented with another original treatise, by \*Baptista Porta, an author of

considerable merit. Nearly about the same period, this subject was handled by Cardanus and Bibliander; afterward by \*Blaise de Vigeuere, Walchius, Isaac Casaubon, \*Schottus, \*Gustavus Salenus, Gerrard Vossius, Herman Hugo, Schweuter *alias* \*Hercules à Sunde, Wecker, Niceron, \*Lord Bacon, Caspi, Seeländer, \*J. Balthasar Friderici, Comiers, Basacioni, La Fin, Dalgarno, Becher, Hiller, \*Bishop Wilkins, J. Nicholas, Buxtorff, Caramuel, Wolfgang, \*Falconer, Horsley, P. Crinitus, Ernst Eidel, J. Gesory, J. C. Amman, Ozanam, \*Breithaupt, \*Conradus, Dutton, Davys, Ware, Gravesande, Twis, De Vaines, Caspi, Carpentier, Bishop Warburton, Stanislaus Mink, Lucatello, Kircher, Paschius, Morhof, \*Thicknesse, Hutton, Hooper, Astle, to whom should be added the mathematician \*Dr. Wallis, whose valuable MSS. on this subject are deposited in the Bodleian library; and the celebrated Marquis of Worcester, whose unpublished performance, written A. D. 1659, may be seen in the Harleian library, No. 2,428. We have named the unedited works of these two Englishmen, because Dr. Wallis' papers have often been quoted or referred to by authors, and some of them, indeed, have been printed since his death, and because the Marquis of Worcester's "Centurie of Inventions," §§ 3d and 4th, contain an evident allusion to the subject of the above MS., which was not discovered to be his lordship's until we lately recognized and verified it at the British Museum.

Several authors who have treated largely on diplomatic affairs likewise give some account of writing by cipher, among whom we ought especially to notice the editors of the "Nouveau Traité de Diplomatie," tome iii, p. ii, § 4, chap. x., and the article Chiffres in the Encyclop. Method.—"Economie Politique et Diplomatie." But we confess that our expectations have been sometimes disappointed in works of that nature, for where we hoped to find the science handled most learnedly and copiously, we have found only meagre and trifling observations.

This remark also applies to what is written, or rather stolen, upon the subject of cipher, in the successive editions of the *Encyclopædia Britannica*, wherein we find merely a long extract from Dr. Hooper's "Recreations," without acknowledgment, or any attempt at improvement. The article might, perhaps, be well enough adapted for the purpose it was originally designed, viz., as a "recreation" for school-boys, but cannot be regarded as an ornament to the great national work into which it has been surreptitiously transplanted.

Lord Bacon refers the practice of writing by cipher to the art of grammar, noting it as a deficient branch of knowledge ; and, in reference thereto, it is treated by most of those authors who have written on grammar. "That art," says Bishop Wilkins, "in its true latitude, comprehending all the ways of discourse, whether by speech, or by writing, or by gesture, together with the several circumstances pertaining to them. So that, besides the usefulness of the subject" (viz., ciphering) "for some special occasions, it doth also belong unto one of the liberal arts." Now, among "the ways of discourse" which have been greatly improved and new-modelled of late years, we ought to mention the art of corresponding by *signals at sea*, an art which the moderns have carried to so great a pitch of excellence, that naval officers in different ships can discourse with each other on almost any topic of importance relative to their military duties. We shall here add only a few words concerning naval signals, as this topic will be hereafter discussed at large in a separate article. See SIGNALS, "Rees' Cyclopædia."

Whether the renowned sea officers of ancient Greece and Rome had a system of signals analogous to that of Polybius by land, is a question which we want evidence to resolve ; but we are not without proofs of their using some sort of signals, however simple and inadequate we might now account them. Thus we read when Ægeus sent his son to Crete, that

it was determined to display a white flag if the ship conveyed back Theseus in safety; and in the history of the Punic wars, mention is often made of certain rude methods of correspondence; besides which Ammianus Marcellinus speaks of the *veccillarii* and *speculatores*, and some of the ancient coins represent both flags and streamers. Again, there is a direct allusion to signals on ship-board by Virgil, *Æn.*, iii, 519.

“Postquam cuncta videt cælo constare sereno,  
Dat clarum è puppi signum.”

Also in *Æneid*, ii. 255, before quoted, which implies that Agamemnon, from his ship, and Cinon from the citadel, gave signals mutually to each other, whereby they were enabled to co-operate. But, probably, these methods were as different from the signals by which the operations of modern nations are regulated, as the Chinese hieroglyphics are different from our alphabetical characters. It was easy to erect a flag, display a torch, or blow a trumpet; but to multiply and combine these or such like signals by sea, so as to form letters, words, and sentences (either immediately or through the intervention of numbers), was a science to which the ancients seem not to have attained.

From the incessant changes of position in ships at sea, it is impossible to put in execution the same means of conveying intelligence as we have adopted by land; and, besides this difficulty, the space which can be spared for the display of flags by day, and lights in the dark, is exceedingly limited on ships under sail. The principle, therefore, by which naval communications are chiefly governed, consists in the representations of arithmetical numbers; for which purpose ten or twelve different flags, &c., are sufficient, and fewer than ten would be inconvenient. (See the “Telegraphic Signals, or Marine Vocabulary,” printed by Sir Home Popham, in 1804, for the use of the East India captains.) By the artful com-

bination of a few pendants or flags, naval officers can thus designate several thousand figures, words, and sentences, which are entered in opposite columns for the sake of easy reference; and by night they can exhibit lanterns, blue-lights, false fires, or rockets, with the occasional report of guns, in such a way as to keep a regular correspondence. The lights displayed for signals in the dark, must always be arranged perpendicularly, to avoid any apparent change of their relative positions, when viewed from several ships at a time.

For example: a single light will represent 1; two, three, and four lights, placed vertically, may represent 2, 3, and 4; three lights over each other, two of which are placed at a certain distance below, and the upper one thrice as far above them, will denote figure 5, three perpendicular lights, reversing the last order, may stand for 6; four lights, the two at each extreme being at a common distance, and a triple space between the middle two, will represent 7; four lights, the three lowermost ones at a common distance, and the upper thrice as far, will signify 8; four lights, the three uppermost at a common distance, and the lower one at a triple distance, may denote 9; a false fire, or a blue light, will stand for 0 or 10; and by the successive exhibition of these as they are wanted, any number of figures, denoting particular instructions or communications, can be made with the utmost certainty and precision. To render this example more clear, we subjoin the respective situations of the lights as described above, viz. :



evinced presently. Some laudable endeavors have been made to distinguish the lamps by different colored glasses; but at a great distance these colors could not be discriminated with certainty, or the lights have been too feeble when seen through dense glasses; in consequence of which this project has wholly failed of success, and can never be revived, except by mere speculators.

Another mode of corresponding by *cipher* (for all these modes come under the general denomination), is by striking on two or three bells of various sizes; or by as many different kinds of audible sounds of any other sort—such as 1, a drum; 2, a fife; and 3, a trumpet. We prefer to use three for alphabetical purposes, which may be combined as follows, so as to represent each letter:

|                             |                             |
|-----------------------------|-----------------------------|
| A is represented by.....111 | O is represented by.....223 |
| B “ “ .....112              | P “ “ .....231              |
| C “ “ .....113              | Q “ “ .....232              |
| D “ “ .....121              | R “ “ .....233              |
| E “ “ .....122              | S “ “ .....311              |
| F “ “ .....123              | T “ “ .....312              |
| G “ “ .....131              | U “ “ .....313              |
| H “ “ .....132              | V “ “ .....321              |
| I “ “ .....133              | W “ “ .....322              |
| J “ “ .....211              | X “ “ .....323              |
| K “ “ .....212              | Y “ “ .....331              |
| L “ “ .....213              | Z “ “ .....332              |
| M “ “ .....221              | Blank, or nothing .....333  |
| N “ “ .....222              |                             |

It must be remembered that the three different sounds stand for only one letter; and that a sufficient pause must intervene after each letter, in order to prevent any confusion. To keep an exact memorandum of this cipher, it will be necessary for the author to write either the figures as above, or three alpha-



The objection which may be started against both these ciphers is, that they are too laborious, and not incapable of being deciphered by persons of skill in this art. The writer does not recommend the above mode of dot-writing as very expeditious, but as simple; he knows it, however, to be much less operose than many ciphers submitted to the public, and he can affirm that it is fully as difficult to decipher as the celebrated plan of Lord Bacon, which he calls writing *omnia per omnia*. But as an example of more ready and undecipherable writing by dots of his own invention, the author refers to *Plate III*, whereon he has ventured to engrave the key itself, and yet defies any of his readers to explain the principle by which it is composed, or to give him a similar piece of writing.

The most legible and common ciphers in use consist of a new alphabet, or of the usual characters transposed so as to alter their powers. Of this latter kind was the cipher of Julius Cæsar and Augustus, viz :

|            |   |   |   |   |   |   |   |   |   |   |   |   |   |   |   |   |   |   |   |   |   |   |   |   |   |   |
|------------|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| For.....   | a | b | c | d | e | f | g | h | i | j | k | l | m | n | o | p | q | r | s | t | u | v | w | x | y | z |
| Write..... | d | e | f | g | h | i | j | k | l | m | n | o | p | q | r | s | t | u | v | w | x | y | z | a | b | c |
| Or.....    | b | c | d | e | f | g | h | i | j | k | l | m | n | o | p | q | r | s | t | u | v | w | x | y | z | a |

Julius Cæsar's method, "per quartam elementarum literam," is not only mentioned by Suetonius and Aulus Gellius, but perhaps is alluded to in Ovid's fourth Epistle :

"His arcana notis terra pelagoque feruntur;"

which is paying this species of secret writing a higher compliment than it would now be thought to merit; for, certainly, there is no great skill required to decipher it; but the ancients had not then directed their attention particularly to this subject, or they might have discovered its imperfections.

The learned Montfaucon, in his "Palæographia Græca," liber i, p. 36, edit. Paris, 1708, makes the following remark

on the state of criptography among the Greeks: “*Κρυπτογραφίαν*, sive arcanum scribendi modum, apud Græcos frequentatum observamus. *Κρυπτογραφία* vero duplici modo fieri deprehendimus, per commutationem scilicet literarum, ac per novam et inusitatam characterum formam; utriusque scribendi rationis alphabeta varia, cum exemplis exhibitus in speciminibus undecimī sæculi libro quarto; ubi quam plurima non minus singularia, quam utilia et occulta, recensebuntur.” Accordingly, he gives, at pp. 87, 286, 288, various alphabets and specimens of occult writing by transposition or malformation of the common Greek letters; and especially as it was practised by amanuenses in the eleventh and following centuries. It is certain, too, that the same practice prevailed in much earlier times, even before the age of Æneas Tacitus; and, therefore, the Roman emperors most probably learned this art from the Greeks. (*Vide Palæographia Græca*, liber iv, c. v., de *Κρυπτογραφίαν*.) But there is great reason to believe that all these ancient modes of writing were decipherable by the ordinary rules of analysis in such cases. We shall hereafter point out the rules necessary to be observed in deciphering, and lay down a few directions for the application of common sense where the species of occult writing does not admit of any positive rule in its development.

We have now carried our history of this art down to a period in which we take leave of the Greeks and Romans. Before we proceed it may be expected that we should illustrate these remarks by more examples; but since it would be very expensive, and of no peculiar advantage to the inquisitive reader, if we were to engrave all the arbitrary characters with which secret writing has been performed, we shall substitute in their place such marks and figures as are found in the printing-office, which will equally well illustrate the principles and practice of the Greeks and Romans in regard to the art of cryptography.



## No. III.

④x④ ④n④④④ ④x④④④④④ ④x④④④④④  
 ④x④④④④④ ④x④④④④④ ④x④④④④④ ④x④④④④④

## SOLUTION.

Une fille gaillante reprochoit a son frere sa passion pour le jeu, qui le ruinoit : quand cesserez vous de jouer, lui dit elle, quand vous cesserez d'aimer, repondit le frere ; ah malheureux ! repliqua la sœur, vous jouerez toute votre vie.

## No. IV.

†PJS† J§ N§P †L K†THT, JVR †T H§NNR J§PHQ†JR Z§  
 N§H§ J§P †L L†E§ N†PXQLXP§ R H§HIL XZL †ZHTL  
 N§PJRHT †L N†RLH† P†T†HL PZZT† T†Z†H§P† H††N-  
 QNN†, L †Y†ZL KRI ZOP§ H††H§ †L H§Q§ V†P§  
 †AZLH§ †E †AZLX§P§ †PJS† H§H††††† ††††† †E-  
 P††, H††††† ††††† ††††† ††††† ††††† ††††† †††††  
 †††††, N†Z††††† ††††† ††††† ††††† ††††† ††††† †††††

## SOLUTION.

Ancor io son di parere, che la tosse contumace lo sputo con di rado sanguigno e tutti gli altri sconcerti di sanita narrati nella relatione trasmessa, i quali per lungo tratto di tempo hanno afflitto ed affliggono ancor tuttavia questa Donna, tragano la lor vera origine dalla Soverchia acutezza salsedine ed acrimonia del sangue e di tutti gli altri liquidi del suo corpore.





Archduke of Austria, who lived in the fourteenth century, was also much versed in the practice of occult writing; but there is no complete cryptographical work extant, of earlier date than that of Trithemius, composed under the sanction of Maximilian, at the end of the fifteenth century, soon after which period Frederic II, Elector Palatine, was induced, by a superstitious outcry against the author, of having practised diabolical mysteries, to commit the original MS. of Trithemius' curious book to the flames!

In *Plate I, fig. 6*, we have represented the cipher used by the Cardinal Wolsey, at the Court of Vienna, in 1524. *Fig. 7* is the cipher which Sir Thomas Smith employed at Paris in 1563. *Fig. 8* is Sir Thomas Chaloner's cipher from Madrid, in 1564. *Fig. 9* is that of Sir Edward Stafford, from Madrid, in 1586. And among the royal MSS. deposited in the British Museum, we have met with various other ciphers of the same period; so that they had then become of general use in the different European courts.

The form of these ciphers, it will be observed, was very arbitrary and capricious; but the mode of secret writing underwent a considerable change in the next century, by the frequent adoption of arithmetical figures instead of letters, as we perceive, for example, among the confidential epistles of Charles I. to his son. (*Vide* MSS. Nos. 132, and 6988 Bibl. Harl.) We subjoin part of one of this unfortunate monarch's letters, dated August 1st, 1648, as a specimen of that kind of cryptography; and for an explanation of many more of them, we refer to Dr. Wallis' unpublished collection in the Bodleian Library at Oxford.

"I thought that 379: 361: 185: 28: 2: 239: 59: 60:  
 "93: 5: 214: 126: 379: 90: 37: 1: 258: 6: 2: 212:  
 "370: 196: 379: 245: 339: 365: 329: 165: 246: 16:  
 "50: 212: 196: 444: 149: 13: 44: 32: 14: 26: 10:  
 "78: 43: 65: 329: 331: 380: 17: 48: 29: 338: 77:

“ 214 : 339 : 93 : 85 : 6 : 23 : 220 : 78 : 57 : 152 : 5 : 65 :  
 “ I command you,” &c.

In another letter, the king writes to his son from Newport (November 7, 1648,) and adds: “ Let none decipher this but yourself, or my Lord Culpeper,” so that this cipher was, doubtless, regarded as very faithful, and was, perhaps, entrusted to only a few confidential persons about his majesty. Somewhat prior to that critical time, however, we find Charles I. using a cipher which could by no means be depended on for secrecy. We allude to an alphabet chiefly composed of twenty-four short strokes variously situated upon a line, and by which, April 5, 1646, he wrote to the Earl of Glamorgan, afterward the Marquis of Worcester. See Royal Letters, Bibl. Harl., vol. iii., 118, 199, &c.

We have exhibited this ogham-like alphabet in *Plate I, fig. 4*. It has been often referred to of late, as a curious and very simple device. (See Biograph. Britan., vol. i., page 433, Art., BALEs), and it was the accidental sight of this alphabet in the year 1804 which first caused the author of the present article to investigate the nature of ciphers; for, till then, he had never once thought or read on the subject. During the course of this examination he discovered (in Bibl. Harl. No. 2,428,) the Marquis of Worcester's peculiar, and hitherto inexplicable, mode of writing, which seems to be briefly described in the 3d and 4th of his Lordship's “Centurie of Inventions,” of which, likewise, there is in the British Museum a fair manuscript copy, dated “from August ye 29th to September ye 21st, 1659.”

We here extract the Marquis' words regarding this remarkable cipher, from pages 5th and 6th of his “Inventions,” which were first written by him in 1655, but not printed till 1663, as we learn from the work itself: “A cipher and character so contrived, that one line, without returns and circumflexes, stands for each and every of the twenty-four

“ letters, and as ready to be made for the one letter as the other.

“ This invention, so refined and so abbreviated, that a point only sheweth distinctly and significantly any of the twenty-four letters, and these very points to be made with two pens, so that no time will be lost ; but, as one finger riseth, the other may make the following letter, never clogging the memory with several figures for words and combinations of letters, which, with ease and void of confusion, are thus speedily and punctually, letter for letter, set down by naked and not multiplied points. And nothing can be less than a point, the mathematical definition of it being *Cujus pars nulla*. And a motion no swifter imaginable than *semiquavers* or *relishes*, yet applicable to this manner of writing.”

This cipher was one of the extraordinary inventions for which the Marquis applied to Parliament, in hopes of remuneration, but as he was not known to have either printed an account of it, or to have left any explanation of it in writing, many shrewd conjectures were afterward made touching the nature of this noble author's contrivance. We shall notice one of these guesses before we proceed to give a further description of it. (See *Gent. Magazine*, vol. xviii., page 55.) An anonymous gentleman proposes “ to rule his paper with quarternions of lines, as if for music, and to let the points representing the letters be placed on between these lines, one half of the alphabet to ascend in the scale, and to be done with common ink ; the other half to descend, and to be done with red ink, the red ink pen in one hand, and the black in the other.” The proposal, however, does not at all correspond with what we believe to have been intended by the Marquis of Worcester ; it is also much too complex and tedious for ordinary practice, and would be far from answering the purposes of a faithful cipher.

As this nobleman was one of the most ingenious and extraordinary personages of his time, and may even be considered

as a prodigy in mechanical acquirements, we take the liberty of stating all we know of discoveries in secret writing, partly divulged by himself in his very scarce volume of "Inventions," and partly collected from a MS. in the Harleian Library, No. 2,428, which bears clear internal marks of its origin, although it was not supposed to be his until we lately convinced the librarian. "The one-line cipher," and mode of dot-writing are thus entitled in the above manuscript: "An explanation of the most exact and most compendious way of short writing, and an example given by way of questions and resolves upon each significant point, proving how and why it stands for such and such a letter, in order alphabetically placed in every page." His method of writing is shown in *fig. 5, Plate I.* An engraved page is given to write upon, in which are made horizontal rows of octagonal squares or checkers, and a straight line is to be drawn from the centre toward the circumference of these squares, in different positions and of various lengths for each letter of the alphabet. Thus A is a short horizontal stroke, made to the right hand, and not touching the circumference; I is the same stroke passing close to the circumference; R is the same stroke going beyond the circumference; E, N, and W are represented by a similar stroke, in the opposite direction, but varying in their lengths. By a like method he suggests that we may write with a dot, or single point only, which is to be placed at a certain distance, and in a certain direction, from the centre of the octagon, for each letter of the alphabet.

The Marquis proposes this contrivance for the purpose of writing with secrecy, as well as with brevity, and leaves it to the will of any person to change the value or name of the letters, as it may suit his fancy or intention, "The points to be written," says he, "and read as they precede or as they are the one above the other," and for the sake of expedition as well as for "husbanding paper," he advises "to omit all

“needless and unsounding letters,” as we do in short-hand writing.”

This ingenious plan is better adapted for secret writing than for short-hand, and yet we do not think it would be difficult to decipher anything written in this way, unless the writer were to change the power of his letters very frequently, because he would not otherwise be able to elude the common rules for deciphering.

That the Marquis had turned his attention particularly to this subject is strikingly evident from the following passages contained in his very curious book entitled “A Centurie of the Names and Scantlings of Inventions by me already practised :”

No. 5. “A way by a circular motion, either along a rule or ring-wise, to vary any alphabet, even this of points, so that the self-same point individually placed, without the least additional mark or variation of place, shall stand for all the twenty-four letters, and not for the same letter twice in ten sheets writing; yet as easily and certainly read and known as if it stood but for one and the self-same letter constantly signified.”

No. 6. “How at a window, as far as eye can discover black from white, a man may hold discourse with his correspondent without noise made or notice taken, being according to occasion given and means afforded, *ex re natá*, and no need of provision beforehand, though much better if foreseen, and means prepared for it, and a premeditated course taken by mutual consent of parties.”

No. 7. “A way to do it by night as well as by day, though as dark as pitch is black.”

No. 32. “How to compose an universal character methodical and easie to be written, yet intelligible in any language; so that if an Englishman write it in English, a Frenchman, Italian, Spaniard, Irish, Welsh, being scollars, yea, Grecian,

“ or Hebritian, shall as perfectly understand it in their own  
 “ tongue as if they were perfect English, distinguishing the  
 “ verbs from nouns, the numbers, tenses, and cases as properly  
 “ expressed in their own language as it was written in Eng-  
 “ lish.”

No. 33. “ To write with a needle and thread, white, or any  
 “ color upon white, or any other color, so that one stitch  
 “ shall significantly show any letter, and as readily and easily  
 “ show the one letter as the other, and fit for any language”

No. 34. “ To write by a knotted silk string, so that every  
 “ knot shall signify any letter, with comma, full point, or in-  
 “ terrogation, and as legible as with pen and ink upon white  
 “ paper.”

No. 35. “ The like by the fringe of gloves.”

No. 36. “ By stringing of bracelets.”

No. 37. “ Pinck’d gloves.”

No. 38. “ By holes in the bottom of a sieve.”

No. 39. “ By a lattin or plate lanthorn.”

Nos.  $\left. \begin{array}{l} 40. \text{ “ By the smell.”} \\ 41. \text{ “ By the taste.”} \\ 42. \text{ “ By the touch.”} \end{array} \right\}$  “ And by these three senses

“ as perfectly, distinctly, and unconfusedly, yea, as readily as  
 “ by the sight.”

No. 43. “ How to vary each of these so that ten thousand  
 “ may know them, and yet keep the understanding-part from  
 “ any but their correspondent.”

No. 51. “ A rule of gradation, which, with ease and method,  
 “ reduceth all things to a private correspondence, most useful  
 “ for secret intelligence.”

No. 52. “ How to signify words and a perfect discourse by  
 “ jangling of bells of any parish church, or by any musical  
 “ instrument within hearing, in a seeming way of tuning it,  
 “ or of an unskilful beginner.”

No. 75. “ How a tape or ribbon-weaver may set down a

“ whole discourse, without knowing a letter, or interweaving  
 “ anything suspicious of other secret than a new-fashion  
 “ ribbon.”

No. 76. “ How to write in the dark as straight as by day-  
 “ light.”

Our limits for this article do not allow us to enter into the merits of every proposal made public for secret correspondence ; but, having before observed that arithmetical figures had become very common in the reign of Charles I., instead of the ciphers previously employed, we shall here offer a few remarks on their use. The celebrated and profound mathematician Dr. Wallis deciphered a great number of intercepted letters, written in figures, about the period of that monarch's unhappy controversy. We have already said that copies of these deciphered papers are deposited in the Bodleian library, at Oxford, and in the prefatory observations to that collection Dr. Wallis declares his judgment of them in these words: “ I  
 “ would not desire to use a better cipher than most of those.  
 “ \* \* \* \* I do scarcely believe that it will be an easy  
 “ matter to contrive a way more intricate than the *figure-*  
 “ *cipher*, ordinarily now in practice, with the like convenience  
 “ for use, and if any affect some more perplexed than these, I  
 “ doubt not but his supposed better way will be equally ob-  
 “ noxious to a discovery, or else will be extremely tedious in  
 “ use, both to him that writes by it and to him that is to read  
 “ it, that it will not admit of any tolerable despatch.” (See also Mr. Davy's “ Essay on Deciphering,” p. 17. General Dictionary, vol. x., p. 93 ; and Biographia Britannica, Art., WALLIS.) This acute author was very different from Scaliger in his opinion of secret writing ; for, while the latter ridiculed the idea of inscribing what could never be developed, because he was able to decipher the Lacedæmonian *scytale*, Dr. Wallis, on the contrary, who had gone fifty times deeper in this science than Scaliger, admits “ there may be a cipher so intricate as shall be beyond the art of man to disclose.”

No person except Vieta (a French mathematician, who was employed by Francis I), had discovered near so much skill in deciphering as Dr. Wallis. He seems not to have known of what Vieta did in his way, nor had he any aid from other persons in his researches; we are, therefore, disposed to pay the greatest deference to his judgment as a decipherer, but we beg leave to observe that it does not follow he should know all the possibilities of this multiform art. He considered the "figure-cipher," as extremely intricate; we doubt not, that others may be contrived equally so, and that superadded to this quality a cipher may be adapted for greater despatch, "both to him that writes by it and to him that is to read it." Besides which, we think it even practicable to invent a cipher, exclusive of its having those properties which shall not be much exposed to suspicion; and this, we conceive, with Lord Bacon, to be a very essential requisite in certain situations of the writer and reader, though not so in all circumstances.

There is a method of employing figures common enough in the present day, which was much recommended by Baptista Porta and Cardanus, and therefore not a novel invention; but Blaise de Vigenere, whose treatise on ciphers was published at Paris in 1587, has pointed out the inconveniences of this method, which consists in referring to words or sentences by the corresponding pages and lines of some rare printed book, in the possession of the confederate parties. Now, says Vigenere (p. 208), this plan is too laborious and slow in operation for business requiring to be described in detail; it will not always provide the words sought for, at least without an immense deal of pains, perhaps after examining through some hundred pages; and unless a dictionary be used, the names of persons, places, or professions, can be found in no book whatever; besides which, many accidents may lead to the discovery of the key or book so confided in; and many others may happen to deprive us of that resource, or to render it inconvenient to depend on such a stratagem. The writing, moreover, is always liable to

suspicion if intercepted. So that this plan is wholly unfit for extensive correspondence, as in diplomatic affairs, and ought rather to be accounted a childish than a scientific invention, however it has been sanctioned by modern practice among military commanders and officers of state.

We do not object altogether to the use of figures and numeral characters as if they were unfit *on account of their form*, to be adopted in cryptographical writing, but we object to the above manner of applying them, because as numerals, denoting only the pages or lines of a book, these figures cannot be written with any tolerable expedition, and must be a perpetual check to the reader's progress in deciphering. This method, it must be acknowledged, possesses the property of being undecipherable without the key; for let us suppose (in writing the example given by Mr. Thicknesse), "That the parties agree to correspond by Newton's first edition of Milton, and thereby direct each other in their letters, to such a page, such a line, and such a word; it may be asked, who would be able to find out that their writing page 7, line 2, words 3, 4, 5, and vol. ii, page 8, line 19, word 4—the same page, line 9, words 3, 4, and 5—was to say, 'The Western empire is degenerated into licentiousness,' without being told that these words will be found in the first and second volumes of Barnesworth's translation of Machiavel's works; the first three words from his History of Florence, and the remainder from his 'Political Discourses on the First Decade of Livy.'" All this will be granted; but as the property of being intricate is not the only one we should look for in a good cipher, we conclude again by observing that the above plan is puerile and unscientific to the last degree; consequently, that it is wholly unfit for men of business, or for any besides incidental occasions, where very little writing is required.

By referring to a dictionary, indeed, these objections are partly lessened because the words may be found with greater facility than in other books; but even such a resource is very

insufficient for all occasions, and it still must prove a most tedious and operose employment in writing only ten or a dozen lines. The French encyclopædists describe a much more feasible mode of writing by figures, which, nevertheless, we cannot approve as the best method of ciphering. It is this :

The correspondents agree on a set of figures to represent all the letters of the alphabet, and also a great many words or phrases. Several ways may be adopted for the representation of any important letter or phrase of frequent occurrence ; such as the five vowels or the words France, emperor, king of this and that nation, states, general, cardinal so and so, the allied armies, an ambassador's name, &c. All these different words are to be classed and arranged in such a manner as to be easily found, both in writing and deciphering ; and another classification must be made, in which the figures stand first and the words in an opposite column. The sentences and entire paragraphs, which are of prime importance in a despatch, should be written wholly in cipher, without any intermixture of common letters ; because by the aid of particles and connecting words, the terms of greater consequence, on which the sense hinges, will often be discovered, and the matter in debate or agitation will thus be understood. It is also proper to write the lines so far apart that the decipherer may subscribe the figures when he reads the despatch, as in the following specimens :

Le ministre d'ici est tout dévoué aux intérêts de la France  
 102 25 44 9 1200 70 330 888  
 c'est le fruit de dix mille Louis semées à propos.  
 54 5 20 60 101 19 501 80

The negotiation is interrupted by the pertinacity and un-  
 2 999 4 10 50 1000 14  
 reasonableness of the Duke, who probably has received  
 350 31 86 5 77 680  
 private instructions from his court.  
 1110 21 89 231

Means may be devised for detecting the unfaithfulness of a subordinate secretary who is supposed to have communicated his cipher to a foreign power. The court may demand of its minister abroad, or the minister require of his court something quite the reverse of what is desired, it being previously agreed by the cabinet that a certain mark or private sign denotes opposition or annihilation, with respect to the particular thing annexed to the said sign. This special mark may be called the annulling sign, and will serve for various important uses; as has often been proved in conducting naval signals, where the enemy was in sight, or where any mistake happened to arise in the course of a correspondence. By the help of such an artifice, when a cipher has been accidentally discovered or traitorously disclosed, a skilful negotiator will be able to deceive the enemy, and lead him into inextricable errors, which may finally turn to the advantage of his own cause.

Sir I. Ware, Colonel Vallancey, and Mr. Astle give remarkable accounts of the Irish steganography, by means of peculiar alphabets, called by the barbarous name of ogums or oghams, of which there are three kinds: the first is composed of strokes and marks, that derive their power from certain positions with respect to one horizontal line, over, or under, or upon which they are drawn; this principal line serving for a rule or guide, its upper part being named the left and its under part the right. The characters or short strokes, by their number or situation, represent not only single vowels and consonants, but also diphthongs and triphthongs.

In our *Plate I., fig. 3*, is seen one of the most simple oghams, copied from Sir I. Ware's "Antiquities of Ireland," (vol. ii., p. 20), which would not be very difficult to decipher; because, although the number of diagonal and perpendicular marks is considerable, it must be obvious how many of them represent one letter, and it will be seen that they make up but twenty-six in all. The marks for diphthongs and triphthongs

do not occur in ancient manuscripts, the vowels being represented singly, as *æ*, not *æ*, &c. Therefore, an ogham having diphthongs, such as that we have selected, cannot be regarded as of ancient date.

The second and third kinds of oghams used by the Irish, differ chiefly in this: that the letter *b* or *c* is placed first, instead of *a*; or, that the mark for one of those letters is substituted for all the vowels, by doubling or reversing it, and by its frequent repetition, so as to confuse the writing. (See "Tractatus apud Hibernos veteres, de occultis scribendi formulis, seu Artificiis Hibernicè ogum dictis;" a MS. lately given to the British museum by the Rev. Dr. Miller.)

Several specimens of Irish oghams are engraved in the second edition of Mr. Astle's "History of Writing," a work replete with interesting matter on various points connected with that subject in general, but extremely deficient on short writing (stenography), and secret writing (cryptography). Upon these two departments of the art, we feel a desire, if opportunity should permit, of laying before the public some results of our own investigations and practice; though we cannot indulge the vain opinion of our feeble efforts which Trithemius entertained of his learned labors: ("Præf. ad Maximil. Imperatorem, Polygr.," p. 100.) "In manibus jam habeo grande opus, quod si unquam fuerit publicatum, totus mundus mirabitur." (See the article on STENOGRAPHY, "Rees' Cyclopædia.")

It might be thought an injustice to the memory of the profound and noble Chancellor Bacon, not to state in detail whatever his lordship has written upon ciphers; as some men of acknowledged ability (for instance, Bishop Wilkins and Mr. Falconer), have considered his proposals superior to every other. Mr. Falconer calls it "the most ingenious method extant;" and the Bishop of Chester says: "This way of writing is justly to be preferred before any other, as containing in it

“more eminently all those conditions that are desirable in such  
“inventions, viz. :

- “1. 'Tis not very laborious either to read or write.
- “2. 'Tis very difficult to be deciphered.
- “3. 'Tis void of suspicion.”

We find the following encomium in Mr. Thicknesse's Treatise: “Those who are acquainted with Lord Bacon's great  
“depth of capacity, will readily agree with me that a secret  
“method of writing contrived by a man of his amazing penetration must be superior to all others, as, indeed, it is, and  
“contains the highest degree of cipher.”

We copy the illustrious Verulam's own proposal, out of Dr. Shaw's edition of his works, vol. i., pp. 141-145 :

“There are several kinds of ciphers; as the *simple*; those  
“mixed with non-significants; those consisting of two kinds of  
“characters; *wheel-ciphers, key-ciphers, word-ciphers, &c.* There  
“are three properties required in ciphers, viz.: (1.) that  
“they be easy to write and read; (2.) that they be trusty  
“and undecipherable; and, (3.) if possible, clear of suspicion.  
“For, if a letter should come into the hands of such as have  
“power over the writer or receiver, though the cipher itself be  
“trusty and impossible to decipher, 'tis still subject to examination and question, unless there be no room to suspect or  
“examine it.

“There is a new and useful invention, to elude the examination of a cipher, viz.: to have two alphabets, the one of  
“significant and the other of non-significant letters; and folding up two writings together, the one conveying the secret,  
“whilst the other is such as the writer might probably send  
“without danger. In case of a strict examination about the  
“cipher, the bearer is to produce the non-significant alphabet  
“for the true, and the true for the non-significant; by which

“ means the examiner would fall upon the outward writing,  
 “ and finding it probable, suspect nothing of the inner.

“ But to prevent all suspicion, we shall here annex a cipher  
 “ of our own, which has the highest perfection of a cipher—  
 “ that of signifying omnia per omnia, anything by everything,  
 “ provided only the matter included be five times less than  
 “ that which includes it, without any other condition or limita-  
 “ tion. The invention is this: first, let all the letters of the  
 “ alphabet be resolved into two only, by repetition and trans-  
 “ position; for a transposition of two letters through five places  
 “ or different arrangements will denote two and thirty differ-  
 “ ences, and consequently fewer, or four and twenty, the num-  
 “ ber of letters in our alphabet, as in the following example :

“ *A bilateral alphabet, consisting only of a and b changed through*  
 “ *five places, so as to represent all the letters of the common*  
 “ *alphabet.*

|           |           |           |
|-----------|-----------|-----------|
| A = aaaaa | I = abaaa | R = baaaa |
| B = aaaab | K = abaab | S = baaab |
| C = aaaba | L = ababa | T = baaba |
| D = aaabb | M = ababb | V = baabb |
| E = aabaa | N = abbaa | W = babaa |
| F = aabab | O = abbab | X = babab |
| G = aabba | P = abbba | Y = babba |
| H = aabbb | Q = abbbb | Z = babbb |

“ Thus, in order to write *A*, you write five *a*'s, or aaaaa;  
 “ and to write *B*, you write four *a*'s and one *b*, or aaaab; and  
 “ so of the rest.

“ And here, by the way, we gain no small advantage, as  
 “ this contrivance shows a method of expressing and signify-  
 “ ing one's mind, to any distance, by objects that are either  
 “ visible or audible, provided only the objects are but capable  
 “ of two differences; as bells, speaking trumpets, fire-works,

“&c. But for writing, let the included letter be resolved into this biliteral alphabet. Suppose that letter were the word *Fly*, it is thus resolved :

|       |       |       |
|-------|-------|-------|
| F     | L     | Y     |
| aabab | ababa | babba |

“Let there be also at hand two other common alphabets, differing only from each other in the make of their letters, so that as well the capital as the small be differently shaped or cut, at every one’s discretion ; as thus, for example, in Roman and italic, each Roman letter constantly representing A, and each italic letter B.

“The first, or Roman alphabet :

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

“All the letters of this Roman alphabet are read or deciphered by translating them into the letter A only.

“The second, or italic alphabet :

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

“ All the letters of this Italic alphabet are read by translating them into the letter *B* only.

“ Now adjust or fit any external double-faced writing, letter by letter, to the internal writing, first made biliterate, and afterwards write it down for the letter or epistle to be sent. Suppose the external writing were *Stay till I come to you*, and the internal one were *Fly*, then, as we saw above, the word *Fly*, resolved by means of the biliteral alphabet, is

F     L     Y,  
aabab ababa babba

“ whereto I fit, letter by letter, the words *Stay till I come to you*, observing the use of my two alphabets of differently shaped letters, thus :

aabab ababa babba  
*Stayt ilico metoyou*

“ Having now adjusted my writing according to all my alphabets, I send it to my correspondent, who reads the secret meaning by translating the Roman letters into *a's* and the Italic ones into *b's*, according to the Roman and Italic alphabets, and comparing each combination of five of them with the biliteral alphabet.

“ This doctrine of ciphers has introduced another relative to it, viz. : the art of deciphering, without the alphabet of the cipher, or knowing the rules whereby it was formed. This, indeed, is a work of labor and ingenuity, devoted, as well as the former, to the secret service of princes. Yet, by a diligent precaution, it may be rendered useless ; though, as matters now stand, 'tis highly serviceable. For if the ciphers in use were good and trusty, several of them would absolutely elude the labor of the decipherer, and yet remain commodious enough, so as to be readily wrote and read ; but through the ignorance and unskilfulness of secretaries and clerks in the courts of princes, the most important affairs are generally committed to weak and treacherous ciphers.”

It becomes us to offer our opinion with extreme diffidence, in presuming to criticise the production of a man so highly distinguished for his capacity and acuteness. But we cannot refrain from believing, that this contrivance of Lord Bacon will appear to most persons too operose and slow of execution for public business; of which, indeed, we desire no better proof, than that it has met with so little encouragement from official and regular practice. It must always be deemed a serious inconvenience attending his lordship's plan, that it requires at least five times more labor than is requisite in ordinary writing. Whereas, if a triformed alphabet were to be invented in lieu of this, and regulated by another alphabet composed of three letters instead of two, the secret writing would then bear only a triple proportion to common writing, and the trouble of an amanuensis might thus be greatly diminished.

A second point on which we beg leave to express our doubt is, whether this cipher be infallibly secure against the scrutinizing eye of a diligent examiner. For if the reader were to place a mark of distinction between every fifth character, reckoning the five as one letter, we ask, Why might not this writing be liable to a discovery as well as any simple cipher, and on the same general principles? Nay, Mr. Falconer himself confesses it may, notwithstanding the compliment he pays to the noble author for his ingenuity and learning. Nevertheless, we think it will be granted on all hands that Lord Bacon's mode, if it had not been published, would have possessed one rare and valuable property beyond the ciphers previously invented, namely, that of being scarcely at all exposed to suspicion; and therefore, in this respect, it is entitled to special attention and praise.

Bishop Wilkins avails himself of the fact, that two signs repeated, as in Lord Bacon's alphabet, or three combined in a certain order, will serve to communicate our thoughts; and he improves upon it in the following manner: Let there be two

bells of different notes, or one bell and some other loud sound, as that of a musket, horn, drum, &c. According to the plan of a biliteral alphabet, a man may express any letter by two such different sounds, repeating them five times. But if the sounds were capable of a triple difference, then each letter may be expressed by a three-fold sound; and if they contain a quintuple difference, or consisted of five sounding instruments, every letter might be signified by two of them only; as we have shown already with two flambeaux, and as will be further obvious from our subsequent remarks.

He quotes a story from John Baptist Porta, in lib. i., cap. 6, of his work, "*De Furtivis Literarum Notis, Vulgo de Ziferis*," who relates, that when the citizens at the siege of Navarre were reduced to the greatest extremity, they communicated their wants to their distant friends by discharging various kinds of cannon in the night time, according to a preconcerted order; by which means they obtained such supplies as they needed, and preserved their city. But the most curious proposal for the management of sounds in correspondence, is that of expressing letters and words by the ordinary notes of a musical instrument; which Bishop Wilkins believed might be adapted "for a universal language, and the writing of them for a universal character," not by expressing words, "but things and notions." Then, says he, "there might be such a general language as should be equally speakable by all nations and people."

We are not sanguine enough to expect the learned bishop's plan of recovering the world from the Babel confusion will very quickly take effect; and certainly the specimen of musical writing which he has exhibited is very unlikely to answer that purpose. Mr. Thicknesse thinks, "writing performed by an harmonic alphabet would be the most void of suspicion of all others;" both he and the bishop have, therefore, given an alphabet of this kind, and they both presume on

his lordship's being "the only writer who has mentioned the method of writing by musical notes;" wherein, however, they are both mistaken. For Augustus, the Duke of Brunswick (*alias* Gustavus Selenus), in his "System of Cryptography," lib. vi., cap. 19, exhibits various specimens of writing in that way, and does not claim the invention himself, but ascribes it to Count Frederic of Oetingen. Nay, it is pretty clear that Trithemius was not ignorant of this device; since he declares, in his epistle to Bostius, A. D. 1499, that he could discourse by playing on the organ, or singing, "ludendum in organo vel cantandum," which seems to be the proposal above mentioned, or something very like it.

That we may not appear to have slighted so curious a proposal, we will offer a few remarks on this subject; and beg our readers to consult *Plate II.*, *figs.* 2, 3, 4, and 5; where we have given a harmonic alphabet, and several specimens of musical writing, an illustration of the present article.

If four or five characters be amply sufficient, by combination and repetition, to denote every word or idea we can express, it is certain that seven musical sounds are more than sufficient for the same purpose. But we must learn to distinguish between these sounds, as they would be represented in ordinary writing, and the scientific arrangement of them, so as to form a musical composition; for those two results may happen to be as different from each other as the chattering of a magpie and the orations of Cicero, or as the jumbling of letters in a box, and the adjustment of them by a typographer.

It is true that the seven musical notes are enough in respect to number (for seven notes will afford five thousand and forty varieties or combinations, without repeating any of them); but we are not therefore to conclude, that they can be made to coalesce and harmonize, according to the practice-order and relation we should wish them in alphabetical writing.

Articulate sounds are represented on paper, &c., by certain

substitutes called letters, which possess whatever quality we may choose to impose on them; but harmonic tones are not at all controllable by arbitrary laws; their inherent powers are fixed by nature; they cannot, therefore, be made subservient to our preconceived methods of speech, or our established notation by letters; and if they are compelled to associate with these, it must be managed by the subversion of our common language, and adapting its structure to the natural qualities of musical sounds. This being our opinion, we should as soon expect a man to converse in two different languages at once, or the wind to blow in two opposite directions, as the laws of harmony to obey any existing plans of articulation and writing. See the article HARMONY, “Rees’ Cyclopædia.”

Having thus freely given our deliberate view of this subject, we lay before the reader some observations of Mr. Philip Thicknesse, who has labored more earnestly than any other author to enlist the powers of harmony into the service of cryptographers. As his opinion differs from our own, we do him the justice to adduce his words at full length. In the specimens of musical composition, however, we have corrected several of that gentleman’s errors; so that his remarks will not suffer any loss from our officiousness.

“Bishop Wilkins, in his chapter relative to a language consisting of tunes and musical notes, without any articulate sound, says, ‘If the musical instrument that is used for this purpose, be able to express the ordinary notes, not only according to their different tones, but their times also, then may each letter of the alphabet be rendered by a single sound; whence it will follow, that a man may frame a language, consisting only of tunes, and such inarticulate sounds as no letters can express, which kind of speech is fancied to be usual among the lunar inhabitants; who, as Domingo Gonzales hath discovered, have contrived the letters of the alphabet upon the notes after some such

“ ‘order.’ But the specimen the bishop has given (by writing  
 “ *Gloria Deo sole*, by minims, on musical lines), will instantly  
 “ appear to any one the least conversant with music, that  
 “ being without harmony or time, it must have no meaning,  
 “ or that some hidden matter is thereby disguised. I shall  
 “ therefore endeavor to write down an alphabet by musical  
 “ notes, in such a manner, that even a master of music shall  
 “ not suspect it is to convey any meaning but that which is  
 “ obvious; and I am persuaded an alphabet of musical notes  
 “ may be so contrived that the notes shall not only convey the  
 “ harmony, but the very words of the song, so that a music-  
 “ master (which is too often his design) may instruct his  
 “ female pupil not only how to play upon an instrument, but  
 “ how to play the fool at the same time, and impose upon  
 “ her parents or guardians, by hearkening to his folly, imper-  
 “ tinence, and wickedness. When a music-master has once  
 “ taught his female pupil to understand a musical alphabet,  
 “ and she will permit him to carry on a secret correspondence,  
 “ he may send her daily a lesson which she may repent having  
 “ learned as long as she lives.

“ In the plate annexed, I have given a musical alphabet  
 “ (*Plate II., fig. 2*), and under it a specimen to explain more  
 “ fully my meaning (See *Plate II., fig. 3*). If a music-master  
 “ be required to play it, he will certainly think it an odd, as  
 “ well as a very indifferent composition, but neither he, nor  
 “ any other person, will suspect that the notes convey also the  
 “ two following harmonious lines from Dr. Goldsmith’s ‘*De-  
 “ serted Village.*’

“ ‘Near yonder copse, where once the garden smil’d,  
 “ And still where many a garden flow’r grows wild.’

“ Now it may be so ordered that the plain notes, *i. e.*, the  
 “ crotchets and minims alone, compose the alphabet, and that  
 “ neither flats nor sharps, nor the smaller notes between (which

“ may be placed as mere graces, and meant to deceive), have  
 “ anything to do with the reading; so that the decipherer  
 “ would not so readily know how to proceed, and many people  
 “ there are who will think it impossible to be made out with-  
 “ out the key; yet I am persuaded one who possesses a very  
 “ moderate turn for such business would read it in a very short  
 “ time.

“ If the words of a song could be thus conveyed by the notes  
 “ as well as the air, it would, exclusive of the contrivance, be  
 “ of infinite service and ease to ladies who sing; indeed, it  
 “ seems to those who are not acquainted with music, almost  
 “ inconceivable how a person at first sight shall be able to read  
 “ the bass and treble staff together with the words, and play  
 “ two parts and sing one at the same time. It is certain that  
 “ two musicians might, by a very little application, carry on a  
 “ correspondence with their instruments: they are all in pos-  
 “ session of the seven notes which express *a, b, c, d, e, f, g*;  
 “ and know by ear exactly when either of these notes are toned;  
 “ and they are only to settle a correspondence of tones for the  
 “ remaining part of the alphabet; and thus a little practice  
 “ might enable two fiddlers to carry on a correspondence  
 “ which would greatly astonish those who did not know how  
 “ the matter was conducted. Indeed, this is no more than  
 “ what is called *dactylogy*, or *talking on the fingers*, which I have  
 “ seen done, and understood as quickly and readily, almost, as  
 “ common conversation.

“ A secret correspondence may be carried on by musical  
 “ notes or by communicating the words of a song, by the same  
 “ vehicle which points out the time and harmony, and this  
 “ may be done (without having any knowledge of musical  
 “ compositions) by any piece of common music whatever. To  
 “ do this, an alphabet must be formed as in *Plate II., fig. 2*, or  
 “ in any other manner, for it may be contrived much better for  
 “ the purpose.

“Then take any piece of music (but such as is composed of  
“the greatest variety of notes will be best) and copy it out  
“upon ruled music-paper, leaving one row of blank lines  
“between, *i. e.*, those lines on which the second or bass is  
“usually written. When you have copied the whole out,  
“draw straight lines on the bass cliff exactly under those  
“which divide the time in the treble. Suppose you would  
“write ‘My time, O ye muses,’ &c., look for the note which  
“is *m* in your alphabet, and then for *y*. Now, suppose there  
“are eight or ten notes between the *m* and the *y*, then those  
“are to be marked as nulls on the bass cliff, just under each  
“note, by that mark which in music imports a rest, which is  
“this  $\sim$ , and the confederate who has the key, knowing that  
“the rest-notes are nulls, only makes use of those which are  
“open, or which may be pointed out, by inserting other notes  
“exactly under them in the bass cliff; and if the under notes  
“are placed three notes lower on the lines than those in the  
“treble are, they will in that case be in harmony, and the rests  
“between being in such an order, will prevent any suspicion  
“except to those who understand music; and yet even those  
“who do would hardly suspect that the notes of Lady Coven-  
“try’s minuet implied, as it might, an assignation in Gros-  
“venor square; or, instead of the rests being under the nulls,  
“as they will of course be very frequently, they might be  
“placed only under those notes which convey the reading, and  
“then the bass cliff would appear as busy as the treble, and  
“tend the more to perplex the decipherer, as he could not be  
“sure but both lines were employed to conceal the private  
“writing; indeed, where letters fall very distant from each  
“other in the treble, it might be supplied, and frequently,  
“too, on the bass cliff, and signified by a dot or some other  
“musical character placed near the treble more immediately  
“above it. A letter thus written in cipher, would disconcert  
“even a good decipherer, and throw him out of the methodical

“ way of coming at the secret contents ; indeed, I rather think  
 “ it must be come at more from ingenuity than method.

“ This, however, is a hint only, how this kind of cipher may  
 “ be completely made use of, rather than a perfect method ; but  
 “ I am persuaded that a good composer of music would be able  
 “ to write any common epistle with the assistance of the treble  
 “ and bass cliff, so as to have very few null notes, and the secret  
 “ meaning instantly obtained by those who are in possession of  
 “ the harmonic alphabet. Or, suppose every crotchet or minim  
 “ which is to express a letter is written with the tail of the  
 “ note downward, and all the nulls upward ; this, indeed,  
 “ might occasion some awkwardness in the appearance of the  
 “ music, but it would not tend at all to a discovery ; but still,  
 “ what I think practicable is, that an harmonic alphabet may  
 “ be so contrived by a good composer of music that every note  
 “ shall be expressive of a letter, and convey the words of the  
 “ song as perfectly to the eye as they do the harmony to the  
 “ ear. The composer of an harmonic alphabet should be care-  
 “ ful to include those notes which are most frequently used into  
 “ his alphabet ; and those, I think, are on or between the five-  
 “ ruled music lines ; but he must carefully avoid having any of  
 “ those notes already so well known to express *a, b, c, d, e, f,*  
 “ *g*, keeping their proper place ; for that would be the first con-  
 “ sideration of an ingenious decipherer.

“ Now, if this art of writing secretly by musical notes was to  
 “ be practised, I question whether a decipherer, to be expert in  
 “ his art, must not only be a master of languages, but even a  
 “ disciple of Apollo. However, according to the musical  
 “ alphabet annexed, provided a letter is written by it, and the  
 “ active notes well chorded between with nulls upon the same  
 “ lines, which might be known to be such by the tail being  
 “ turned up or down, or characterized by the mark for a beat,  
 “ a shake, a trill, a pause, a flat, or a sharp, it would be scarce  
 “ possible for a decipherer to make out with certainty the

“sense; and this method, unpublished, would be the least  
“liable to suspicion; for who that examined a suspected mes-  
“senger would think an old song without words, in which,  
“perhaps, the messenger’s tobacco or snuff might be put, con-  
“tained the secret he was to convey? Nor could an ordinary  
“messenger, either by bribes or threats, discover anything more  
“than that the bearer was strictly charged to deliver that piece  
“of music into which he puts his tobacco, to such a particular  
“person.

“It may seem at first difficult to remember what letters the  
“notes imply, and I should have thought so too, had not the  
“making out of the alphabet only impressed my mind with the  
“remembrance of every letter; and yet I cannot boast of hav-  
“ing a good memory; but upon trying the experiment in my  
“family, I find that it is attainable by writing them down two  
“or three times, without any further trouble. Indeed, to  
“remember a name or a word, it is best done by writing it  
“down, though it be only with the finger, upon a table, with-  
“out any mark, as the having turned the form of the letters  
“by the hand will greatly assist the memory.

“Bishop Wilkins thinks it possible that if inarticulate sounds  
“can be contrived to express not only letters and words, but  
“things and notions, then there might be such a general lan-  
“guage formed as might be equally speakable by men of all  
“nations, and so restore to us what we lost by the second gen-  
“eral curse, which is yet manifested unto us, he says, not only  
“in the confusion of writing, but also in speech. But I am  
“apprehensive this universal language may sleep quietly with  
“the ‘flying chariot’ the same author was once so busy in con-  
“structing.

“In the specimen given (in *Plate II., fig. 3*) of secret writing  
“by the harmonic alphabet, it must be observed that every  
“note implies a letter also; and, consequently, under such a  
“restraint, it can only have the appearance and be the picture

“ of music without harmony; yet it is such a picture as must  
 “ pass unsuspected by all who do not understand music thor-  
 “ oughly, and by many who do; at least those who do would  
 “ most likely consider it only a wretched attempt to compose  
 “ music without suspecting that the notes conveyed two lines  
 “ of true poetic harmony from that sweet poem of Dr. Gold-  
 “ smith, ‘The Deserted Village,’ and, therefore, this method  
 “ is in one respect to be preferred to every other yet practised  
 “ of secret writing, *i. e.*, that it is least liable to suspicion. An  
 “ itinerant fiddler or musician, with his dog’s-eared music-book  
 “ in his pocket, might get admittance into or from a town  
 “ besieged, unsuspected. A tune might be pricked down in  
 “ his book, among many others, and he might be desired to  
 “ give a copy of it to any particular person where he is going,  
 “ without suspecting the mischief or good office he is employed  
 “ to execute, and consequently unable to betray the secret;  
 “ and though suspicion should arise, how will the decipherer  
 “ know which among a great number of musical airs, conceals  
 “ the secret information?

“ In this case a good decipherer should be a good musician  
 “ also, that he may pick out the most uncouth and constrained  
 “ composition; for that would most likely prove to be the  
 “ harmonic epistle. Therefore, to obviate this, and to render  
 “ the matter less liable to suspicion and much more difficult to  
 “ be deciphered (in *Plate II.*, *fig. 4*), an air composed of treble  
 “ and bass, according to the rules of true composition, is given.  
 “ In this plate there are a great number of null notes to fill up  
 “ and to complete the harmony. The confederate, who is in  
 “ possession of the key and alphabet, will know the null notes  
 “ by their tails being all turned upward; and therefore he  
 “ passes over them, and takes down in order, from the bass  
 “ and treble cliff, those only which are turned downward, a  
 “ circumstance which would greatly perplex the decipherer,  
 “ first, to find out whether all the notes were active; secondly,

“ whether the bass and treble cliff were both employed ; and  
“ lastly, which were the null notes. Yet this method is not  
“ without some inconveniences, and such as would create sus-  
“ picion or surprise in an examiner who understands music ;  
“ for, being confined to turn all the nulls one way and the  
“ active notes the other, it must sometimes happen that both  
“ must be occasionally constrained, and the tails frequently  
“ turned contrary to the usual practice of writing music.

“ It is possible to render this method of writing still more  
“ secret by placing a very thin bass under the treble, and to put  
“ rests, &c., under some of the active notes, and to point out  
“ the other by a mixture of liquor (of which there are many)  
“ that would not appear till the paper is held to the fire, dipped  
“ in water or fine dust thrown over it ; and under all these  
“ impediments it would be very difficult to come at the secret  
“ matter ; yet it is what a good decipherer would not, I believe,  
“ give up as a thing not to be done.

“ Were I, however, under a necessity to send a letter of the  
“ utmost importance, which was to pass through the hands or  
“ under the inspection of cautious examiners, I should think a  
“ good piece of harmonic composition without any words an-  
“ nexed to it, the safest and most secret vehicle to convey it  
“ under. In letters, where it is necessary to be particular as to  
“ the day, month, or even the hour, that may be done by a kind  
“ of short hand ; for it would be very unsafe to write, though  
“ in ciphers, *Dear sir*, at the top of a letter, or *your humble*  
“ *servant*, at the bottom ; or even the month, the year, or the  
“ day of the month, as those words would be first examined by  
“ a decipherer. To avoid any of these clues, therefore, where  
“ the month and the day are to be given, it may be conveyed  
“ according to the Quaker’s *by-way*. Let the twelve first  
“ music lines be considered to stand for the twelve months of  
“ the year, and then counting from the first to the thirty-first,  
“ the days of the month. If, therefore, I would date my letter

“ the 8th of April, a small dot on the fourth line preceding the  
 “ first note, as in *Plate II., fig. 4* would imply the *fourth month*,  
 “ and a little dash across the eighth line, in the same manner,  
 “ would show it to be dated the *eighth day* of the *fourth month* ;  
 “ and a little *x* from the first to the twelfth line, would imply  
 “ any particular hour in the day ; or an *o*, the hour of the  
 “ night.

“ It is very certain that if such a sentence as the specimen in  
 “ *Plate II., fig. 4*, contains, can be conveyed by a few lines of  
 “ music, a long letter may easily be framed within the compass  
 “ of an Italian air in score ; nay, that *any* Italian piece of  
 “ music of a tolerable length, may, by writing it with the tails  
 “ properly turned up or down, according to the specimen here  
 “ given, be made the vehicle of a letter or a piece of important  
 “ information ; and still more easily might a good composer  
 “ convey the words and the harmony also by the same char-  
 “ acters.

“ I am convinced that a good composer of music, either by  
 “ framing the harmony by the alphabet or the alphabet by the  
 “ harmony, may not only render every note active, but by har-  
 “ monic alphabets, might write two letters on different sub-  
 “ jects, one in the treble cliff and the other in the bass ; and it  
 “ is evident, therefore, from the specimen I have given, that the  
 “ words of a song may be conveyed by the harmony ; for any  
 “ judicious singer, by dividing properly the words and repeat-  
 “ ing them, as is usual in singing songs, may sing those in due  
 “ time, with the air which conveys them ; and though I con-  
 “ fess I see much harm might arise from it, yet it may be right  
 “ to observe, hy-the-by, that a harmonic letter thus written,  
 “ could not easily be brought *home* with any degree of cer-  
 “ tainty (especially where null notes are employed) so as to  
 “ convict the writer in a court of justice ; yet I cannot think  
 “ myself guilty of an injury to society in pointing this method  
 “ out, as it may be productive of much good, as well as of mis-

“chief; for secret writing is absolutely necessary on many important occasions of state.

“It therefore might be right for foreign ambassadors or princesses, who are separated from their families by foreign alliances, to be in possession of some kind of musical alphabet by which they may write or receive letters which are not suspected to be so. The present mode, I believe, is to do all this business by what is obviously writing in cipher; and that, too, by some method which has long been in use, the key to which I have more than reason to believe, most of the princes in Europe are in possession of. I will hardly believe that the K—— of ——, for instance, is a stranger to every mode of cryptographical writing by the several princes and states in Europe. How often do we hear of a courier being murdered and his despatches carried off? and for what other purpose but information? and without the key to decipher letters so written, to what purpose should they be intercepted by such a deed? I have considered every method of secret writing which I have heard of, either of ancient or modern practice, and I submit it to the reader’s consideration, whether writing by an harmonic alphabet is not, of all others, the most void of suspicion. Perhaps I should say *was not*, because, having published it, the secret is divulged.”

The reader is now in possession of all the arguments by which Mr. Thicknesse endeavors to recommend the practice of musical writing; and we doubt not that this author has done his best in composing the specimens alluded to; but we will venture to predict that no good judge of musical composition would mistake his pieces for the productions of a *master*. We have added in *Plate II., fig. 5*, another specimen, by a different hand, copied from the *Encyclopædia Britannica*, which, however, contains only the treble, and is as unsupportably poor and unharmonious as *fig. 3*. We allow that *fig. 4*, having both the bass and the treble, looks more like music after the altera-

tions we have made; but if it were perfectly corrected in the mechanical part, it still would be called bad harmony, and a puerile composition by any real judge of music. This latter piece might very possibly pass without suspicion; and then it signifies nothing what faults it contains, only let it not be held up for imitation, while the tails of some notes are turned the wrong way, the treble and bass ill adjusted to each other, and the several component parts of the specimen do not (or at least, did not before we amended it) accord truly in time.

If the difficulty in conducting a correspondence in this way be so great, and the labor of composing it so considerable, we should rather give the preference to Lord Bacon's idea of a bifurmed alphabet, which is not more liable to suspicion than the musical cipher, and is much less intricate as well as better adapted for the use of persons unskilled in harmonics.

The mere circumstance of exposure to *suspicion* may easily be shunned by interlining or writing across any common epistle with diluted acids; as, for instance, with one part of oil of vitriol, mixed in ten parts of water, which will be rendered visible only when the paper is held to a fire. Authors mention the same peculiarity in a saturated solution of *sal ammoniac* and the juice of onions; or we may write with a strong decoction of galls, which will not be apparent until the paper has been washed over with a solution of copperas. (See the article, *INX*, "Rees' Cyclopædia.") Another method of preventing suspicion, insisted on by Schottus and others, is this:

Take two pieces of pasteboard or stiff paper, through which cut long squares at different distances, as you will see in the following example. One of these pieces you keep yourself, and the other you give to your correspondent. When you would send him any secret intelligence, you lay the pasteboard upon a paper of the same size; and in the spaces cut out you write only what you would have understood by him, and then fill up the

intermediate spaces with something that makes a different sense with those words :

I shall be much obliged to you, as reading alone engages my attention at present, if you will lend me any one of the eight volumes of the Spectator. I hope you will excuse this freedom ; but for a winter's evening, I don't know a better entertainment. If I fail to return it soon, never trust me for the time to come.

A paper of this sort may be placed four different ways, either by putting the bottom at the top, or by turning it over ; and by these means, the superfluous words may be the more easily adapted to the sense of the others.

This is an eligible cipher so far as it is free from suspicion ; but it will do only for short messages ; for if the spaces be frequent, it will be very difficult to make the concealed and obvious meanings agree together ; and if the sense be not clear the writing will be liable to suspicion.

It would be an endless task, which we by no means attempt, to lay before our readers all or even half the various methods proposed for secret writing. By far the greater number of them, especially the more ancient ones, are insecure ; and however their respective inventors may have held them up to public notice, the art of deciphering has of late been so ably cultivated, that very few indeed are entitled to full confidence in a time of extremity. Mr. J. Falconer, who has shown uncommon industry and acumen in this way, believed, " that the " most sure cipher practicable in current converse may make " a discovery ;" and " if you once understand the rules for de-

“ciphering in one language” (says he), “you may really and “without reservation, in a few hours, understand as much of “any other language as is needful to reduce it to a cipher.” With like confidence, the learned Conrad, author of “*Cryptographia Denudata*,” thinks this branch of the art is so completely *infallible* that the “explication of any secret writing may “be securely undertaken for a large wager.” We will endeavor to condense the best rules given for this purpose, not only by both the above authors, but by other persons skilled in deciphering; to which we shall add, occasionally, some practical remarks of our own.

A writer in the Gentleman’s Magazine (June, 1761), although he acknowledges himself “not versed in secret alphabets,” but who “happened to hit upon one,” which gave him an high opinion of his own abilities, was so presumptuous as to affirm “it might be demonstrated, that there never hath “been invented, and that it is impossible to invent another “cipher which shall not be inferior to his by very many degrees.” This overweening conceit is not at all uncommon in such cases. Persons who have never studiously applied to this subject, are apt to fancy the art of writing by cipher is easily acquired, and that what they “happened to hit upon,” perhaps without mature deliberation, is incapable of a disclosure: whereas they who have most seriously weighed all the subtleties of this art, confess that it is a very difficult matter to write by any alphabet, admitting of a current use, without hazarding a discovery of the secret.

The two earliest systematic authors, whose cryptographic labors have descended to posterity, viz., Trithemius and J. Baptiste Porta, appear to have entertained very high notions of their respective discoveries; but before the end of the sixteenth century it was found that no method then invented could escape detection, when submitted to the examination of Vieta. (See Dict. Moreri, art. VIETA.) The modes of writing

employed more than forty years afterward, from A. D. 1642 to 1652, when our countryman, Wallis, flourished, were also deemed inscrutable by their respective advocates, until this able mathematician proved the contrary. And although some general rules may be laid down for the assistance of decipherers, it is to be observed, "that every new cipher, being contrived in a new way, does not admit any constant method of finding it out; but (says Dr. Wallis), he that will do any thing in deciphering, must first furnish himself with patience and sagacity, and make the best conjectures he can, till he happen upon something that he may conclude with for truth." (See Davy's "Essay on Deciphering," &c., 4to, 1737.) Many writers have handled this science with great learning and ability; but, for an enumeration of them, we refer to Breithaupt's "Ars Decifratoria," 1737; wherein will be seen a regular history of its progress, especially as it relates to deciphering on the continent.

Dr. Wallis properly remarks that "all persons are not qualified or capable of acquiring the art of deciphering, and that a certain degree of acumen is requisite for this purpose; indeed, those who are equal to the task, are not always willing to give the labor and time necessary to accomplish their design." (Letter to Leibnitz, January 16, 1698-9.) We are therefore not to wonder that so few persons attain to a moderate degree of excellence, or even endeavor to cultivate this art in any age. It is not only requisite that a student should meet with a quantity of writing suitable to the difficulty of the cipher he examines, "without which," says Dr. Wallis, "he may easily fail of success;" but he must obtain all the collateral information possible, relative to the language in which the cipher may probably be written—the period in which it was composed—the device mostly used in that period, the quarter from whence it comes—the place whither it was intended, and such other external circumstances as

will lead to a discovery of the business in agitation ; for a decipherer needs all the incidental aids within his reach : he must learn to fortify himself previous to the engagement, “*et consilium in arenâ capere.*”

We have mentioned the Lacedæmonian scytale as one of the most ancient ways of secret correspondence (but not invented by Archimedes, as Trithemius and others suppose); and, therefore, it may be proper first to show the means of frustrating the design of that contrivance. Mr. Falconer, after Scaliger, proposes to join the edges of the paper together by a serpentine revolution, so as to unite both portions of the divided letter, which will give the circumference of the scytale to frame a staff by ; or you may add piece to piece, says he, after the first letter is joined until the solution has been completed. But Mr. Thicknesse wonders that Scaliger did not think of a much more ready method ; that is, by cutting the scroll quite through the middle between the half letters, and then, by applying the two broken edges of the letters together on a table, they will appear perfect so as to expose the reading.

Something like the plan of Polybius for corresponding by flambeaux, is generally practised during a war at St. Roak, a high situation near Gibraltar, to inform the Governor of Cadiz of the number of men-of-war off Gibraltar, or the number which have sailed out of the bay, &c., which might be disconcerted by exhibiting the same kind of lights at the signal house on Gibraltar-hill, at precisely the same time when the Spaniards showed theirs. Mr. Thicknesse tells us, the Spaniards, by those lights, expressed letters and figures ; nay, that he had even acquired their method in some measure, but dared not disclose it to the English Governor, “*fearing a court-martial and a cashierment ; for I do insist upon it,*” he adds, “*that a governor so ignorant or indolent as not to defeat such a kind of correspondence, would be wicked or foolish enough to punish any officer who presumed to dictate to*

“him,” as it would be called. “Yet every information of this kind may be defeated, and false alarms given to the Spaniards at Cadiz, by a governor who would take half the trouble to serve his country which he does to enrich himself and distress those under his command.” See p. 33 of “A Treatise on the Art of Deciphering,” 1772.

In examining a piece of writing performed by newly-invented characters, we should endeavor to ascertain whether the number of them corresponds, or nearly so, with the ordinary number of alphabetical letters. We may sometimes detect a weakness in the writer, of having selected the most simple marks either for the vowels or the first letters in the alphabet, and his complex marks for the consonants or the letters most remote from *a, b, c,* &c. We must observe which of the characters, whether taken singly or combined, occur the oftenest in the whole specimen; and of these, probably, the most frequent will represent *e, a, i, o;* *e* being much more common than the rest of the vowels, but *u* and *y* are even less frequent than many consonants.

Endeavor next to ascertain the beginning and ending of words, which are sometimes distinguished by spaces, or points, or nulls interposed; but however it be done, you must expect these signs to occur after every few letters, and the frequency of their occurrence may serve as some guide.

When you have found out the distinction between words, take particular notice of the order, number, frequency, and combination of the letters in each word; and first examine the characters of which the shortest monosyllables are composed. Remember, 1. That no word can be without a vowel; a word of one letter must therefore be a vowel, or a consonant with an apostrophe. 2. That the vowels are more frequently doubled at the beginning of words, than the consonants; indeed, the latter are only doubled in the beginning of Spanish and Welsh words. 3. That the vowels mostly exceed the

consonants in short words; and when the double consonants are preceded by a single letter, that letter is a vowel. 4. That the single consonant which precedes or follows double consonants, is *l*, *m*, *n*, or *r*. 5. That the letter *q* is always followed by *u*; and when two different characters occur, the latter of which is often joined with other letters, but the former never found alone, nor joined with any other than the latter, those characters stand for *qu*, which two, except in a few Scotch words, are always followed by a vowel. 6. That although every language has something peculiar in its structure, the foregoing observations will apply to all the specimens we have given of the European tongues in the several parts of this article. See especially the series of examples above, in eight different languages.

In the English, let it be remarked, that *and* and *the* are more often found than any other words; *h* is frequently preceded by *w*, *c*, *s*, and *t*; *y* is seldom used in the middle of a word; the double letters *ll* and *ss* appear frequently at the end of words; *ed*, *ty*, *ly*, *ing*, and *tion*, are very common terminations; *em*, *in*, *con*, and *com*, are frequent prepositions; *a*, *i*, and *o*, may stand alone; *o* is often followed with *u*; *e* is much more frequent in the beginning and end of words, than in the middle; and in English, the *e* is continually employed, as in *yes*, *yet*, *her*, *never*, *me*, *we*, *the*, *he*, *she*, *they*, *ye*, *fee*, *see*, *be*, *ever*, *speed*, *need*, *deference*, *excel*, *excess*, &c. Though this will not hold good in the Latin, as *e* and *i* are equally frequent in the latter, and next to these *a* and *u*; but *o* not so common as any of them; and yet in the Spanish and Italian *o* occurs very frequently. When you meet with a character doubled, in the middle of a word of four letters, it will be necessary to consider what words of four syllables are so spelled. It is probable the vowels *e* or *o* are these: as *mect*, *feel*, *good*, *book*, *look*, &c. In polysyllables, where a double character appears in the

middle of a word, it is for the most part a consonant; and if so, the preceding letter is always a vowel.

Observe also, that *i*, in English, never terminates a word, nor *a* or *u* except in *flea*, *sea*, *you*, or *thou*; again, by comparing the frequency of the letters, you will generally find *e* occur the oftenest; next *o*, then *a*, and *i*; but *u* and *y* are not so often used as some of the consonants, especially *s* and *t*. Among the vowels, *e* and *o* are often doubled; the rest scarce ever; and *e* and *y* often terminate words, but *y* is much less frequent, and consequently easily distinguished.

To find out one consonant from another, you must also observe the frequency of *d*, *h*, *u*, *r*, *s*, *t*; and next to those, *c*, *f*, *g*, *l*, *m*, *w*; in a third rank may be placed *b*, *k*, *p*, and lastly *q*, *x*, *z*. This remark, however, belongs to English; for in Latin, the common consonants are *l*, *r*, *s*, *t*; next *c*, *f*, *m*, *n*; then *d*, *g*, *h*, *p*, *q*; and lastly, *b*, *z*, *z*. But the first difficulty is to come at the knowledge of three or four letters; therefore, where a word of four letters hath the first and fourth the same, it is most likely to be *that*; to discover which, look for another of four letters, beginning with the two first, and ending with two others, and it will probably prove to be *this*; and more especially if you find another with three letters, beginning with the first two; for in that case, it must be *the*. Now, having found out in any part of the cipher these three words, *that*, *this*, and *the*, place them over the characters which you know to be *t*, *h*, *a*, *i*, *s*, *e*, and then consider what letters are deficient, and what words, from the number of letters which compose them, they are most likely to be. You will thus find such ready and surprising intimations from the above six deserters, previously apprehended, that you will soon be in possession of the whole battalion.

Where words of two letters appear of the same characters, differently placed, it is most likely one is *ou*, the other *no*; so

*of*, and *for*, and *from*, discover and convict each other; and *th* are very often used in the beginning of English words, as, *the*, *that*, *this*, *them*, *their*, *thirst*, *thwart*, &c.

Besides these peculiarities, Mr. Falconer points out the following, as applicable to the English :

|   |  |  |
|---|--|--|
| A | } Beginning a word is regularly followed by— | most of the letters.                                     |
| B |  | a, e, i, l, o, r, u, y.                                  |
| C |  | a, e, h, i, l, o, r, u.                                  |
| D |  | a, e, i, o, r, u.  |
| E |  | most of the letters.                                     |
| F |  | a, e, i, l, o, r, u, and sometimes y.                    |
| G |  | a, e, h, i, l, n, o, r, u, y.                            |
| H |  | vowels only.   |
| I |  | most of the letters.                                     |
| K |  | a, e, i, n.  |
| L |  | vowels only.   |
| M |  | vowels only.   |
| N |  | vowels only.   |
| O |  | most of the letters.                                     |
| P |  | a, e, h, i, l, o, r, s, sometimes t, u, y.               |
| Q |  | only by u, and Q U by a, e, i, o.                        |
| R |  | a, e, sometimes h, i, o, u, y.                           |
| S |  | a, c, e, h, i, k, l, m, n, o, p, q, t, u, w, y.          |
| T |  | a, e, h, i, o, u, w, y.                                  |
| U |  | sometimes d, and g, l, m, n, p.<br>sometimes r; s, t, x. |
| V |  | vowels only.   |
| W |  | a, e, h, i, o, r, y.                                     |
| X | sometimes a, or e.                           |  |
| Y | e, sometimes i, o.                           |  |
| Z | e, sometimes o.                              |  |

It would be too prolix in us to give an equally minute account of the particularities in other languages; but the inquisitive reader will find them very well specified in the "Cryptographia Denudata" of D. A. Conrad, Svo, Lug. Bat., 1739, and in the latter part of Breithaupt's "Ars Deciffratoria, sive Scientia Occultia Scripturas Solvendi et Legendi." Helmst., 12mo, 1737.

To exercise the English scholar, we here subjoin one example of plain ciphering, in which two figures answer to each letter:

39. 38,31,21,35. 35,14,20,18,21,19,20,35,34. 20,38,39,  
19. 32,35,31,18,35,18. 22,39,20,38. 13,31,14,24 20,38,39,  
14,37,19. 31,19. 20,15. 20,38,35. 13,31,14,31,37,39,14,37.  
15,36. 20,38,35. 31,36,36,31,39,18. 18,35,17,21,39,19,39,  
20,35. 36,15,18. 24,15,21. 20,15. 11,14,15,22. 18,35,13,35.  
13,32,35,18. 20,38,31,20. 15,14. 14,15. 31,33,33,15,21,14,  
20. 24,15,21. 36,31,39,12. 20,15. 13,35,35,20. 13,35, 31,  
20. 14,39,14,35. 20,15,13,15,18,18,15,22,19. 14,39,37,38,  
20. 36,15,18. 22,35. 13,21,19,20. 14,15,20. 14,15,22,  
34,35,12,31,24. 20,38,35. 19,21,18,16,18,39,25,35. 15,36.  
20,38,35. 33,31,19,20,12,35. 22,38,35,14. 20,38,39,14,37,  
19. 31,18,35. 39,21,19,20. 18,39,16,35. 36,15,18. 35,23,  
35,33,21,20,39,15,14.

By practising the foregoing rules, the student will find that this method of secret writing in plain cipher may, with as much ease, if not with as much speed, be deciphered as written.

In all cases, begin first to decipher the single characters and shortest monosyllables; mark down on a separate paper any corresponding letters and signs you discover, and count the different characters throughout the piece, in order to compare

their frequency, etc. It will generally, if not always, happen that the most frequent is *e*.

We shall now consider some ways of frustrating these rules, and the methods of procedure in such cases. The first we notice, is that of writing not only without any distinction between the words, but also by altering their relative position; this was the late Earl of Argyle's method, and it was then thought absolutely undecipherable. See "An Account of the Discoveries made in Scotland of Conspiracies against his Majesty's Government." Mr. Thicknesse says he has seen many ways of explaining this cipher, but he thinks the best is to mark the concurrence of *proper* words. Take this as a specimen :

|          |             |             |            |                |            |                |               |
|----------|-------------|-------------|------------|----------------|------------|----------------|---------------|
| <i>I</i> | <i>knew</i> | <i>not</i>  | <i>the</i> | <i>grounds</i> | <i>our</i> | <i>friends</i> | have          |
| gone     | upon        | which       | hath       | occasioned     | them       | to             | offer         |
| so       | little      | money       | as         | I              | hear       | neither        | know          |
| I        | what        | assistance  | they       | do             | intend     | to             | give          |
| and      | till        | I           | know       | both           | I          | will           | neither       |
| refuse   | my          | service     | nor        | do             | so         | much           | as            |
| object   | against     | any         | thing      | is             | resolved   | till           | I             |
| first    | hear        | what        | Mr.        | Red            | or         | any            | other         |
| you      | send        | shall       | say        | only           | in         | the            | mean          |
| time     | I           | resolve     | to         | let            | you        | know           | as            |
| much     | of          | the         | grounds    | I              | go         | on             | as            |
| is       | possible    | at          | this       | distance       | and        | in             | this          |
| way      | I           | did         | truly      | in             | my         | proposition    | mention       |
| the      | very        | least       | sum        | I              | thought    | could          | do            |
| our      | business    | effectually | not        | half           | of         | what           | I             |
| would    | have        | thought     | requisite  | in             | any        | other          | junction, &c. |

When Lord Argyle had written a letter, of which the above is a part of one, he filled up the spaces with any words which occurred, and then it appeared thus :

I gone so I and refuse object first you time much is way the our world have business very I possible of *I* send hear against my till what little upon *knew not* which money assistance I service any what shall resolve *the* at did least effectually

thought requisite not sum truly this *grounds* to say Mr. thing nor know they as hath grounds occasioned I do both do is Red only let I distance in I half in our thought my and go you in or resolved so I intend he or them *our friends*, etc.

Now, as we observed above, mark but the concurrence of proper words, and especially if they be at equal distances (and so his letter is written); then the number of words between these is the column, and thus the business is done; there may indeed, be a proper coincidence by chance; but if you lay hold of such only as are equidistant they must develop the matter, where the writer goes down one column and up another. And this is a much readier and more certain method than that laid down by *Falconer*.

The Earl of Argyle was much used to write also without distinguishing words; “but,” says Mr. Falconer, “you may nevertheless distinguish between vowels and consonants, and each of these amongst themselves; nay, you may make suppositions for words; and having found two or three letters, or one word, your difficulty is over; so that the rules already laid down, will be sufficient for deciphering the remainder.”

Notwithstanding Mr. Falconer's extreme confidence, we believe it would be no easy thing to distinguish one word from another, and one letter from another, whether vowels or consonants, in a species of writing we ourselves have invented, of which some examples occur at the end of this article, and in *Plate III*.

The insertion of nulls, or non-significant letters, is another mode of confusing the cipher; and to overcome this difficulty it is requisite—

1st. That you take the number of the different characters in the epistle; and if that exceed the number of the alphabet, it is probable mutes are intermixed with the significant letters.

We have said probable, because there may be characters inserted to express relatives and syllables, &c.

2d. Observe the frequency of the several characters, and by this means you may distinguish those nulls from significant letters; for it is obvious, that if many insignificant characters be used, they shall not be frequent; at least most of them shall be but rarely inserted, which will do no great feats; if only a few in number, and consequently their places the more frequent, they are yet by supposition distinguishable from the vowels and consonants of most use in writing, especially if you consider the order and coherence among the several characters. This admits of no particular rules, nor will the judicious need any.

3d. After you have found out the real alphabet, or all the mutes, there is no new difficulty.

There is an invention of secrecy much insisted on (though none of the swiftest) by the author of the "Secret and Swift Messenger," and others, which is beyond any yet mentioned, for intricacy, wherein each particular line, word or letter, is written by a new alphabet, but the cited author himself acknowledges it too tedious for a current correspondence, which cannot be entertained this way, but at a vast expense of time and trouble to put it in, or take it out of cipher, even by the key. And secret information, in several exigencies, must be speedy, or it will be unprofitable; so that in effect it is impracticable for the end it is designed.

However, lest it should obtain too much credit if supposed undecipherable, its difficulties are considered by Mr. Falconer.

And, first, the way of writing by it is this: the confederates determine upon some word or sentence that shall lock and unlock their missives; or the key may be sent in the letter, in some word or sentence privately marked, or by compact agreed on, such as the first or last line, &c., to serve for the

key. Suppose, says Mr. Falconer, it should be "Policy's Preheminence," there must be several alphabets framed for each of its letters in the manner following:

|    |   |   |   |   |   |   |   |   |   |   |   |   |   |   |   |   |   |   |   |   |   |   |   |   |
|----|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| 1  | A | b | c | d | e | f | g | h | i | k | l | m | n | o | p | q | r | s | t | u | w | x | y | z |
| 2  | P | q | r | s | t | u | w | x | y | z | a | b | c | d | e | f | g | h | h | k | l | m | n | o |
| 3  | O | p | q | r | s | t | v | w | x | y | z | a | b | c | d | e | f | g | i | i | k | l | m | n |
| 4  | L | m | n | o | p | q | r | s | t | u | w | x | y | z | a | b | c | d | e | f | g | h | i | k |
| 5  | I | k | l | m | n | o | p | q | r | s | t | u | w | x | y | z | a | b | c | d | e | f | g | h |
| 6  | C | d | e | f | g | h | i | k | l | m | n | o | p | q | r | s | t | u | w | x | y | z | a | b |
| 7  | Y | z | a | b | c | d | e | f | g | h | i | k | l | m | n | o | p | q | r | s | t | u | w | x |
| 8  | S | t | u | w | x | y | z | a | b | c | d | e | f | g | h | i | k | l | m | n | o | p | q | r |
| 9  | P | q | r | s | t | u | w | x | y | z | a | b | c | d | e | f | g | h | i | k | l | m | n | o |
| 10 | R | s | t | u | w | x | y | z | a | b | c | d | e | f | g | h | i | k | l | m | n | o | p | q |
| 11 | E | f | g | h | i | k | l | m | n | o | p | q | r | s | t | u | w | x | y | z | a | b | c | d |
| 12 | H | i | k | l | m | n | o | p | q | r | s | t | u | w | x | y | z | a | b | c | d | e | f | g |
| 13 | E | f | g | h | i | k | l | m | n | o | p | q | r | s | t | u | w | x | y | z | a | b | c | d |
| 14 | M | n | o | p | q | r | s | t | u | w | x | y | z | a | b | c | d | e | f | g | h | i | k | l |
| 15 | I | k | l | m | n | o | p | q | r | s | t | u | w | x | y | z | a | b | c | d | e | f | g | h |
| 16 | N | o | p | q | r | s | t | u | w | x | y | z | a | b | c | d | e | f | g | h | i | k | l | m |
| 17 | E | f | g | h | i | k | l | m | n | o | p | q | r | s | t | u | w | x | y | z | a | b | c | d |
| 18 | N | o | p | q | r | s | t | u | w | x | y | z | a | b | c | d | e | f | g | h | i | k | l | m |
| 19 | C | d | e | f | g | h | i | k | l | m | n | o | p | q | r | s | t | u | w | x | y | z | a | b |
| 20 | E | f | g | h | i | k | l | m | n | o | p | q | r | s | t | u | w | x | y | z | a | b | c | d |

If they agree that the lines only shall be written by a new alphabet, the first line shall be made according to the first

alphabet A. P., the second line according to the second alphabet, viz., A. O.; the third alphabet is A. L., &c., the first line being an index successively to all the rest. And when they have gone through the table they may begin anew, or go backward again, &c.

If words are only written by one alphabet, then every new word is written by a new alphabet, and so of letters. We have hereunto subjoined an example for each, viz:

I. EXAMPLE IN THE LINE.

Ypb vdgrts id ztte ixt hdasytgh  
 idcb wofr rihm obr worf rxsh:  
 dfaawi fd, zc espi gtww cpfzwe ez  
 cqa nwnug bynn mrtg. Qiben.

SOLUTION.

I am forced to keep the soldiers  
 upon hard duty and hard diet:  
 supply us, or they will revolt to  
 the enemy speedily. Haste.

1. When there is only one alphabet used for a line, the writing might be discovered, as in plain cipher, if you make a new operation for each line. But there may be other ways to decipher any such writing: for

2. If you find out but one letter in a line, (and that may certainly be done by a few suppositions,) it will of itself give an alphabet for that whole line, as you may perceive by the counter-table which follows; for the confederate's table being framed so as the first line may be an index to all the rest of the lines which are ordered by some word or sentence that is the key, every letter of such a word or sentence must be once supposed to stand for A. Now, in the counter-table you see

all the letters in the alphabet to be once supposed A, therefore you need only to search for I in the upper line of it, and try in what line Y is opposite to it, and those two lines give you an alphabet. Or set down the letter found under the letter that expresseth its true power, and completing the last line, you have the alphabet; *e. g.*, if you supposed Y, in the example given, to express the power of I, first write down the twenty-four letters in their usual order, and under I place Y; then, going on in order, your alphabet is thus for the first line:

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

|    |   |   |   |   |   |   |   |   |   |   |   |   |   |   |   |   |   |   |   |   |   |   |   |   |
|----|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| 1  | A | b | c | d | e | f | g | h | i | k | l | m | n | o | p | q | r | s | t | u | w | x | y | z |
| 2  | B | c | d | e | f | g | h | i | k | l | m | n | o | p | q | r | s | t | u | w | x | y | z | a |
| 3  | C | d | e | f | g | h | i | k | l | m | n | o | p | q | r | s | t | u | w | x | y | z | a | b |
| 4  | D | e | f | g | h | i | k | l | m | n | o | p | q | r | s | t | u | w | x | y | z | a | b | c |
| 5  | E | f | g | h | i | k | l | m | n | o | p | q | r | s | t | u | w | x | y | z | a | b | c | d |
| 6  | F | g | h | i | k | l | m | n | o | p | q | r | s | t | u | w | x | y | z | a | b | c | d | e |
| 7  | G | h | i | k | l | m | n | o | p | q | r | s | t | u | w | x | y | z | a | b | c | d | e | f |
| 8  | H | i | k | l | m | n | o | p | q | r | s | t | u | w | x | y | z | a | b | c | d | e | f | g |
| 9  | I | k | l | m | n | o | p | q | r | s | t | u | w | x | y | z | a | b | c | d | e | f | g | h |
| 10 | K | l | m | n | o | p | q | r | s | t | u | w | x | y | z | a | b | c | d | e | f | g | h | i |
| 11 | L | m | n | o | p | q | r | s | t | u | w | x | y | z | a | b | c | d | e | f | g | h | i | k |
| 12 | M | n | o | p | q | r | s | t | u | w | x | y | z | a | b | c | d | e | f | g | h | i | k | l |
| 13 | N | o | p | q | r | s | t | u | w | x | y | z | a | b | c | d | e | f | g | h | i | k | l | m |
| 14 | O | p | q | r | s | t | u | w | x | y | z | a | b | c | d | e | f | g | h | i | k | l | m | n |
| 15 | P | q | r | s | t | u | w | x | y | z | a | b | c | d | e | f | g | h | i | k | l | m | n | o |
| 16 | Q | r | s | t | u | w | x | y | z | a | b | c | d | e | f | g | h | i | k | l | m | n | o | p |
| 17 | R | s | t | u | w | x | y | z | a | b | c | d | e | f | g | h | i | k | l | m | n | o | p | q |
| 18 | S | t | u | w | x | y | z | a | b | c | d | e | f | g | h | i | k | l | m | n | o | p | q | r |
| 19 | T | u | w | x | y | z | a | b | c | d | e | f | g | h | i | k | l | m | n | o | p | q | r | s |
| 20 | U | w | x | y | z | a | b | c | d | e | f | g | h | i | k | l | m | n | o | p | q | r | s | t |
| 21 | W | x | y | z | a | b | c | d | e | f | g | h | i | k | l | m | n | o | p | q | r | s | t | u |
| 22 | X | y | z | a | b | c | d | e | f | g | h | i | k | l | m | n | o | p | q | r | s | t | u | w |
| 23 | Y | z | a | b | c | d | e | f | g | h | i | k | l | m | n | o | p | q | r | s | t | u | w | x |
| 24 | Z | a | b | c | d | e | f | g | h | i | k | l | m | n | o | p | q | r | s | t | u | w | x | y |

This *counter-table* needs not much explanation, being but an exhibition of such alphabets as you may frame by yourself upon every new supposition.

Having found one alphabet for the first line, you have likewise by this means the first letter of the key. *E. g.*, in the fifteenth line of the table, Y standing against I, and P beginning that line (as you may perceive) P must be the first letter of the key; and if you peruse the foregoing collection of what letters can be joined in the beginning of words, you will find *a, e, h, i, l, or o, &c.*, must follow P; so that, at worst, to get another alphabet for the next line, it will cost but so much pains as to make trial of those letters by supposition; as first, what letter in the first line is against *i*, in the fifth line beginning with E (for A cannot regularly follow P in this particular method, else the letters in the second line of the writing should have their usual signification without any transposition,) and finding that E cannot be the second letter of the key, because the cipher from that supposition is in as great confusion as ever, next try what letter is opposite to *i* in the line H. Still supposing anew, until you find the second line to produce sense. And so of all the rest.

Or you may take the same measures from the letters or syllables found in the writing itself.

Or you may proceed to find the alphabet of the second, third, or any other line, as you did for the first, *viz.*, searching after the power of some letter in the second line, by the ordinary rules; and, according to the greatest probability, in that search, from the frequency of the letter, or other help, to make trial by your counter-table.

## II. EXAMPLE IN THE WORDS.

Y oa qzempo ex mgg rfc lgdwbxkl  
 kede zriv hzyc hul mewh puqf:  
 bdyytg hf, sw gorl ylnn wizspy id  
 hws pypxi bynnmrtg. Keuwg.

## SOLUTION.

When the alphabet is changed at every word, you may either make supposition from words, or from letters that fall in the end or beginning of the several words in the writing, until you have made some progress in the letters of the key, and then proceed as before.

You may likewise find out by supposition, the number of letters in the key, &c., which will much facilitate the work. Thus :

1. Having found an alphabet for the first, second, or indeed any word near the beginning of the epistle, go through all the immediate following words, until you find another that is deciphered by the same alphabet.

2. From the last found word count the like number, and you have a new word decipherable by the found alphabet ; and thus you may go on until you have once gone through the whole writing, marking the whole series with some peculiar mark ; and then,

3. Begin the epistle again at some word immediately before or after that which was first found, and count forward as before, until you come to the end of the epistle.

4. Afterward observe the same method, until you have distinguished the whole writing, giving each respective series of words some particular mark of distinction. And in the end, having found out but one letter in such a series of words, it gives an alphabet to decipher all that series by, as was observed in lines, &c., *E. g.* Y, therefore, the first word in the example, expressing the power of I, you shall find the twentieth word *id* decipherable by its alphabet, viz. : A. P., and consequently *hws*, the one and twentieth after *oa* the second word, to have one alphabet with it ; and in the same order, *pypxi* to have one alphabet with *qzcnpo* ; and *bynmrtg* and *ex* to be denoted by the same alphabet, &c.

Now, if the writing were long (as it must be to contain *Proposals*, *Emergencies*, and other circumstances), the use of the foregoing observations will be evident.

But there is an exception to these rules; for you will see in the example, that the first word, Y, and the seventh word *Lydwbakkl*, are written by the same alphabet, but not the seventh from that, viz., *puqf*, nor the seventh from *oa*, viz., *Kede*, &c., and the reason is, because the letter P is twice repeated in the words of the key. So that when you find this happen in deciphering, leave such words, and go on to the next, until you find the true number of letters that make up the key by the former rule; and then this difficulty becomes a help in the operation, &c.

### III. EXAMPLE IN THE LETTERS.

Y ox ogpvtv yw oqne yvq xdzorgpl  
 Kgsn mmaq hhwc pbo qcpw saib:  
 Xgyepl xx, df eqgw oyep, zigxyy gq  
 Yxs pwgkq hgimhotl. Mnoyhl.

#### SOLUTION.

To decipher this kind of secret writing you must begin with suppositions; and,

1. Extracting out of it the monosyllables, &c., you may suppose all the words in it of three letters successively to stand for *the*, or *and*, &c., and you may prove your several suppositions thus, viz: 1. Mark down the powers supposed. 2. Observe in what lines of your counter table the letters expressed in the cipher, are opposed to them in a perpendicular line. 3. Observe the first letters of those lines, and you will soon find whether they can be joined to make up a part of the key: *e. g.*, let *yvq* in the first line of the example be supposed *the*; *y* is opposite to *t* in line fifth, beginning with E; *h* to *v*,

line thirteen, beginning N; and *e* to *g*, line third, beginning C. So that having found *enc* in the beginning of these several lines, it is probably some part of the key.

2. You may proceed in the same manner to other monosyllables, &c., in any part of the epistle; or you may consider what letters can follow *enc*: and then *e* being most probable, look in that line of your table beginning with E for *x* the following letter in the cipher, and its opposite letter in the upper line, which is S; and afterward you may go on with probable suppositions, either from the letters found in the key or in the writing.

Perhaps these methods will not so readily give you the entire key, yet they are good helps.

You may otherwise begin your suppositions with the first letters in the writing; and, for that end, we have heretofore added, in alphabetical order, the letters which can be joined to each other to begin words.

And from all together you may in a short time find out the number of letters in the key; and here that is of as much use as in the other ways of writing by the key character, since thereby you have the several returns of each alphabet.

When the alphabet is changed for every word or letter, the frequency of the letters will not agree with that in an epistle written in plain cipher, where one character always expresses the same power; for as to this last, you shall but rarely find two or three characters of the same frequency; but by a continual altering of the alphabet you shall have a great many. *E. g.*, in the last sample you have no less than seven different letters twice repeated, viz.: *a, b, d, k, s, t, z*, three letters thrice repeated, two letters four times repeated, three letters five times repeated, three letters seven times repeated, and two letters nine times repeated.

Again, in one line of an epistle, where the alphabets are con-

tinually altered you shall have more differing characters than in two where one alphabet is only used in the whole writing. In the example you have the complete number of the alphabet; where, as in the writing, viz. :

I am forced to keep the soldiers  
upon hard duty and hard diet :  
supply us, or they will revolt to  
the enemy speedily. Haste,

there are wanting, *b, g, q, x, z.*

We have already observed, that this method of cryptography requires too much time to be put in practice : but besides, it is not only impracticable upon that score (for by the least mistake in writing it is so confounded, that the confederate with his key shall never set it in order again), but withal, it is liable to suspicion ; so that it has none of those things required in secret writing, except that there is difficulty in deciphering it ; and that not insuperable, as is made apparent.

For many of the subsequent, as well as preceding observations, we are indebted to Mr. Falconer, an author we have had frequent occasions to commend, and who particularly excelled in such intricate discussions. As that gentleman's work is very scarce, we shall render the public a service in making some part of it better known, by these copious extracts.

We next mention the mode of communicating any secret intention with ordinary letters, by the aid of a few figures ; which Schottus says, was the invention of Count Grousfeld, and seems to elude the common rules for deciphering.

1. The confederates dispose the letters of the alphabet in a line or circle, over which they place any number of figures, *e. g.*, 436, in this manner :

436

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

2. They write their secret intentions on a paper apart, and over the tops of the letters they place the number of figures agreed on. Let the words be these :

“The governor of the city is beyond corruption, so that we  
“may conclude there is nothing of bribery will serve the  
“turn.”

Which words, according to the example, will stand thus :

436 43643643 64 364 3643 64 364364 36436436343 64

The governor of the city is beyond corruption so  
3643 64 364 36436436 43643 64 3643643 64 36436436 4364  
that we may conclude there is nothing of bribery will  
36436 436 4364.

serve the turn.

3. Observe what figure stands over the first letter of the writing (viz., T), which is 4, and counting forward as many letters, write down the fourth, viz., *x* ; again, see what figure is over the second letter (viz., *h*), which figure is three ; then counting three letters from *h*, the third is *k* ; next write down the sixth letter from *e*, which is also *k* : and so they proceed, always observing the letters in the writing to be secretly communicated, and the figures above it, until they come to the end of the epistle. The example being finished, will stand thus :

xkk kqahtsr t i wnh coxa ow dkbqsg etvtasworp yr wndw  
bh ofb etqeqyfk xkkvg ow ptxkoqi ti dxmdkvlk zlqo vkvzk  
xkk xxxq.

## SOLUTION.

To decipher this kind of secret writing, you may—

1. Transcribe the cipher out of the epistle, keeping the lines and letters at such a distance from one another, that each letter may admit of a figure distinctly above it.

2. Endeavor to find the number of figures in the key which must be inquired into by several suppositions.

3. The number of figures being supposed, *e. g.*, 3, take any three figures, *e. g.*, 123, and place them above the tops of the letters in cipher in this order

123 12312312 31 231 2312 31 231231 2312312312 31  
 xkk kqahtsrt ti wnh coxa ow dkbqsg etvtasworp yr  
 2312 31 231 23123123 12312 31 2312312 31 23123123  
 wdw bh ofb etgeqyfk xkkv ow ptxkoqi ti dxmdkvlk  
 1231 23123 123 1231.  
 zlqo vkvxk xkk xxxq.

4. Observe where the same character and the same figure happen to fall together, and you will find that thus it always expresseth the same power as in the example; K, with 3 placed above it, has the power of E through the whole writing; X, with 1 upon the top of it, signifies H, &c. But,

5. The same letter, when its figure is altered, cannot express the same power: *e. g.*, Q with 1 expresses N; but Q with 2 signifies O, and Q with 3, L, &c.

6. One and the same letter, will be expressed by different characters: *e. g.*, Q with 2, R with 1, and T with 3, express severally O in the writing.

7. Two letters of the same power cannot be joined together in the same character; and, consequently, where you find any character double in a writing of this nature, it expresses different powers.

8. Having made these or the like general remarks, you may proceed to discover particular syllables or words, as in the preceding paragraphs; and having one, you will find with it the true numbers that are contained in the key, at least some of them, which will discover the rest.

It is almost superfluous to add, that in your several operations, you must count the letters backwards, since regularly

the cipher is written forward : but because the cipher may be otherwise contrived, you may try both ways, &c.

#### OF SECRET WRITING BY POINTS, LINES, &c.

The secrecy in an epistle may consist in points, lines, &c., which are distinguishable, one from another, by their place, not their figure ; all of the same situation (whatever the nature of the figure be) expressing the same character. *E. g.*, suppose the paper to be written upon be secretly divided into twenty-four equal parts, according to the breadth of a plate upon which the letters are described ; and then by application of this to the epistle, it is easy to conceive the way of writing it. This is published in the " Secret and Swift Messenger," p. 92, but contains no great nor new intricacy ; for you may extract the points, &c., that fall in the first perpendicular line in any character, and the points that are in the next perpendicular line by a different character, and those points in the third line by a third character ; and so on for all the rest, until you come to an end, or rather the side of the epistle, toward the right hand ; and then it is resolvable by the common rules.

Having now removed the most material difficulties, arising from a change in the powers of the letters, we proceed to

#### SECRET WRITING, BY ALTERING THE PLACES OF THE LETTERS WHERE THEIR POWERS REMAIN THE SAME.

Bishop Wilkins observes that the difference of characters men use in the world, is part of the general curse upon their once one tongue ; and, from a parity of reason, we may infer that the different methods of writing those characters is so too.

The Oriental languages, Hebrew, Chaldaic, Samaritan, Syriac, Arabic, Persian, Coptic, &c., are written from the right hand to the left. Only the Ethiopic and Armenian proceed

from the left to the right hand; as also do all the Occidental languages, Greek, Latin, French, Spanish, Italian, German, English, Slavonic, &c.

At first the Greeks wrote from the left to the right hand, and again from the right hand to the left, forward and backward. Hence *literas exarare* signifies *to write*, a metaphor taken from plowing the ground.

Thus the sense of an epistle in a known language might be perplexed, if the writing should be contrived after the method of writing some foreign tongue. And we have this example from the "Secret and Swift Messenger":

T i l w e l d f r e  
 h t l s s o o t e i  
 e s e u h h u u s l  
 p h n t a o t o h p  
 e t c s l t t h a p  
 s o r g l e h t n u  
 t d e n n l e i d s  
 i e a o o b s w s y  
 l c s m t a i e p d  
 e n e a b e e g e e

Here the rows are introduced instead of the lines. And if you begin at the first letter toward the left hand, and read down that row of letters, then read the next upward, and the following down again, and so to the end, you will find these words: "The pestilence doth still increase amongst us; we shall not be able to hold out the siege without fresh and speedy supplies."

This is the ordinary way of writing among the inhabitants of China and Japan. It only needs exposure, in order to be detected when it occurs.

Another remarkable kind of cryptography consists in altering the places of letters by combination. But it is desirable,

before we proceed, to show how many different ways any given number of letters may be combined, or varied in their relative position; for which purpose we subjoin a table. (See, likewise, the articles ALTERNATION and CHANGES, "Rees' Cyclopædia.")

Our calculation is, however, carried no higher than the number of changes in an alphabet consisting of thirty-six letters and figures. Schottus has computed that a thousand millions of men, in as many years, could not write down the different transpositions of only twenty-four letters, if each of them completed forty pages a day, and every page contained forty permutations; and Mr. Falconer has shown that this is vastly too low a supposition! So that those transpositions, inscribed on a scroll, would reach far beyond the planet Mercury!

How much farther, then, would a chain reach of thirty-six letters, in their immensely numerous combinations? for example, in such an alphabet as this, which is adapted for the telegraph at the Admiralty, viz.:

|   |    |   |   |   |   |
|---|----|---|---|---|---|
| 1 | a  | b | c | d | e |
| 2 | f  | g | h | i | j |
| 3 | k  | l | m | n | o |
| 4 | p. | q | r | s | t |
| 5 | u  | v | w | x | y |
| : | 6  | 7 | 8 | 9 | z |

$$1 = 1$$

$$2 = 2$$

$$3 = 6$$

$$4 = 24$$

$$5 = 120$$

- 6 = 720  
 7 = 5040  
 8 = 40320  
 9 = 362880  
 10 = 3628800  
 11 = 39916800  
 12 = 479001600  
 13 = 6227020800  
 14 = 87178291200  
 15 = 1307674368000  
 16 = 20922789888000  
 17 = 355687428096000  
 18 = 6402373705728000  
 19 = 121645100408832000  
 20 = 24322902008176640000  
 21 = 51090942171709440000  
 22 = 1124000727777607680000  
 23 = 25852016758884976640000  
 24 = 620448401733239439360000  
 25 = 15511210043330985984000000  
 26 = 403291461126605635584000000  
 27 = 10888869450418352160768000000  
 28 = 304888344611713860501504000000  
 29 = 8841761993739701954543616000000  
 30 = 265252859812191058636308480000000  
 31 = 8222838654177922817725562880000000  
 32 = 263130836933693530167218012160000000  
 33 = 8683317618811886495518194401280000000  
 34 = 295232799039604140847618609643520000000  
 35 = 10333147966386144929666651337523200000000  
 36 = 371993326789901217467999448150835200000000

Here are 42 places of figures, which may be read thus :

| Sextillions. | Quintillions. | Quadrillions. | Trillions. | Billions. | Millions. | Units. |
|--------------|---------------|---------------|------------|-----------|-----------|--------|
| 371993       | 326789        | 901217        | 467999     | 448150    | 835200    | 000000 |

*i. e.*, Three hundred and seventy-one thousand nine hundred and ninety-three sextillions.

Three hundred and twenty-six thousand seven hundred and eighty-nine quintillions.

Nine hundred and one thousand two hundred and seventeen quadrillions.

Four hundred and sixty-seven thousand nine hundred and ninety-nine trillions.

Four hundred and forty-eight thousand one hundred and fifty billions.

Eight hundred and thirty-five thousand two hundred millions.

To write secretly by the method here proposed, a certain number of letters are combined to lock and unlock the epistle.

1. The differences of writing down the positions, as which shall be first, which second, which third, &c., in order, may be varied to a vast number: *e. g.*, three letters, A, B, C, having six regular ways of combination, these six positions are capable of 720 several orders, for the rows may be combined among themselves, the same way as letters. Therefore,

2. The order of the rows is agreed upon at the parting.

3. The number of letters combined, which is the key, may be expressed in the epistle by some mathematical figure, as  $\Delta$  for three letters,  $\square$  for four, &c., or by some other private mark.

4. They form a rectangular table of as many columns as there are letters combined.

5. The letters so combined are placed in their natural order upon the top of the table.

6. Having determined of how many lines the table shall consist, the order of the combination agreed upon is set down in a row, in the first column toward the left hand, as you may see in the subjoined table.

7. The table being thus prepared for writing, they observe the order of their combinations, and write according to its direction.

8. When they have placed one letter in every column of all the lines, they begin again, and so go on until the writing is finished.

9. Lastly, they take the letters out of the table according to their partitions, as so many barbarous words, upon a paper apart, and send it to the confidant.

#### EXAMPLE.

Let the key for the number of letters combined be a triangle; and the subject of the writing,

“We are big with expectation to know the success you have had, whether the arms you have undertaken for will be ready upon occasion. Let your next be writ by the square key.”

#### FORM OF THE TABLE FOR WRITING.

| ORDER<br>OF POSITIONS. |       | A                | B                 | C                 |
|------------------------|-------|------------------|-------------------|-------------------|
| 1                      | C B A | <i>atsaskdct</i> | <i>ccchmaaliy</i> | <i>wchertenre</i> |
| 2                      | C A B | <i>etcwonuyy</i> | <i>bichufpot</i>  | <i>raudycytb</i>  |
| 3                      | A C B | <i>iocchoouh</i> | <i>wtshvwons</i>  | <i>gnstarnre</i>  |
| 4                      | B C A | <i>hnutnlata</i> | <i>ioycciccq</i>  | <i>tkorulcxu</i>  |
| 5                      | B A C | <i>xwaccicc</i>  | <i>cohhdbbsbr</i> | <i>ptvarrowk</i>  |

#### A FURTHER EXPLANATION OF THIS TABLE.

C B A, being the first position, *w*, the first letter in the writing is placed under C, in the last column; and *e* being the second letter is put under B, in the next column; and *a* the third letter, under A.

C A B, being the second position, the fourth letter in the

writing, *r*, falls in the second line under C; the fifth letter, *e*, under A; and the sixth, *b*, under B in its column, all in the same line.

A C B, being the third position, the seventh letter in the epistle, *i*, is put under A, in the third line; the eighth letter, *g*, under C; and the ninth letter, *w*, in column B.

And so they go through the writing, always beginning again when they are at the end of the table, so long as there is anything to write.

The writing, taken out of the table, will stand thus :

△ *Atsaskdet. cechmaaliy. wehertenre.*  
*ētewonuiyy. bičhufspot. raudycytlb. iocehoouh.*  
*wiſhwvons gñstarnre. hñutnlata ioyceicq.*  
*tkorulexu. xiwaccicc. eohhdsbr. ptvarrowk.*

The terminal letters may be so marked to prevent confusion.

We have insisted the more upon this method, because the manner of combining, and the way of writing by such combinations, being once perfectly understood, the rules for deciphering may be the more succinct, and the more easily comprehended.

#### SOLUTION.

I. If the figure of the key be prefixed to the epistle, expressing the number of letters combined, take as many letters out of the first places of seeming words in the epistle, as shall be equal to that number so expressed, and you may soon find out their true order without the trouble of a new combination; though the trouble of combining is not so very great, as the discovery of a treasonable design may be of importance to the public.

Thus in the example given, you have △ (which must be

supposed to show that three letters are combined); extract the first three letters from the first three seeming words of the epistle, viz., *a, e, w*; here at first view you may perceive the order. Then taking out the next three letters, *e, b, r*, you have *a* for the first letter of the word from the first line, and *e* for the last letter; and then you are only to consider whether *b* or *r* is the middle letter, which is easily determined; so *b* (being left out there) must be the first letter of the next word: thus you may proceed, for it is needless to enlarge in a case so plain.

2. If there be no key given, take the number of partitions of seeming words in the epistle, and find out their several divisors; which may be performed by the following rules:

#### HOW TO FIND OUT THE EQUAL DIVISORS OF ANY NUMBER.

1. Divide the number given by some prime number, *i. e.*, such a number that cannot be divided but by itself, or unity, and the quotient by some other prime number, and so go on until the last quotient of all but one; and thus you shall find a certain number of prime divisors.

2. Make a rectangular table that shall consist of as many columns as you have prime divisors, which you must place one after another at the tops of the columns; and by the help of them you will find all the rest of the divisors, viz:

By multiplying the first prime divisor, toward the left hand of the table, by the second, and writing the product under the second. Next by the third prime divisor, multiplying all the figures in the table toward the left hand, setting the several products in the third column; and so forth, throughout all the prime divisors, but with this caution: that one product be not written twice; and in the end, the several numbers in your table will be all the aliquot parts, or just divisors of the given number.

EXAMPLE TO FIND OUT ALL THE DIVISORS IN 450.

|     |     |    |    |   |   |
|-----|-----|----|----|---|---|
| 450 | 225 | 75 | 25 | 5 | 1 |
| 2   | 3   | 3  | 5  | 5 |   |

The first line contains the first dividend, and the respective quotients; the lowest line is the several prime divisors.

Now, 450, the number given, being divided by 2, a prime divisor, the quotient is 225; which, being divided by 3, you have 75 for a new quotient; and that again divided by 3, you have 25 for another quotient. This last, divided by 5, gives 5; which, being a prime number, you have 1, or unity in the last quotient of all; so that your prime divisors are, 2, 3, 3, 5, 5; all which set down in the tops of the columns, and multiplying them according to the rule given, the operation will stand thus:

|   |   |    |    |     |
|---|---|----|----|-----|
| 2 | 3 | 3  | 5  | 5   |
|   | 6 | 9  | 10 | 25  |
|   |   | 18 | 15 | 50  |
|   |   |    | 30 | 75  |
|   |   |    | 45 | 150 |
|   |   |    | 90 | 225 |
|   |   |    |    | 450 |

All the divisors of 450 are 2, 3, 5, 6, 9, 10, 15, 18, 25, 30, 45, 50, 75, 90, 150, 225; and one of them (supposing the epistle to have consisted of 450 seeming words) should have

been the number of letters combined for the key; for the number of seeming words in such an epistle is equal to the rectangle made of the figure of the key, or number of lines; and consequently the figure of the key, or number of letters combined, is some aliquot part, or equal divisor of the number of seeming words.

But to save all trouble in search of the key, you may take a certain number of letters out of the first places of the seeming words and write them down in a line; next, take just as many letters out of the second places of the same partitions, and then the letters out of the third, fourth, and fifth places, &c., placing them directly one under another, in order; or rather for dispatch, take out the seeming words, and write them down in rows, beginning at the first, and then proceed to the second, third, fourth, fifth, &c., until you have gone through them; and if the number be too great, take as many as you think fit at a time, placing all the dots you find above the heads of the letters at their sides, *e. g.* :

|     | 1' | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 | 11 | 12 | 13 | 14 | 15 |   |   |   |
|-----|----|---|---|---|---|---|---|---|---|----|----|----|----|----|----|---|---|---|
| 1.  | A  | e | w | e | b | r | i | w | g | .  | h  | i  | t  | x  | e  | p |   |   |
| 2.  | t  | c | e | t | i | a | o | t | n | n  | .  | o  | k  | w  | .  | t |   |   |
| 3.  | s  | e | h | c | c | u | e | s | . | s  | u  | y  | o  | a  | h  | v |   |   |
| 4.  | a  | h | e | w | h | d | e | h | t | t  | e  | r  | .  | e  | h  | a |   |   |
| 5.  | s  | m | r | o | u | . | y | h | v | a  | n  | e  | .  | u  | e  | d | r |   |
| 6.  | k  | a | t | n | f | e | o | w | r | .  | l  | i  | l  | e  | h  | r |   |   |
| 7.  | d  | a | e | w | p | y | . | o | o | n  | .  | a  | c  | c  | i  | s | o |   |
| 8.  | e  | l | u | . | y | o | t | . | u | n  | .  | r  | t  | e  | x  | e | b | w |
| 9.  | t  | i | r | y | . | t | b | h | s | .  | e  | a  | q  | u  | e  | r | k |   |
| 10. | —  | y | e | — | — | — | — | — | — | —  | —  | —  | —  | —  | —  | — |   |   |

We have marked the lines and rows with figures for their more easy distinction.

Having brought the writing into this order,

1. Search in the several lines for some of the particles of

that language you may suppose the *épistle* to have been written in ; if in English, make suppositions, *e.g.*, for such little words as *the, that, for, of, to, and. &c.*, and the like, without some of which no man can well express business of any moment.

2. Having searched in any of the lines for some one of those mentioned, or the like particles, you may prove the truth of your supposition by taking out the opposite letters of all the other lines ; and if they do not make up words or syllables, or produce such letters as can probably follow one another in that order, your first supposition is false, and you must guess again.

3. Having by fresh suppositions found some usual word, and the letters of the other lines in the same order agreeing, the words or syllables arising from them will direct you to some new row that goes before or after in their true order ; and thus you may proceed till you have found out the whole writing, which by this time will be no great difficulty.

## EXAMPLE.

In the sixth line you have *f* once, and *r* twice ; so that probably amongst these letters you may find the word *for* ; and upon trial, the supposition is proved by the other lines : *e. g.*, line 6 by lines 1, 2, 3, 4, 5, 6, 7, 8, 9.

| Rows | 5          | 7        | 9          |
|------|------------|----------|------------|
| 6.   | <i>f</i>   | <i>o</i> | <i>r</i> . |
| 1.   | <i>b</i>   | <i>i</i> | <i>g</i> . |
| 2.   | <i>i</i>   | <i>o</i> | <i>u</i> . |
| 3.   | <i>c</i>   | <i>e</i> | <i>s</i>   |
| 4.   | <i>h</i>   | <i>e</i> | <i>t</i>   |
| 5.   | <i>u</i> . | <i>h</i> | <i>a</i>   |
| 7.   | <i>p</i>   | <i>o</i> | <i>n</i> . |
| 8.   | <i>o</i>   | <i>u</i> | <i>r</i> . |
| 9.   | <i>t</i>   | <i>h</i> | <i>e</i> . |

Here in the fifth line you find *u* a terminating letter; which must then have before it the vowel *o*, as in *you*, or *e*, as in *lieu*. And in this line you have *o*, once, and *e* twice; so that in three suppositions at most, you shall have the preceding row in its natural order; thus supposing it *o*, in the fourth row that joins the vowel *u*, the writing will stand thus:

| Rows | 4  | 5  | 7 | 9  |
|------|----|----|---|----|
| 1.   | e. | b  | i | g. |
| 2.   | t  | i  | o | n. |
| 3.   | c  | c  | e | s  |
| 4.   | w  | h  | e | t  |
| 5.   | o  | u. | h | a  |
| 6.   | n. | f  | o | r  |
| 7.   | u  | p  | o | n. |
| 8.   | y  | o  | u | r. |
| 9.   | y  | t  | h | e. |

Now having *ou*, it is most probable that *y* is wanting to join with it; which standing in the sixth row of the line, write down that row in order thus:

|    | 6  | 4  | 5  | 7 | 9  |
|----|----|----|----|---|----|
| 1. | r  | e. | b  | i | g  |
| 2. | a  | t. | i  | o | n. |
| 3. | u  | c  | c  | e | s  |
| 4. | d. | w  | h  | e | t  |
| 5. | y  | o  | u. | h | a  |
| 6. | e  | n. | f  | o | r  |
| 7. | y. | u  | p  | o | n  |
| 8. | t. | y  | o  | u | r  |
| 9. | b  | y. | t  | h | e  |

And so you may go on until you get through the whole writing; which will in the end stand thus:

W e . a r e . b i g . w i t h . e x p  
 e c t a t i o n . t o . k n o w . t  
 h e . s u c c e s s . y o u . h a v  
 e . h a d . W h e t h e r . t h e . A  
 r m s . y o u . h a v e . u n d e r  
 t a k e n . f o r . w i l l . b e . r  
 e a d y . u p o n . o c c a s i o  
 n . L e t . y o u r . n e x t . b e . W  
 r i t . b y . t h e . s q u a r e . K  
 e y .

There are sometimes other helps obvious, to discover the sense of an epistle obscured by this invention; *e. g.*, you see only two letters falling in the last line of the example; whereby I not only conclude that the epistle ends with them, but may also infer from the supposition of a regular procedure in writing it, that the letter began at some of the seeming words that composed those two rows, *viz.*, *eעהמאליג*, or *weherteure*. The reason is evident, &c.

This method of secret writing is, at first sight, distinguishable from any other, only by observing the equality in the division of its letters.

There are great varieties of inventions of this kind, more easy to the confederates; whereby they only write their secret intentions in a parallelogram, or other mathematical figure, and confound the sense by the method of extracting it. (See the "Account of Discoveries made in Scotland," p. 18, &c.)

OF SECRET WRITING BY MEANS OF A PARALLELOGRAM  
 WHERE THE LETTERS ARE EXTRACTED OUT OF THAT FIGURE  
 DIAGONALLY.

To perform this, a man needs only form a parallelogram or table, and without any combination or other obscurity in the

writing, insert his secret intentions therein ; *e. g.*, let the sense of the epistle be,

“ I suppose that things are so forward by your diligence  
“ that we may venture at all, once a week ; meet me towards  
“ ten to-morrow’s night at the old place.”

It is first inserted in the table thus :

|    |    |    |    |    |    |    |    |    |   |    |          |          |          |          |           |
|----|----|----|----|----|----|----|----|----|---|----|----------|----------|----------|----------|-----------|
| I. | s  | u  | p  | p  | o  | s  | e. | t  | h | a  | t.       | t        | h        | i        | n         |
| g  | s. | a  | r  | e. | s  | o. | f  | o  | r | w  | a        | r        | d.       | b        | y.        |
| y  | o  | u  | r. | d  | i  | l  | i  | g  | e | n  | c        | e.       | t        | h        | a         |
| t. | w  | e. | m  | a  | y. | a  | d  | v  | e | n  | t        | u        | r        | e.       | a         |
| t. | a  | l  | l. | o  | n  | c  | e. | n  | e | x  | t.       | w        | e        | e        | k.        |
| m  | e  | e  | t. | m  | e. | t  | o  | w  | a | r  | d        | s.       | t        | e        | n.        |
| t  | o- | m  | o  | r  | r  | o  | w  | s. | n | i  | g        | h        | t.       | a        | t         |
| t  | h  | e. | o  | l  | d. | p  | l  | a  | c | e. | <i>b</i> | <i>x</i> | <i>y</i> | <i>f</i> | <i>q.</i> |

Here the last five letters, *b, x, y, f, q*, are of no use but to fill up the void places in the table.

The first method of obscuring the meaning of such an epistle is by copying it out of the table diagonally, upon a paper apart ; *i. e.*, by supposed lines extending from the second letter in the first row toward the left hand, to the second of those in the uppermost line, and from the third letter in that row to the third in the upper line ; next, from the letters of the last line to those in the upper line that remain, and then to the last row toward the right hand, &c. *Diagonal* is a mathematical term, from *διὰ*, and *γωνία*, an *angle* or *corner*.

#### EXAMPLE.

They first write down *I*, beginning at the upper corner of the parallelogram ; next they take the other two letters which lie in order to it, viz. : *g, s* ; then they extract the next three in order, viz., *y, s, u*. And so they go on until they come to the last corner, viz., *q*. The whole writing being extracted in this manner, will stand thus :

I. g s y s. u t. o a p t. w u r p m a e. r. e. o t e l m d s s t  
 o- e l. a i o. e. h m t. o y. l f t e. o m n a i o h o r e. c d g r a  
 l r t e. v e w t. d. o o n e n a t p w w e n c r h l s. e x t e. d  
 i a n r t. u t b n c i d w r h y. e. g s. e e. a b h t e a x t. e k.  
 y a u f t. q.

For the solution of this and such like manner of secret writing, the only difficulty is to find out the number of the lines, and the number of rows. And here you may observe, that the number of letters in the epistle is equal to the rectangle made of the number of lines and rows; so that if you take the divisors or aliquot parts of the number of letters, you may find out the number of lines and rows by a few suppositions, and, consequently, the involved meaning.

Nay, you may soon discover any writing of this nature, by reducing the letters of the epistle into diagonal lines, as if you had found out its true figure; *e. g.* :

First, you mark down *I*, the first letter in the writing, by itself, as in the margin. Next write the two following letters, *g*, *s*, by it, thus : then to these, join the three following letters *y*, *s*, *u*, thus : afterwards the following four letters, *t*, *o*, *a*, *p*, thus : and so of the following five letters, &c. You will perceive when words or syllables appear ; and withal if you observe the cohesion of words or letters, between the end of the first line and the beginning of the second, you will find out where these two lines join in the sense, and, consequently, where the first line ends : thus you shall have the number of rows, by which if you divide the whole letters, the quotient gives you the number of lines, &c.

This way of deciphering may seem to be eluded two ways :

1. By beginning (when they copy the epistle out of the table) at some of the other angles.



2. Having written down their secret intentions on a paper apart, they contrive an epistle of some ordinary business in any language.

3. They search for the numbers of the alphabet that express the letters of the secret writing; and counting the letters in the common missive from the beginning, they subjoin some private mark under every character where the respective numbers end; *e. g.*, let the secret intimation be this:

|          |          |          |          |          |           |          |           |          |          |          |          |          |          |          |
|----------|----------|----------|----------|----------|-----------|----------|-----------|----------|----------|----------|----------|----------|----------|----------|
| 3        | 6        | 18       | 4        | 12       | 12        | 6        | 11        | 16       | 2        | 15       | 5        | 18       | 3        | 6        |
| <i>I</i> | <i>s</i> | <i>h</i> | <i>a</i> | <i>l</i> | <i>l</i>  | <i>s</i> | <i>ee</i> | <i>y</i> | <i>o</i> | <i>u</i> | <i>t</i> | <i>h</i> | <i>i</i> | <i>s</i> |
| 20       | 3        | 13       | 18       | 5        | 45        | 16       | 2         | 15       | 7        | 12       | 2        | 9        | 13       |          |
| <i>n</i> | <i>i</i> | <i>g</i> | <i>h</i> | <i>t</i> | <i>at</i> | <i>y</i> | <i>o</i>  | <i>u</i> | <i>r</i> | <i>l</i> | <i>o</i> | <i>d</i> | <i>g</i> |          |
| 3        | 20       | 13       | 6        |          |           |          |           |          |          |          |          |          |          |          |
| <i>i</i> | <i>n</i> | <i>g</i> | <i>s</i> |          |           |          |           |          |          |          |          |          |          |          |

And the epistle may run thus:

“ Having understood that I could not be safe any longer  
 “ where you are, I have chosen rather a voluntary banishment  
 “ to wander with my liberty abroad, than to lie under the  
 “ daily hazard of losing it at home : ’Tis in my opinion the  
 “ least of the two evils. ’Tis true I am innocent ; but inno-  
 “ cence is not always a buckler ; so that I hope you will not  
 “ condemn, even though you cannot approve my choice, at least  
 “ till you have the particulars of my case ; which expect *per*  
 “ next.”

You see the figure for the first letter, to be put in cipher, is 3 ; therefore a secret mark or point must be placed directly under, or above, the third letter of the epistle, viz., *v* ; and number 6, expressing the second letter in secret writing, a dot must stand under the sixth letter from *v*, viz., under *d* ; and eighteen letters from *d*, will stand another dot, &c.

## EXAMPLE.

Having understood that I could not be safe any longer where you are, I have chosen rather a voluntary banishment, to wander with my liberty abroad, than to lie under the daily hazard of losing it at home: 'Tis in my opinion the least of the two evils. 'Tis true I am innocent; but innocence is not always a buckler; so that I hope you will not condemn, even though you cannot approve my choice, at least till you have the particulars of my case; which expect *per* next.

These points may be written with such ink that they shall not be visible till held by the fire, or dipped in water.

## SOLUTION.

For deciphering this, you have no more to do but take the number of letters, from the beginning of the epistle to the first point, from that to the second, and so from point to point until you come to the last; writing down the several numbers, distinctly one after another, and then you have it in a plain cipher resolvable by the former rules.

Nich. Machiavel tells us that in his own time, a certain person designing to signify some secret intention to his friends, interlined private marks in letters of excommunication that were to be publicly affixed, by which the secret was afterward communicated to the confederates; and this has in all probability been performed by the former, or such like method of secret information.

We have already considered the obscurity arising from the insertion of nulls at random, as to several of the ways of secret writing mentioned: but here we shall inquire into them as inserted by compact, either to prevent or divert suspicion; and

indeed the great design of persons who use them, is generally one of these two.

When they would quite remove suspicion, the epistle is so contrived, as to outward appearance, that it may appear to have nothing in it but some trivial business, as news, &c., or a private concern, as borrowing of money, paying of bills, &c.

But if the person to whom the epistle is written might render the paper suspected, they endeavor to divert that suspicion by inserting a false design to cloak a true one.

The nature of this secrecy will more fully appear in the subsequent examples :

Suppose two or more confederates had agreed to confine their secret intentions to one side of the paper in the writing, according to some private compact. Thus, upon discovery of a plot, if a speedy flight were designed, and to be communicated by this contrivance, it might be written at first in the following manner :

This measure is not  
secret ; there is now no  
safety but by flight,  
Do not fail to meet me  
half an hour hence.  
Let the next meeting be  
just without the gate  
(if my senses are sound)  
we may conclude to have  
clear infallible evidence  
the snare is prepared,  
effectually to entrap  
you and

Your, &c.

POSTSCRIPT.

Pray  
expose not yourself to  
imminent danger.

Now, to obscure the sense, and prevent suspicion, the unfinished parts of the lines may be supplied with something foreign to the design; and afterward the epistle is to be pointed according to the seeming sense; *e. g.*:

This measure is not  
secret; there is now no  
safety but by flight  
Do not fail to meet me  
half an hour hence  
Let the next meeting be  
just without the gate  
(if my senses are sound)  
we may conclude to have  
clear infallible evidence  
the snare is prepared,  
effectually to entrap  
you and

in danger; to all it is as yet  
thing in view to threaten our  
should ruin all our designs.  
by six in the usual manner:  
I intend to be at the council.  
where they will, I'll have notice:  
was the governor this morning  
secure as we could wish him;  
hit right in the means, and more  
is not on this side conjuration:  
they are misted, and see not 'tis  
them, and on their ruin to raise

Your, &c.

#### POSTSCRIPT.

Pray  
expose not yourself to  
imminent danger.

throw off those vain fears:  
scorn when there is not any

Here, to divert suspicion of what is designed for the confederates, the secret intelligence is divided from the rest of the epistle, by a supposed perpendicular line; but however it be divided, the sense cannot well escape a discerning eye; and to propose a solution would be superfluous.

We have already detailed Lord Bacon's mode of secret writing, and need not much enlarge on the means of deciphering it; for if you once find out whether two or three alphabets be used (and the different kinds of letters in the epistle will inform you of that), you may suppose one alphabet  $\alpha$ , a second to stand

for *b*, and if there be a third, let it be supposed *c*. Afterward extract the writing out of the epistle, as if these letters *a*, *b*, or *c*, only, were inserted; and then it falls under the former considerations.

It is nothing to the purpose, whether your supposition and the writer's be the same, or not; for if you suppose always an *a* for his *b*, the operation will be alike easy.

This way of secret correspondence will therefore signify very little, unless to spend the time and paper of the writer; for if you put a mark of distinction between every two, three, or five of the characters (as they make up a significant letter), they are liable to discovery, the same as an ordinary cipher.

And it is easily discernible when two, three, or five characters express one letter, either from the number of characters in a word, or in the whole writing:

1. From the number in the word; for when two letters go to the composition of the alphabet, they must have five places; and the words will consist of five, ten, fifteen, twenty, or twenty-five letters, &c. If three letters are in three places, you will find three, six, nine, fifteen, or eighteen characters, &c., in each word; if five letters in two places, the words shall have two, four, six, eight, ten, or twelve characters, &c., apiece.

2. From the number of letters in the whole; as if two be only used, in one rank, you shall have five differing characters in the whole at least: *e. g.*, *a, b, c, d, e*. If three in a rank, then you may have three characters: *e. g.*, *a, b, c*; and if five in rank, you will possibly have but two characters in the writing, &c.

By these remarks it will be seen, that Lord Bacon's plan of writing *omnia per omnia*, as he calls this we allude to, is not deemed undecipherable, although it possesses the merit of ingenuity; and indeed all alphabets composed after that manner, in which each letter is represented by one uniform sign (whe-

ther composed of few or many characters does not matter) will be liable to exposure; because if you once find out the substitute of any single letter, you discover it in all other instances where that same letter is represented. Thus suppose *aabaa* to signify *E*, this letter will be always found by detecting its substitute *aabaa*, and of course the recurrence of every other letter may be easily known; so that you are not embarrassed by this cipher with any extraordinary difficulty, as some inexperienced men have imagined.

And here we shall leave this kind of cryptography by *mere letters*, &c.

The reader who duly attends to the foregoing directions, will be able to extend his knowledge to a variety of other methods, in which *fewer letters* or characters are used than are commonly required in forming words; but of this kind the most difficult of all, which indeed we fear it is impossible to decipher, is the mode that consists in representing whole words, or even sentences, by single notes and figures. For by this method, we confess, there seems to be no ground whereon a decipherer can set his foot, no principle by which he may be guided in his operations; but all must be conjecture, and discouraging uncertainty! On many accounts, however, the alphabetical modes of writing are preferable for ordinary use; as the labor of putting an epistle into cipher and taking it out by any other process, is insufferably tedious and operose.

One of the ingenious conceptions of a lady who intended to puzzle Mr. Thicknesse with a new cipher, was this:—she composed an epistle in English by means of Etruscan characters, and rendered the whole according to French orthography, after the following manner:

“ Sur, as yeux air il, doux comme & change the climat :  
 “ here, yeux mai have game, fiche, duc, fat mutin, foule, porc,  
 “ aile, port, fruit, & admirable meuchette an butter; an mi  
 “ sistre (a joli nymphe) tu chat tu yeux, & sing yeux an ode,

“ to the lute, or violin : yeux canne have a stéble for ure hors,  
 “ & a place for ure chaise. Mi son met a physician neér the  
 “ river, tissé fetal signe ! thé sai the pour Docteur dos grive  
 “ about the affaire, oing tù the rude Squire : but pardon mi  
 “ long lettre, pré doux comme tu us about mai, if yeux canne :  
 “ mi service tu ure niece : houé dos Raffé doux  
 “ Adieu mi friend,

“ \* \* \* \* \*

“ *P. S.*

“ Pré doux comme ; for ure pour Nenni seize but feu  
 “ beaux.”

This feminine production would create no difficulty to a decipherer who understands French, but might perhaps help a little to perplex any other person on his first entering upon the task. We add a device of our own, with which some other lady may possibly amuse herself. The means of deciphering it will be obvious, we suppose, from what has been said in the preceding pages :

Take a sufficient number of ornamental beads of five colors (though fewer will do), and string them upon a thread in pairs according to the plan of combining two signs for one letter. Suppose them to be red, green, yellow, black, and white ; an alphabet may then be formed many thousand ways, of which the following is one : Let A be red and green ; B, red and yellow ; C, red and black ; D, red and white ; E, green and red ; F, green and yellow ; G, green and black ; H, green and white ; and so on with all the other letters. Now, when a message has been composed after this manner, upon a long thread, it may serve for an ornament to some person's neck ; or it might pass in a basket of peddler's toys, without the slightest suspicion of its insidious contents. If only three colors were used, three beads must unite in representing each letter.

Among the incredible pretensions of men who have studied the art of cryptography in former times, we find this one of

Trithemius, who certainly mistook his own talents in several particulars: “Possum hominem idiotam, scientem tantum  
 “linguam maternam, qui nunquam novit verbum Latini ser-  
 “monis, in duabus horis docere scribere, legere, et intelligere  
 “Latinum satis ornate et disertè quantumcunque voluerit; ita  
 “ut quicumque viderit ejus literas, laudent verba, intelligant  
 “Latinè composita.”

The idea here held out, of teaching an ignorant person to write, read, and *understand* elegant Latin in two hours, although he never before knew one word of it, is most absurd, and repugnant to all our experience of human ability! none but the Almighty himself could thus instantaneously confer the power of *understanding* a foreign language, although, without doubt, a man who can write, may be taught to copy any Latin words in less than two hours. And Trithemius seems to have attempted nothing more.

To explain this, suppose a great multitude of common alphabets written in order; and to each of the letters in those alphabets synonymous Latin words are annexed, as denoting the respective letters. If all the words expressing A, in the different alphabets, make up an oration, and all the words in each rank be of like signification; and if A, in writing by this method, begins the first alphabet; let one word be taken from thence, another from the second, and another from the third alphabet, as they are required, until the intention of the writer shall be fulfilled; it is easy to perceive how a man unacquainted with Latin shall thus write it “satis ornate et  
 “disertè”; but he would nevertheless remain totally ignorant of the meaning of those Latin words, any otherwise than as they expressed the various letters for which they were substituted, and whereby he has composed some secret message conceived in his mother tongue. We here remark:

1. That there must be a new alphabet constructed for every letter in the secret writing.

2. These alphabets require more than an ordinary degree of ingenuity in their contrivance.

3. When the alphabets are exactly framed, the least mistake in the writer turns the secret intimation into a chaos.

4. But suppose there were nothing amiss in the whole design (which is enough, in all conscience, to grant), yet there is much more time required in writing and reading by this artifice, than a man in business can dispense with : for (as we have said), according to Trithemius, the key must contain as many alphabets as the secret epistle has letters in it. Now, in Argyle's long letter, inserted in the "Discoveries made in Scotland," there are upward of a thousand words ; and if he had taken Trithemius's way of concealing it, there would have been five or six thousand alphabets used in the key ; we leave it to arithmetic to resolve how much time a particular search of those alphabets will amount to ; and to stoicism (for none but men of that sect will try) how much patience.

Athanasius Kircher, in his "Steganography," endeavors to improve Trithemius's method. The alterations we observe are these :

1. Kircher contrives his key in the form of any ordinary epistle ; whereas, Trithemius conceives his in forms of prayer, which are more liable to suspicion, especially in an age when the greatest villanies are committed under a mere form of godliness.

2. Kircher has alphabets of several languages, whereby a man may choose what speech he pleases for his exterior letter, though he understand not the genuine meaning of one word. But this was proposed by Trithemius.

3. Kircher's key consists not of many words ; so that if the secret or interior epistle be not conceived in a few, it gives ground of suspicion and of resolution, too.

For the words that express every particular alphabet, as before, being of like signification (that the outward writing

may seem to have a seeming sense), at every few lines you shall have the same sense, though not in the same words; which gives ground to suspect it, and if the writing be long, to attempt a solution.

Again, suppose that several letters, written by the same key, were seized (which is no great improbability), the sense of all will be to the same purpose, and that gives cause enough of jealousy, and facilitates the discovery.

The compiler has now laid before his readers a concise history of the origin and progress of cryptography, and has pointed out some of the best means hitherto suggested for deciphering; but he has not aimed at giving many new ciphers; nor has he endeavored to show in how many ways a skilful writer might prevent the discovery of even an intention to deceive. He is confident, however, that ciphers may be constructed of a much superior kind to any he has met with; more ready in execution, more simple in their principle, more intricate to disclose, and (in some examples) not liable to suspicion.

It only remains, at present, to explain the nature of *Plate III.*, and the lower part of *Plate II.*

The musical writing, on *Plate II.*, *fig. 5*, containing the words, "Let me know you are safe," &c., was composed and published by an author of no ability in music, and the specimen is here added, only to show how puerile any common endeavor of that kind must appear to a judge of harmony; so that this proposal, which has been much vaunted and recommended by Mr. Thicknesse, is never likely to prove of extensive practical utility.

*Fig. 6*, *Plate II.*, represents one of the various modes of cryptography invented by the writer of this article. In its present form, it is not difficult to decipher, but is more simple and regular in its structure than any of the Irish Oghams; and, by an artifice exemplified in the next plate, which consists of dots instead of strokes, it may be rendered absolutely inscrutable.

*Plate III.* exhibits a perfectly new plan of secret writing, where there are only three dots, (over the line, upon it, and under it,) representing eighty-one letters or figures conformably to the alphabet engraved upon the same plate. This method is capable of a surprising variety, but in every variety shall seem to be the same writing; it is also practiced by letters and figures, or words, or by all mingled together, without any apparent difference in its form. The reader will never discover anything here besides a simple dot in three positions, and cannot tell whether one, two, three, or more of them compose each character. The inventor presumes to think that this contrivance is deserving the attention of ingenious men, and might be a very advantageous acquisition in the Foreign Secretary of State's Office; but it would be incompatible with his feelings to submit any such proposal to the judgment of inferior clerks, who, perhaps, know nothing beyond the mechanical use of ciphers, and are totally unqualified to appreciate the merits of a scientific invention. At present he has, therefore, not chosen to divulge the principle of this cipher to any person living.

The following paragraph gives the explanation of the dot-writing on *Plate III.*, with the interpretation of the two succeeding examples; and also, in Italic letters, it expresses the author's name, profession, place of residence, and the date of the year: these four different specimens are all deciphered by ONE KEY, which is engraved at the top of *Plate III.*, and it would have been easy to have given several hundred more varieties, to be likewise deciphered by the same key.

The art of writing in cipher has been studied by men of the greatest talents and rank in every civilized country; but among the various ciphers which have been

*made public, we have never seen any that are exempt from considerable objections. Some of them are too laborious for diplomatic uses or dispatch of business, others are not sufficiently faithful to elude a discovery when examined with scrupulous attention, and others are of such a nature as to be inadmissible for practice, except under very peculiar circumstances; besides which the generality of ciphers are complex and difficult to write in proportion to their intricacy.*

1526180354666 93599507192735855362 10283693121732  
 724592064539401118394705666 7685736342011 439314394  
 70659507737799321929 697778856580665 35445361513932  
 9478504635364193557407 96163924393 7589619816289196  
 340128376746646439311251 5053225947210666463061534  
 64959686701255322618 929407172737526 93373561630111  
 839470223534399324251 116177507163 0646961450473961  
 96849394796382053824306637 2958035467993 9681881424  
 150528465220756547484942454 66911161802711 31181215  
 1727364809499224 5065440152639140 354645058 59380163  
 511275728596894 0959992034 28246265 1435584 975076564  
 567065570429894 32351512260595201125569847 18139408  
 3232618571303546450748 31505668954 4551217183615164  
 304435285837446 8160666509 65476858803 5938598941227  
 6163844393717263 74934 5819714173639349371 737726939  
 475848724251 6277656 938677664547584959369353364293  
 9977726384 94935346459333 5293948775729335036291525  
 57399386940779 9931118017 36353414494867 89115463939  
 599920324653121517757904 58112182458936847 34454606  
 16346439332391225 16173546075 73841287224 8587874759  
 69493000111848494 245569371 729875 64006672639321183  
 63946355 4557743 9383950075892426184 656933546450007  
 5651432544581938674 8508589954 45512251615 937799071  
 57495845939882 03246652465847728383693585993152618  
 174693987477572812357543.



written so as not to be deciphered without any clue but a close application to the letter itself; and that, too, though it were written in a language the decipherer does not understand." This author has only re-echoed the words of Mr. Falconer, and seems to believe he had even arrived at the ne plus ultra of his art; but to shew that the writer of this article entertains a very different opinion, and that he challenges all the scrutinizing powers of man, these few specimens are here adduced. The two former, as has been already stated, contain the same internal sense as the dot-writing, and are explained by the same key. Although the key and explanation may serve to develop the principle on which this cipher is constructed, the writer has nevertheless hazarded making a discovery by adding this one example more; wherein the involved sentiment is expressed by points, and which is also decipherable by the same key as the other specimens.

The present mode of corresponding, as well as the preceding, may be conducted with a triformed alphabet, without any suspicion of a cipher being employed. The words represented by the points, in this example, may be found in the paragraph itself; so that the student will not have to look far for an interpretation of its contents. If, after such an unprecedented challenge, and

so many helps toward an explanation, the reader still cannot develop this cipher, he ought to concede that the "craft of man" is inadequate to the task of deciphering it "without any clue."

Before the student attempts to decipher the above specimens, or the dot-writing on *Plate III.*, it may be proper to inform him that the alphabet by which these paragraphs were composed is wholly unlike any other. The alphabet consists of letters arranged in eighty-one places, forming a square of nine letters which are most wanted in ordinary writing, are there repeated most frequently; so that it is possible to produce an immense variety in the appearance of the specimens, while that great variety shall make no real difference in their sense or internal meaning. In consequence of such a construction of this alphabet, all the rules for deciphering with which the author is acquainted are easily and effectually frustrated. The ingenious reader must, therefore, hit upon some new mode of analyzing and explaining what is written in the paragraphs alluded to.

A similar method of corresponding admits of such an arrangement of the letters as to seem like a foreign language; this mode has not any peculiar advantage in practice, but is somewhat remarkable in the appearance of the writing. As for example: *Relieve us speedily, or we perish; for the enemy has been reinforced, and our provisions are nearly expended*, is thus written:

Sika jygam a fuva quaxo Rolofak adunabi ye, Rase quema Lovazig-arodi; Moxati Ho hyka Fagiva myne qui paxo Aukava in Oufa yani moxarico, Pangdo Spulzi jorixa mugaro ya zangor Alsiva yival ponbine Kazeb re linthvath.

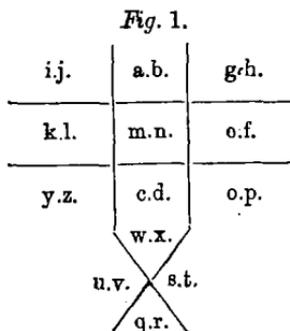
---

From the few specimens that have been made public during the past fifty years, it is evident that the art of writing in cipher has been as extensively and skilfully used as during any previous period; but owing to the natural jealousy with which such secrets are guarded, it has been difficult to get possession of many varieties of sufficient importance to merit notice.

The following examples have been collected from different sources as worthy of attention and preservation.

Figure 1 illustrates the form of cipher used by Aaron Burr in his celebrated conspiracy, and possesses more historical interest than real merit, being difficult to use and easily deciphered. The shape of the characters clearly indicates the form

of key, while their value, remaining unchanged throughout a whole message, renders them subject to the ordinary rules



for deciphering. The letters are indicated by the lines enclosing them—blank for the first letter of each couplet, and dotted for the second letter. Thus

□ □ represent "A" and "M," while [.] [ ] represent "B" and "N."

Figure 2 gives the form used by Bonaparte, and is better than the one described above, but is far from being safe.

To use it, a key-word is chosen, the first letter of which being found in the column of capital letters, the first letter of the word to be enciphered is found in the same horizontal line to the right, and the letter immediately beneath it will be the cipher letter.

Figure 2.

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

The following is a proclamation from Bonaparte to the French army, enciphered from the above table, the key being "La France et ma famille." A copy of this proclamation is said to have been in the hands of one or more persons in every regiment of the army :

## PROCLAMATION.

“Ney ip twhkl mope n clz iuwi cetttkl me p r t q z k  
 p a c h w h r d p k d a b k f u t z i m e p u n g g w y m g  
 f t g q e f d e s r o n w x q f k z x b c h q n f m y s n q a n g  
 o p o l f a p m m f a m p a b j a r w c c q z n a u r u v z  
 s k q d k n h H i h y d g h b a i l x d f q k n g t x y o g  
 w r l n l w t o y P b c i z o p b g a i r f g k p z a w r w  
 l q i p d g a e r k f f m w z f e r g p e c h.”

From the frequency with which the letter “w” occurs in this example, one would not suspect that it was a French cipher, and thus would be thrown off the scent at the outset.

The principle on which this cipher is formed is similar to that described on page 76 of the Manual, but is easier to decipher, because to render it practically useful it was necessary to arrange the alphabet in a form that could be memorized readily and rapidly. The rules given for the example referred to will apply in this case.

---

Figure 3 is an ingenious modification of Mr. Blair's challenge cipher, suggested by Second Lieutenant A. W. Greely, Acting Signal Officer, United States Army, and is arranged so as to give several word terminals and to be easily memorized. It is described by Lieutenant Greely, as follows:

“To use this cipher, the rows of letters are numbered from top to bottom—from ‘1’ to ‘9’ inclusive. The letters in each row are numbered from left to right in the same manner.

“To designate any letter, the number of the row in which it is situated, followed by the number of its place in the row, expresses it.

“To further complicate it, these numbers may be expressed by the letters of the alphabet. Either of the

first three letters in any row will stand for the number of that row, as 'D,' 'X,' or 'M' is 6, 'F,' 'V,' or 'O' is 3.

"The key can be easily committed to memory from its peculiar formation. The first column of squares contains the entire alphabet and a period, and is written in regular order up the first, up the third, and down the second column of letters.

"'Declum' is the remainder of the first row, 'Saide' of the second, 'Ishea' of the third, 'Thine' of the fourth, 'Faset' of the fifth, 'Erona' of the sixth, 'Trona' of the seventh, 'Trone' of the eighth, and 'Hitos' of the ninth.

"A word-pause follows 'Saide,' precedes 'Ishea,' and alternately follows and precedes the other words. Two short parallel lines stand for word-pauses and a period for end of sentence."

Figure 3.

|   |   |   |   |   |   |   |   |   |
|---|---|---|---|---|---|---|---|---|
| I | S | R | D | E | C | L | U | M |
| H | T | Q | S | a | i | d | e | = |
| G | U | P | = | I | s | h | e | a |
| F | V | O | T | h | i | n | e | = |
| E | W | N | = | F | a | s | e | t |
| D | X | M | E | r | o | n | a | = |
| C | Y | L | = | T | r | o | n | a |
| B | Z | K | T | r | o | n | e | = |
| A | . | J | = | H | i | t | o | s |

Telegraphers find an alphabetic cipher worthless for their use, owing to the rapidity with which letters are sent over the wires, and the consequent impossibility of

getting every letter. They, therefore, use a form of Route Cipher, based upon arbitrary words which are decipherable by means of printed keys, issued to cipher operators only.

Figure 4 illustrates the manner of sending the route, and indicating the number of columns employed during the late war by telegraphers.

Figure 4.

|   |    |    |    |    |    |    |    |    |   |    |   |  |    |
|---|----|----|----|----|----|----|----|----|---|----|---|--|----|
| 4 |    | 5  |    | 8  |    | 1  |    | 12 | 2 |    | 6 |  | 11 |
|   | 19 |    | 15 |    | 16 |    | 18 |    | 5 |    |   |  | 21 |
|   |    | 32 |    | 19 |    | 20 |    | 23 |   | 24 |   |  |    |
|   | 9  |    | 3  |    | 10 |    | 7  |    |   | 13 |   |  | 14 |

|            |    |           |
|------------|----|-----------|
| Able.      | 14 | Jail.     |
| Academy.   | 13 | Jaundice. |
| Adage.     | 12 | Jaw.      |
| Adverb.    | 11 | Jealous.  |
| Agony.     | 10 | Jericho.  |
| Ague.      | 9  | Job.      |
| Alabaster. | 8  | Joke.     |
| Alacrity.  | 7  | Josephus. |
| Alcove.    | 6  | Joshua    |
| Alike.     | 5  | Joy.      |
| Almanac.   | 4  | Journey.  |
| Almond.    | 3  | Jubilee.  |
| Anchovy.   | 2  | Jump.     |
| Anecdote.  | 1  | Justice.  |

The figures in the upper and lower horizontal lines are significant, while those in the two central lines are "blinds." Figures at the top of a column indicate that the column is to be read downwards, while figures at

the bottom show that the column is to be read upwards. The column of numbers below the route shows the number of columns in the message, and is indicated by either of the words placed opposite. If the message is a long one, and requires a large number of columns, the figures are doubled by sending *both* words.

In addition to this, the time, day of the month, month, and year are also expressed by other arbitrary words, as well as the names of all prominent persons and places, and words of common occurrence in dispatches. Thus, copying from the book before me, "10 o'clock A. M., January 31, 1865," is thus expressed: "Clotilda Todd Abbott Thomas." It is evident that in this case all rules for deciphering are valueless, and that the cipher is a safe one as long as the key is unknown.

In the earliest days of telegraphy, the necessity of some form of cipher was obvious, and Professor Vail gives a number of rules for enciphering words alphabetically, illustrating them with examples, of which one is given below. This kind of cipher was unavailable for reasons previously stated, and was soon discarded for the route cipher already described. The professor's rules are as follows:

- 1st. Let the last letter of a word remain unchanged.
- 2d. Let the *first* letter remain unchanged.
- 3d. Let the first and last letters remain unchanged.
- 4th. Let the middle letter of a word of five, seven, nine, or eleven letters remain unchanged.
- 5th. In *even*-numbered words, let the two middle letters remain unchanged.
- 6th. Let the middle letter of odd-numbered words commence the word transposed.
- 7th. Let the two middle letters commence in even-numbered words.

8th. In a word of even number of letters, let the first half be substituted for the last half.

9th. Let each alternate word be reversed.

10th, 11th, and 12th. Let every third, fourth, or fifth word be reversed.

13th. Let the three middle letters of every word having an odd number of letters be reversed.

14th. Let every word of two or three letters be affixed or prefixed to the word immediately preceding or following.

15th. Omit *one* of double letters.

16th. When several words of two or three letters follow each other, let them be joined together.

17th. Make no separation between words of less than eight letters.

18th. Make no separation at all between words.

19th. Reverse the order of the letters in the whole message.

20th. Change the key alternately every ten or fifteen words, using two keys.

21st. Let the two first letters of all words of four letters be affixed to the preceding word and the remaining letters prefixed to the word following.

22d. Change the key irregularly, e. g.: The first three words transpose from one key, the next three from another key, and so on indefinitely.

23d. Reverse the termination of those words ending with "tion," "sion," "ness," "less," "tive," "ty," "ly," "ed," &c.

24th. Make a division of long words into two words.

25th. Let those words which occur frequently and have only two or three letters remain unchanged.

26th. Let every 2d, 3d, or 4th word be reversed.

27th. Omit *one* vowel in every word.

28th. Omit the letter "E" at the beginning and end of words.

29th and 30th. Omit the letters "i," "o," and "y" at the beginning and end of words.

31st. In words of even number of letters, let the *first* of the two middle letters commence the word and the *last* one end it.

These rules are rendered practically useless by the fact that they are based upon the simple transposition of the alphabet, and, consequently, decipherable by the usual rules.

The change of key suggested makes the operation more difficult by the increased complication, but does not give sufficient security to compensate for the labor of enciphering.

The following is one of Professor Vail's examples in the application of the above rules:

"Z bpup yslup nbguxpyu z by i loomy & ynx gxp z legot lovappai luby rz lv j i hozoop s y z plup cbyn b z boloxbgm *the* jjpgviz l nlep. ibgm izgua z Invlvleu *the* inypoup lhlov xmlvyloi mgua *the* pupwzvyn wmgrlhz b gzh mgibpili pv *the* itj cbpu *the* gypagolpui *and the* izlveyi byxbwj wlma yu & puzyla *and* iovs gnyux ily-mule wlci, giowkpuzl *the* boegu cymicy bzip z bgn z blox bz zb yuzpurp *and* iowzmp Zlal equ'i wyayux hmy-pi gmlux *the* cyop. Lmazyep yinlufopopa, ay iz gunpyil pvbvleu *and* ulxg rpewmy klyni *the* zloyarlup Hgep ibgmwp by icblip ipgvubyux eya byixy & pu Zlegn *the* blvipi *of the* ion, speule ulhgwmpi iyunp elop eluav-loihgv bpj lbpi *the* myxbzuyux zlbyi vgsya ngv; pg epi bgmwp byi; *and* cbpuy n hzoop agji sbymlllsbj bpvelu-vepuz ibym gy zp zlzbi p eblwlmapi z mgci luth eigep zgwm p z cyzblv hogulmyn'i ugep zbyup, olvip, yuwm-gryux nbgvguzpvi ibgmhmgep."

The Professor asks: "Who can decipher this?" A question which can be satisfactorily answered by any person who carefully applies the following rules for deciphering ordinary transposed alphabetical ciphers:

1st. Observe the letters or characters that occur most frequently, and set them down for the six vowels, including "y." Of these the most frequent will generally be "E," and the least frequent "U."

2d. The vowels most frequently united are "ea" and "ou."

3d. The consonant most frequent at the end of words is "s," and the next frequent are "r" and "t."

4th. When two similar characters come together, they are most likely to be "f," "l," "s," or the vowels "e" or "o."

5th. The letter that precedes or follows two similar characters is either a vowel, or "l," "m," "n," or "r."

6th. Begin with the words of a single letter, which will be "I," "A," "O," or "&."

7th. Then take words of two letters, *one* of which will be a vowel. The most frequent are an, to, be, by, of, or, on, no, so, as, at, if, in, is, it, he, me, my, us, we, and am.

8th. In words of three letters there are usually two consonants. The most frequent are the, and, not, but, yet, for, how, why, all, you, she, his, her, our, who, may, can, did, was, are, has, had, &c.

9th. The most common words of four letters are this, that, then, thus, with, when, from, here, some, most, they, them, were, have, been, &c.

10th. The most common words of five letters are their, these, those, which, whose, where, shall, might, could, would, there, since, &c.

11th. Words of two or more syllables often begin with double consonants, or with a prefix formed of a vowel

joined with one or more consonants. The most common double consonants are, bl, br, dr, fl, fr, gr, pb, pl, pr, sh, sp, st, th, tr, wh, and wr. Of the prefixes, the ones most used are, com, con, de, dis, ex, im, in, int, mis, per, pre, pro, re, sub, sup, un.

12th. The double consonants most frequent at the end of long words are, ch, ld, lf, mn, nd, ng, rl, rn, rm, rp, rt, sm, st, xt, &c. The most common terminations are, ed, en, er, es, et, ing, ly, son, sion, tion, able, ence, ent, ment, full, less, ness, &c.

13th. The relative frequency with which the letters of the alphabet occur in a font of type is in round numbers as follows:

|   |    |   |   |   |    |        |   |
|---|----|---|---|---|----|--------|---|
| A | 10 | H | 7 | O | 9  | V      | 2 |
| B | 2  | I | 9 | P | 2  | W      | 3 |
| C | 4  | J | 1 | Q | 1  | X      | 1 |
| D | 5  | K | 1 | R | 7  | Y      | 2 |
| E | 13 | L | 5 | S | 9  | Z      | 1 |
| F | 4  | M | 4 | T | 10 | &      |   |
| G | 2  | N | 9 | U | 4  | Period | 2 |

14th. The order in which the letters of the alphabet occur as initial letters is as follows: T, A, I, W, H, O, M, S, B, F, D, C, N, P, L, G, E, R, U, J, K, Y, V, Q, X, Z. Of these, the letter "T" occurs much the oftenest, owing to common use of words beginning with "th."

A patient application of the above rules will enable any person of ordinary intelligence to decipher a common English cipher.

The following method of using a countersign number is ingenious, and produces an excellent cipher. It, however, requires some skill in framing sentences that will read sensibly and not fall under suspicion.

A number is selected, as 32145, and it is arranged by preconcert that a certain word in each sentence is to be

significant, as the 2d, for example. Then the message is written in sentences that convey no idea of the hidden meaning. To decipher it, the correspondent, being provided with the same key-number, knows that the second word of the first sentence is the third word of the message, the second word of the second sentence is the second word of the message, the second word of the third sentence is the first word of the message, and so on. The following is an example of this kind of cipher, with the above number for the countersign :

“The <sup>3</sup>*gone* days of our acquaintance induce me to write. It <sup>2</sup>*has* been a source of regret that each of us has so neglected our old time memories. General <sup>1</sup>*Bragg* has sent to this prison our mutual friend R. Jones, and by him I am reminded of you. If <sup>4</sup>*to* write revives your affection, I should be happy. In <sup>5</sup>*Richmond* there is little else to amuse us prisoners.”

This plan might be successfully used in correspondence, and would pass without exciting suspicion, even when examined as closely as were the letters of our prisoners during the late rebellion.

---

Another plan is to have the message resolvable into lines of a certain *known* number of words, and every second, third, or other line to be used, as might be determined by preconcert, the others being simply “blinds.” The message as sent is written without regard to the number of words in the lines. This is another form of the Route Cipher, and is open to several objections, the principal of which is the difficulty of

writing the message so as to avert suspicion, as, once suspected, very little skill is required to get out the meaning. The following example will illustrate the manner in which this cipher may be used:

“Do not at all prevent the meeting of or interfere with assembling the convention, it must be known it will not be even called, unsatisfactory if properly ordered by proclamation of governor who is highly esteemed.”

Here the division is made into lines of *four* words each, the alternate lines only being significant, commencing with the second. The real meaning to be conveyed is, “Prevent the meeting of the convention. It must not be even called by proclamation of governor.”

---

The following plan was adopted for the transmission of messages in cipher by the Signal Corps of the United States army during the late rebellion, and put in practice for a short period, but was abandoned for the cipher-disk used at the present time. It is well adapted for the transmission of *written* messages:

“Upon Sunday, the *seventh* letter following the one to be transmitted will be used to represent that letter; on Monday, the sixth; on Tuesday, the fifth, and so on, diminishing one for each day in the week.”

For convenience, the alphabet might be arranged in columns, so as to indicate at a glance the cipher letter and the true letter. Then, for the letter desired to be read, that in the same line in an immediately succeeding column would be used. The following different arrangement of the alphabet will illustrate the method suggested.



To use this, the paper is divided into five spaces deep, and five, six, seven, or more spaces in length, according to the number of letters to be enciphered, so that the letters composing the message shall fill all the squares thus formed, or as nearly as possible. Set the first letter in the *first* square of the first space, the second letter in the *last* square of the second space, the third letter in the first square of the third space, the fourth in the last square of the fourth space, and so on, until the squares are all filled in the first and fifth lines, when the same course is pursued for the remaining lines until the whole message is enciphered.

To further complicate this, the dividing lines might be omitted, the division being *secretly* indicated to the correspondent by a key-number or by preconcert.

A convenient arrangement of the cipher described in the "Manual," (pages 75-84,) was employed by the confederates in the trans-Mississippi department. It consisted of a pocket-book with fifteen leaves of stiff pasteboard, on each of which were two alphabets, one stationary and the other printed on linen, and moving freely, so that the relative positions of the two could be changed at will. To use it, a countersign word was selected, the letters of which indicated the position of the movable alphabets on the different leaves. The objection to this form of cipher is the arrangement of the different alphabets in their regular sequence, in consequence of which the rules laid down by Mr. Blair can be applied successfully in deciphering any message of this kind. It amounts in fact to a transposition of the alphabet, and all transpositions can be readily deciphered in the following manner.

Write the alphabet in regular order on a horizontal line, thus:

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

And then find *one* letter of the cipher, which can be easily done by a few suppositions. Having done this, find how many letters from the *true* one the cipher-letter is, and write under the *true* alphabet a new one, commencing with that letter of the alphabet that gives the transposition.

Suppose that the fifth letter is selected; we commence the new alphabet with the fifth letter of the original one, which is "E," and the letters in their usual sequence as above; then the letters in the lower line will represent the letters above them in the true alphabet. This process saves much time in counting, as is customary in this kind of cipher.

#### SYMPATHETIC INK.

Sympathetic or Invisible inks are those which leave no trace or color upon the paper; but when exposed to heat or chemical action of some kind become more or less distinctly visible.

They have been proposed and occasionally used as the means of secret correspondence, but are of little value, because their properties change after a few days' exposure to the air, and all of them leave some faint trace upon the paper when first written, unless unglazed paper is used.

However unreliable they may be in practice, a knowledge of the various kinds employed cannot fail to be of interest and, perhaps, service to the student of cipher, to whom every variety of secret writing should be familiar, and it is for his benefit that the present article has been compiled.

All sympathetic inks may be divided into different classes, according to the means necessary to be used to

make them visible, and of these methods there are four, viz :

1st. By giving a new liquor or the vapor of a new liquor a place on the same paper with the letters written with the otherwise invisible ink.

2d. By exposing the paper to the air, when the letters previously invisible will appear.

3d. By passing gently over the letters a substance of some conspicuous color reduced to powder.

4th. By exposing the paper written on to a fire. This last method is much the best, and is so generally successful that it may be safely used upon all papers suspected of containing any secret writing.

Of the first class are the following kinds :

1st. Write with a solution of sugar of lead, or of ternitrate of bismuth, and wash the paper with a solution of hydro-sulphuric acid, (sulphuretted hydrogen,) when the letters will appear *black*. This kind is only adapted for use on *colored* paper, however, as it has no effect upon white.

2d. By writing with a solution of nitrate of cobalt, and washing with a solution of oxalic acid, the letters will appear *blue*.

3d. Use a solution of sub-acetate of lead, and wash with a solution of iodide of potassium, when the letters will appear *yellow*.

4th. Write with a solution of arsenite of potash, and wash with a solution of nitrate of copper, when the letters will appear *green*.

5th. The materials of the common ferro-gallic inks may be used separately, the letters being written with the solution of sulphate of iron, and rendered visible by washing with a solution of galls. This process is fre-

quently employed to render legible the writing of old manuscripts.

6th. Common black ink may be rendered sympathetic by destroying the color with a mixture of nitric acid. It becomes visible when moistened with a solution of some volatile alkali.

7th. Lead dissolved in vegetable acid gives a colorless liquid, which becomes *black* when exposed to the vapor of arsenical liver of sulphur, even at a considerable distance. This ink is believed to have been first mentioned in 1653 by Peter Borel, who called it a "magnetic water which acted at a distance."

8th. Mix in a suitable bottle three parts of unslaked lime, with one part of yellow orpiment powder and sixteen parts of water, stop the bottle with a cork, and cover securely with a bladder, and place it over a fire, where it should remain five hours, being shaken occasionally. At the expiration of that length of time, it should be carefully decanted into another vessel. (Instead of this preparation, a saturated solution of common brimstone may be used, by boiling the brimstone either with quick-lime, or in strong alkaline ley.) Next, burn a piece of cork thoroughly, and, when well inflamed quench it in water or brandy, the latter being best. The friable coal thus produced is then ground with water, in which gum arabic has been dissolved, and a liquid as black as common ink is the result. While this is being done, dissolve a quantity of red lead with three times as much strong vinegar over a fire for three or four hours, or until the mixture has a sweet taste and is as clear as common water. A solution of lead in aquafortis answers the same purpose, but is apt to corrode or injure the paper written upon. Having prepared the liquors, if we write anything on paper with the last kind and dry

it, nothing is visible. Over this first writing write what you please with the second liquor, and it will appear as if written with common ink. When thoroughly dry, dip a small brush or sponge in the first liquor and pass it over the paper, when the black writing will disappear, and that written with the invisible ink will appear black and legible. A curious experiment with this ink may be tried as follows:

Take an ordinary-sized book, and on the first leaf write anything with the invisible liquor. Then turn to the back part of the book, and, with a rag dipped in the first liquor, moisten the part directly opposite to the writing, and leave the rag there with a piece of paper over it, then shut the book smartly, and strike it four or five blows with the hand, and then, turning it over, put it into a press or under a good weight for a few minutes, when the writing done with the invisible ink will be legible in the back part of the book. These experiments may be varied by writing the invisible characters with a solution of bismuth in nitrous acid, and exposing them to the vapors of liver of sulphur.

9th. Dissolve white or green vitriol in water, and write with the solution, when nothing will appear. Boil galls in water, and dip a linen rag into the decoction, and with it moisten the letters before written, when they will appear black and legible. Rub this over with spirit of vitriol, or its oil, and the writing will again disappear, to be again brought out by moistening with oil of tartar, but of a *yellow* tint instead of black, as at first.

10th. Golden sympathetic ink is made by dissolving in *aqua regia* as much *gold* as that menstruum will take up, and then adding to the liquor five or six times as much water. The letters are written with this, and rendered visible by washing with a solution of tin in

aqua regia, and an equal quantity of water, when they appear of a beautiful *purple*. This purple color is effaced by rubbing some simple aqua regia over the paper, and may be made to appear again by rubbing over that the solution of tin.

Of those belonging to the second class, we have the following:

1st. The golden ink is made by adding to a solution of gold in aqua regia so much water that the liquor will not stain a white paper. Letters written with this will not appear until the paper has been exposed for several hours to the open air, when they will begin to acquire a color by degrees, until they at length become of a deep *violet* color, tending to *black*. If, instead of exposing the paper to the air, it is kept closely shut up in a box, it will remain invisible two or three months; but at the end of that time it will begin to appear, and become at length of a deep violet color. So long as the gold remains united to its dissolvent it is yellow; but the acid that dissolves it being of a volatile nature, the greater part of it evaporates, and leaves no more than is just necessary to color the calyx of gold which remains upon the paper.

2d. The silver ink is made by a solution of silver in aquafortis, weakened by distilled water until it will not stain the paper. Letters written with this solution will remain invisible three or four months, if closely shut up in a box. If exposed to the heat of the sun, the evaporation of the acid is hastened, and the letters appear of a *slate* color. This is not permanent, for the sulphureous part of the aquafortis finally evaporates, and leaves the letters of a fine true silver color, if the metal used was pure and the exposure thorough.

In this class there may also be placed several other

metallic solutions: as that of lead in vinegar, and of copper in aquafortis, which give at length a color upon paper; as also the solution of tin in aqua regia, of mercury in aquafortis, of iron in vinegar, and of emory and several of the pyrites in spirit of salt. Each of these solutions gives its own particular color; but all labor under the disadvantage that in time they eat away the paper, and the letters are seen in the shape of so many holes. All of them become legible slowly from exposure to the air, and instantly if heated at a fire.

Examples of the third class:

To this class belong nearly all the expressed glutinous juices of plants which have no positive color in themselves, and the milk of animals, or any other thick and viscous fluids. To use them, the letters are written with the liquid chosen upon white paper; and when it is desired to make them visible there is thrown over them the fine powder of any colored earth, or other similar substance, and the writing becomes legible, because its viscous quality retains a portion of the fine powder. The ancients frequently used the juices of plants in their secret correspondence; and Ovid informed maidens that, when closely watched by suspicious guardians, they might communicate with their lovers in safety by writing with fresh milk, having previously arranged with the amorous swain that he would be obliged to sprinkle the apparently harmless sheet with coal dust, when the glowing words of love would become visible to his eager gaze. Encas, Pliny, and Ausonius also speak of such means being employed for the purposes of secrecy.

Inks of the fourth class:

This class is, perhaps, the most numerous of all, as all infusions answer the purpose whose ingredients are quickly burned to a sort of charcoal by the application

of a moderate heat. The best example is the sal-ammoniac ink, which is made by dissolving a scruple of sal-ammoniac in two ounces of fair water. Letters written with this solution are invisible until heat has been applied, either by holding the paper containing them before a fire or passing a heated iron over it.

The *rationale* of this is, that the inflammable part of the sal-ammoniac is burned to charcoal by a heat which is not sufficient to scorch the paper; and this is the case with the remainder of this class. Letters written with the sal-ammoniac soon become illegible, for the salt gathers moisture from the air, and the letters spread and run together in a confused manner. Dr: Lewis, who made numerous experiments with this class of inks, says all the salts which he has tried produce this effect in a greater or less degree: nitre, alum, and tartar, very slightly; sea salt, more strongly; fixed alkaline salts, still more so; but sal-ammoniac, the greatest of all. Metallic solutions made in acids, and diluted so as not to corrode the paper, act in the same manner, as also does the juice of lemon.

Letters written with a diluted solution of sulphate of copper, when gently heated, become of a beautiful *yellow* tint, which, however, disappears on cooling.

Besides the different kinds that have been described, there is another which possesses remarkable qualities, and appears to form a distinct class of its own, as far as known. The following detailed description of it will prove interesting to all who are curious in the matter:

Although in itself invisible, it becomes of a bluish green when held to the fire; and this color disappears again when the paper cools, but can be brought out by reheating, and the process may be repeated several times. The manner of preparing it may also be varied

so as to give blue, green, red, yellow, and other colors. Mr. Hellot, the inventor of the ink, got the idea of it from a German chemist, who, early in the eighteenth century, showed the Academy at Paris a salt of rose-water, which became blue on holding it to the fire, and also showed a specimen of the ore from which he procured the salt, and which proved to be bismuth. Mr. Hellot, after many experiments, found that all the salts of cobalt and one of bismuth afford a similar tincture, capable of undergoing these changes by heating.

His ink is prepared by pouring upon two ounces of arsenic ore, grossly powdered, a mixture of five ounces of aquafortis and five ounces of pure water. After the first ebullition is over, the vessel containing the ingredients is placed in a gentle *sand* heat, where it should stand until no more air bubbles seem to rise, when the fire may be increased so as to make the liquor boil for about one-quarter of an hour, when it is removed and allowed to cool.

The liquor, when cool, is of a reddish color, and should be decanted carefully into a phial, from which it is, after a short period, again decanted, and so on for several times until it is quite clear. It must not be *filtered*, because it might retain foreign matter enough to injure the paper on which it is afterwards used. There is now added to it two ounces of white sea-salt, and the whole evaporated over a gentle *sand* heat, until nothing remains except a dry saline mass, which is of a dirty green color, like that of verdigris in the cake. As it becomes dry, it must be stirred with a glass rod or pestle, to prevent it from uniting in a solid mass, and it must be removed from the fire before perfectly dry, otherwise the color will be lost from overheating, and the salt, from green, become of a dusky yellow. If taken off while

green, it cools to a beautiful rose color. To prepare the ink for use, the powder is dissolved in pure water, and then written with upon fine smooth paper, and allowed to dry. After it is once dried, the writing can be brought out by heating before a gentle fire, and will appear of a beautiful *bluish* green, but will remain visible only while the paper is warm. The colors of course disappear much sooner in winter than summer, and it is often necessary in hot weather to lay the paper on marble, or some other cold body, in order to produce the desired effect. If at any time during the experiment the paper is scorched, the color will *not* disappear again. A very interesting experiment can be made by drawing in pencil the figure of a plant or tree, and then tracing over the same lines with this liquor. When dry, the pencil-marks can be rubbed off with bread crumbs, and the paper will appear fair, although the lines made with the ink are sunk deep into it, and will appear of a beautiful bluish green when heated. The experiment may be varied by drawing a landscape, in which the earth and trees, destitute of verdure, being drawn with common ink, give a prospect of winter, but which may be made to assume the appearance of spring, by drawing the foliage and grass with the invisible ink and exposing it to heat. The effect is very pleasing, and the whole experiment worth trying.

If alum be used in the preparation instead of sea-salt, and the letters are written with the red liquor, as it is taken out of the vessel before evaporation, they will not appear even when heated, unless first washed over with a clear solution of marine salt, when they appear *blue*. Nitre added, instead of sea-salt, gives the precipitate, or dried salt, a fine *purple* color, which becomes white when water is poured on it, and from which a *rose-colored*

tincture is drawn off, and used for writing. Borax has the same effect as nitre. All the salts of cobalt give a blue color to the letters. By adding salt of nickel, they are rendered *green*.

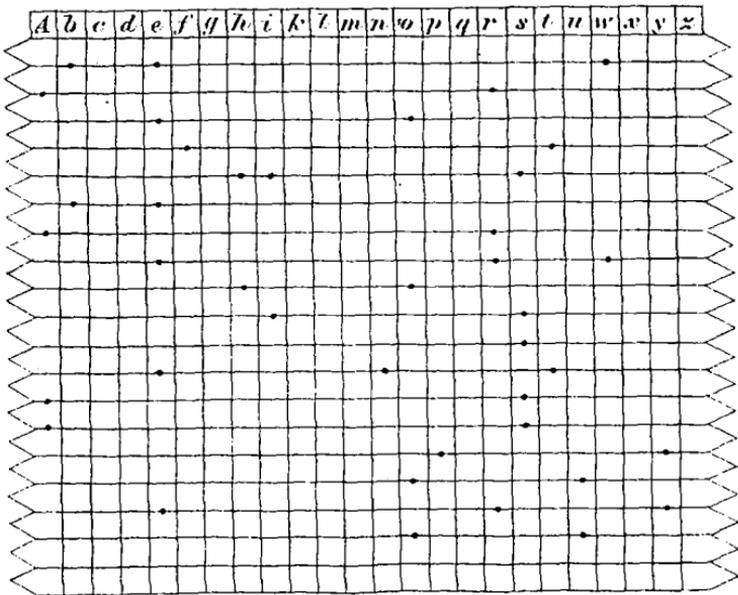
The simplest way of preparing this ink is to digest zaffre in aqua regia, thus obtaining the soluble part of it, which is the calx of cobalt, and diluting it in common water.

The chemical action of the different salts and acids used in preparing sympathetic inks destroys the enamel of common paper, and renders any writing upon it visible when held between the eye of the observer and the light. This objection is removed by using ordinary printing paper, which is unglazed, care being taken to prevent the letters from running into each other. This chemical action also renders it necessary to use quill pens, instead of steel ones, in writing with these inks

---

Bishop Wilkins, in "The Secret and Swift Messenger," gives a plan for conveying information secretly by means of knots tied upon a thread or string at certain distances, according to some preconcerted plan, which he describes as follows:

Let there be a square piece of plate, or tablet of wood, like a trencher, with the twenty-four letters described on the top of it at equal distances, and after any order that may be agreed upon beforehand; on both the opposite sides let there be divers little teeth, on which the string may be hitched or fastened for its several returns, as in the following figure:



Where the string is supposed to be fastened by a loop on the first tooth, towards the letter A, and afterwards to be drawn successively over all the rest, the marks upon it do express the secret meaning: "Beware of this bearer, who is sent as a spy over you."

When it is taken off and sent to a confederate, he may easily understand its intention by applying it to his own tablet, which must be answerable unto this. The instrument may be made much longer than is here expressed; but if the matter to be revealed should happen to be more than the tablet would bear, then may it be supplied either by another string, or else by beginning again with that part of the same string, wherein the last letter was terminated.

A board of the proper size being prepared with "saw teeth" on both sides of it, and divided as this board is marked, the first knot in the string is to be larger than the others, and is that by which the string is to be caught between the first and second teeth upon the upper left-hand side. Two knots close together may indicate that the letters, capable of being shown by the first part of the string as appended to the tablet, has been exhausted; and the string is to be readjusted by catching these two knots between the teeth at the top of the tablet, and continuing the message with the rules as before, and so for whatever length of string may be needed to convey any messages.

There is yet another way of secrecy, by more letters than are naturally required to the inward sense: if we write with a double alphabet, wherein each letter shall, in the fashion of it, bear some such small distinction from the other of the same kind, as is usual in common mixed writing. For example—

*Aa. Bb. Cc. Dd̄. Ee. Ff. gg. H h  
 Fi. Kk. Ll. Mm. Nn. Oo. Pp. Qq.  
 Rr. Ss̄. Tt̄. Vuv. Ww. Xx. Yy. Zz.*

*the second Alphabet.*

*Aa. Bb. Cc. Dd̄. Ee. Ff. Gg. Hh  
 Fi. Kk. Ll. Mm. Nn. Oo. Pp. Qq.  
 Rr. Ss̄. Tt̄. Vuv. Ww. Xx. Yy. Zz.*

1. Write an epistle of an ordinary matter, or (if it be needful) contrary to what you intend. Let the body of it consist chiefly of the first alphabet, only inserting (as you have occasion) such letters of the second as may express that inward meaning which you would reveal to a confederate.

For example, from those that are besieged—

*We prosper still in our af-  
fares. and shall (without  
having any further helpe)  
endure the siege.*

In which clause the letters of the second alphabet are only significant, expressing this inward sense.

*We perish with hunger  
helpe us*

But because the differences betwixt these two alphabets may seem more easily discoverable, since they are both generally of the same kind, the letters of the second being (all of them) more round and full than the other; therefore, for their better secrecy in this particular, it were safer to mix them both by compact, that they might not in themselves be distinguishable.

Now, if this kind of writing be mixed with the latter way of secrecy, by two letters transposed through five places, we may then write *omnia per omnia*, which (as a learned man speaks\*) is the highest degree of this ciphering.

For supposing each letter of the first alphabet to be

instead of the letter A, and those of the other for B, we may easily inscribe any secret sense in any ordinary letter, only by a quintuple proportion of the writing infolding to the writing infolded. As for example—

*All things do happen according to our desires, the particulars you shall understand when wee meete at the appointed time and place of which you must not faile by any means. The success of our affairs dos much depend vpon the meeting that wee have agreed vpon.*

The involved meaning of which clause is: *Fly, for we are discovered; I am forced to write this.*

If you suppose each letter of the first alphabet to be instead of A, and those of the second for B, then will the former clause be equivalent to this following description:

|       |       |       |       |       |       |
|-------|-------|-------|-------|-------|-------|
| F     | l     | y,    | f     | o     | r     |
| Aabab | ababa | babba | aabab | abbab | baaaa |
| babaa | aabaa | aabaa | aaaaa | baaaa | aabaa |
| w     | e     | e     | a     | r     | e     |
| aaabb | abaaa | baaab | aaaba | abbab | baabb |
| d     | i     | s     | e     | a     | v     |
| aabaa | baaaa | aabaa | aaabb | abaaa | aaaaa |
| e     | r     | e     | d;    | I     | a     |
| ababb | aabab | abbab | baaaa | aaaba | aabaa |
| m     | f     | o     | r     | e     | e     |
| aaabb | baaba | abbab | babaa | baaaa | abaaa |
| d     | t     | o     | w     | r     | i     |
| baaba | aabaa | baaba | aabbb | abaaa | baaab |
| t     | e     | t     | h     | i     | s.    |

This way of secrecy may be serviceable for such occasions as these. Suppose a man were taken captive, he may by this means discover to his friends the secrets of the enemy's camp, under the outward form of a letter persuading them to yield. Or, suppose such a man were forced by his own handwriting to betray his cause and party, though the words of it in common appearance may express what the enemy does desire, yet the involved meaning (which shall be legible only to his con-

federates) may contain anything else which he has a mind to discover to them—as in the former example.

But now if there be a three-fold alphabet, (as is easy to contrive,) then the inward writing will bear unto the outward but a triple proportion, which will be much more convenient for enlarging of the private intimations.

And this way of writing is justly to be preferred before any of the other, as containing in it more eminently all those conditions that are desirable in such kind of inventions; as—

1. It is not very laborious, either to write or read.
2. It is very difficult to be deciphered by the enemy.
3. It is void of suspicion.

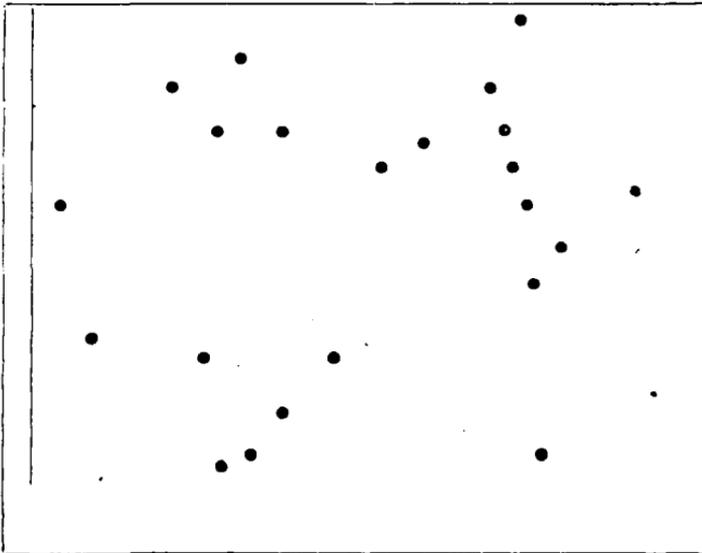
But by the way, it is to be generally observed, that the mixture of divers kinds of secret writing together (as suppose this with the key-character) will make the inward sense to be much more intricate and perplexed.

---

The great objection to the use of special signs or characters for purposes of secrecy is that they are open to suspicion. To remedy this several plans have been devised of writing by points, or lines, or figures, wherein a man would never mistrust any private message, there being nothing discerned in these forms of cipher, except some confused and casual dots and lines, or else some mathematical descriptions, as will be seen in the four following examples, each of which expresses the words:

“There is no safety but by flight.”

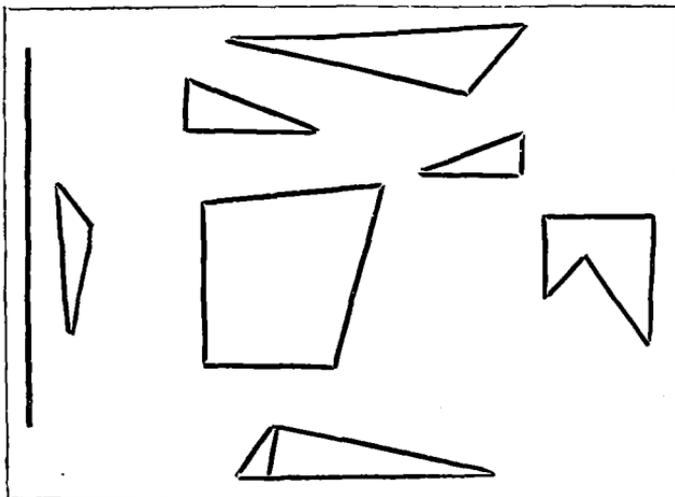
*Figure I.*  
BY POINTS ALONE.





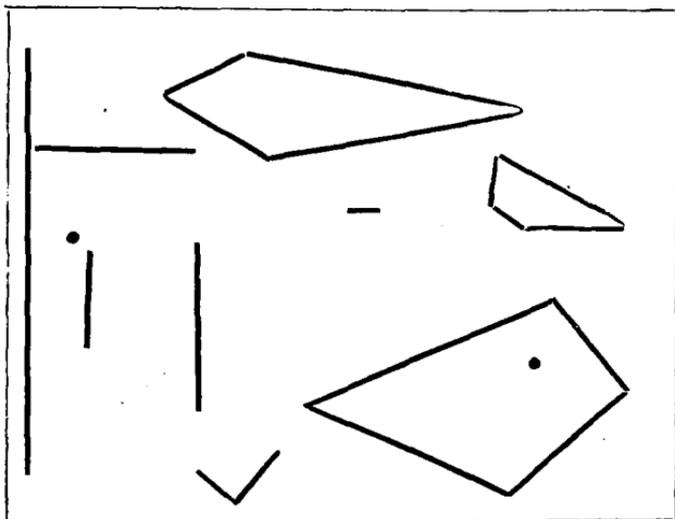
*Figure III.*

BY MATHEMATICAL FIGURES.



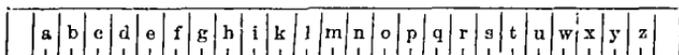
*Figure IV.*

BY POINTS, LINES, AND FIGURES MIXED TOGETHER.



The direction, both for the making and unfolding of these descriptions, is this: let the alphabet be described at equal distances upon some thin and narrow plate, pasteboard, or the like, thus:

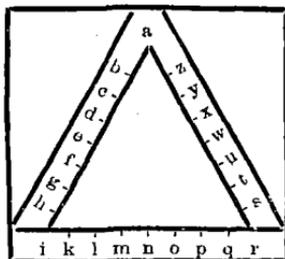
*Figure V.*



Let the sides of the paper which you are to write upon be secretly divided into equal parts, according to the breadth of the plate, and then by application of this to the epistle, it is easy to conceive how such a writing may be both composed and resolved. The points, the ends of the lines, and the angles of the figures, do each of them, by their different situations, express a several letter.

This may likewise be otherwise performed, if the alphabet be contrived in a triangular form, the middle part of it being cut out, as in figure VI.

*Figure VI.*



The larger these directories are, by so much the less liable unto error will the writing be that is described from them.

It is easy to apprehend by these particulars how a man may contrive any private saying in the form of a landscape or other picture. There may be divers the like ways whereby this invention of secrecy may be further obscured, but they are in themselves so obvious that they need not any larger explication.

---

The high official source from which the two following examples of cipher were received, entitles them to more consideration than their intrinsic merits alone would seem to authorize.

It is believed that both forms have been used for the transmission of important matter, with a full belief in their security from interpretation.

How well founded this belief was can be judged after examining their formation and applying the rules for deciphering laid down in a preceding portion of this manual.

The first form resembles in principle that kind of gibberish in which school boys delight, and termed by them "Hog Latin," differing only from that, in having a *prefix* as well as a *suffix*, as shown in the following sentence:

*"Dofinder grouten sowhater goiter lemeansor."*

Here the two initial and the two terminal letters are foreign to the sense, and used only as "blinds," a purpose they but poorly accomplish, as the merest tyro in cipher could not fail to "Find out what it means," after a few moments patient investigation.

This form of cipher might be rendered more difficult, and, consequently, safer, by making each alternate letter a blind one, and thus overcoming the fatal error of

leaving the words themselves intact. Pursuing this plan, the same sentence would read—

*"Ofriomedy olunts wehiamte isth moedabucs."*

This is still a simple form of cipher, but undoubtedly much better than in its original shape.

The second form referred to is more difficult than the preceding one, and is illustrated in the following example:

7125811. 714167312221. 6271214. 121233267. 6171742. 412561.  
 712 25 16 10 7 12 5 12 1. 7143 10 10 13 21 91. 12 72 13 12 18 17 1.  
 71 23 13 19 11 4. 16 17 1867 12962. 5 12 17 13 14 19. 71253123-  
 16 25 10 10 11. 18 18 18 67 17 16 4. 69717129. 87625 162161.  
 1491813127. 7147122121. 12 11 13 19 18 16 14. 71474612. 914-  
 23 13 19 14 7. 7621361. 9 14 23 13 19 6 14. 2412516339. 610-  
 17 11 25 16 18 14 16.

In this, as in the first one, the two initial and two terminal letters are "blinds," while the genuine letters are transposed a concerted number of places, and then represented by the figures that denote the place in the alphabet of the letter to which the transposition has been made.

Beginning with "a" as "1," and numbering to "z," "26," the nine letters, "a" to "i" inclusive, are represented by single figures, while the remaining seventeen

letters are expressed by double figures; therefore, when any one of these is used, the two figures representing it are united by a dash above them, which indicates that they are to be read together; without this dash, each figure represents a letter. In the example given, the letters have been transposed *backwards* two places; therefore, to decipher it, two must be added to each figure, representing a letter. The dots indicate word pauses, and in practice should be omitted. Taking the first word, we find that it is composed of five numeral combinations, three single and two double ones; striking out the "7" and "1" at the beginning, and the "8" and "11" at the end, we have 25 left, which gives us the letter "y," that being the twenty-fifth letter of the alphabet. Counting forward two places from this, we get "a" as the true letter and the first word. This process repeated will unravel the whole paragraph, as the student may prove by experiment.

As most of the ciphers in ordinary use consist of transpositions of the alphabet, the manner of deciphering them should be thoroughly understood. The subject has been referred to twice already in the manual, but is again repeated here to guard against any chance of mistake. If this form of cipher is suspected, it is only necessary to write down the cipher letters, and under each of them form a complete alphabet, beginning with that letter, when, if any transposition has been regularly made, the word enciphered will be found in one of the twenty-six lines thus formed. This rule is general and easy of application.

To illustrate, let us take the second word of the last cipher example and apply this rule.

We first write down the figures used, and under them

the letters that occupy corresponding places in the alphabet.

|                   |   |   |   |    |   |   |    |   |   |   |
|-------------------|---|---|---|----|---|---|----|---|---|---|
| Figures.....      | 7 | 1 | 4 | 16 | 7 | 3 | 12 | 2 | 2 | 1 |
| Letters.....      | g | a | d | p  | g | c | l  | b | b | a |
| New Alphabets.... | h | b | e | q  | h | d | m  | c | c | b |
|                   | i | c | f | r  | i | e | n  | d | d | c |

Here we find on examination the word "friend" spelled out, and as such a result could scarcely be accidental, it is fair to suppose that we have found the true solution, and that the alphabet has been transposed two letters. If it had been transposed five places, we would have found the solution in the fifth line instead of the second, and so on for any number of letters.



# WRITING BY CIPHER.

1

2

*i a e i o u s t r y r q k w b f e d m p h g z*

3

*near you under o p s w h ere one et he g ardens m i l e d  
and s t i l l w h e r e m a n y a g a r d e n f l o w e r g r o w s w i l d*

4 Lento

*a l l t h a t o f t h e c a n n o t s e e n t h e s o f t n u m b e r  
l e t m e k n o w y o u a r e s a f e d  
n d e a s e m y t o r t u r e d m i n d*

6

*i m p e r i t a . e t . i n s c i t i a . s e e r  
e t a r i o r u m . e t . a m a n u e n s i u m .  
i n . a u l i s . p r i n c i p u m . t a n t a .  
e s t . u t . m a x i m a . p l e r u n q u e . n  
e g o t i a . c i p h r i s . i n f i r m i s . e  
t . f u t i l i b u s . c o m m i t t a n t u r .*

187-182 181-180 179-178 177-176 175-174 173-172 171-170 169-168 167-166 165-164 163-162 161-160 159-158 157-156 155-154 153-152 151-150 149-148 147-146 145-144 143-142 141-140 139-138 137-136 135-134 133-132 131-130 129-128 127-126 125-124 123-122 121-120 119-118 117-116 115-114 113-112 111-110 109-108 107-106 105-104 103-102 101-100 99-98 97-96 95-94 93-92 91-90 89-88 87-86 85-84 83-82 81-80 79-78 77-76 75-74 73-72 71-70 69-68 67-66 65-64 63-62 61-60 59-58 57-56 55-54 53-52 51-50 49-48 47-46 45-44 43-42 41-40 39-38 37-36 35-34 33-32 31-30 29-28 27-26 25-24 23-22 21-20 19-18 17-16 15-14 13-12 11-10 9-8 7-6 5-4 3-2 1-0

# WRITING BY CIPHER.

Alphabet and Key.

|             |            |            |
|-------------|------------|------------|
| <i>bcs</i>  | <i>mtl</i> | <i>ico</i> |
| <i>gmt</i>  | <i>puh</i> | <i>ota</i> |
| <i>jpu</i>  | <i>dan</i> | <i>hor</i> |
| <i>kyd</i>  | <i>fer</i> | <i>nsi</i> |
| <i>ql'a</i> | <i>lis</i> | <i>rto</i> |
| <i>vle</i>  | <i>hot</i> | <i>sua</i> |
| <i>whi</i>  | <i>ncu</i> | <i>tae</i> |
| <i>xno</i>  | <i>rda</i> | <i>uei</i> |
| <i>zr.</i>  | <i>sfe</i> | <i>aio</i> |

Handwriting practice lines for cipher writing, consisting of multiple horizontal lines with small dots spaced along them.