

THE  
**CYCLOPÆDIA;**

OR,

*UNIVERSAL DICTIONARY*

OF

**ARTS, SCIENCES, AND LITERATURE.**

BY

**ABRAHAM REES, D.D. F.R.S. F.L.S. *S. Amer. Soc.***

WITH THE ASSISTANCE OF

EMINENT PROFESSIONAL GENTLEMEN.



ILLUSTRATED WITH NUMEROUS ENGRAVINGS,

*BY THE MOST DISTINGUISHED ARTISTS.*



FIRST AMERICAN EDITION,

REVISED, CORRECTED, ENLARGED, AND ADAPTED TO THIS COUNTRY,

BY SEVERAL LITERARY AND SCIENTIFIC CHARACTERS.



IN FORTY-ONE VOLUMES.

**VOL. VIII.**



***PHILADELPHIA:***

PUBLISHED BY SAMUEL F. BRADFORD,

AND

MURRAY, FAIRMAN AND CO.

PETER A. MESIER, NEW-YORK; BLAKE & CUNNINGHAM, BOSTON; CUSHING & APPLETON, SALEM;  
HEZEKIAH HOWE, NEW-HAVEN; CHARLES WHIPPLE, NEWBURYPORT; JOHN W. ADAMS, PORTS-  
MOUTH; STEPHEN PATTEN, PORTLAND; FIELDING LUCAS, BALTIMORE; DANIEL RAPINE, WASH-  
INGTON; JOSEPH MILLIGAN, GEORGETOWN; JOHN A. STEWART, ALEXANDRIA; D. HENDERSON;  
FREDERICKSBURG; WM. H. FITZWHYLLSONN, RICHMOND; RICHARD COTTOM, PETERSBURG; JOHN  
HOFF, CHARLESTON; WILLIAM T. WILLIAMS, SAVANNAH; HOBBY & BUNCE, AUGUSTA; CRAMER,  
SPEAR, & EICHBAUM, PITTSBURG; AND JAMES W. PALMER, LEXINGTON, KENTUCKY.

## CIPHER.

**CINYRA**, in the *Jewish Antiquities*, a musical instrument. This and the Hebrew *cinnor*, which is generally translated *cithara*, *lyra*, or *psalterium*, are the same. It was made of wood, and was played on in the temple of Jerusalem. Josephus says, that the cinyra of the temple had ten strings, and that it was touched with a bow. In another place he says that Solomon made a great number of them with a precious kind of metal called *electrum*, wherein he contradicts the Scripture, which informs us that Solomon's *cinnors* were of wood.

**CINYRAS**, in *Fabulous History*, the first king of the island of Cyprus; was the grandson of Pygmalion, and father of Adonis. Paphus, his father, is supposed to have been the first that introduced into the island the worship of Venus, and is said to have built the city which bears his name. He had, according to the fable, Adonis, by his own daughter Myrrha. Paphus is feigned by the poets to have been the son of Pygmalion, by a woman, who had before been an ivory statue. Pygmalion, they say, upon his arrival in the island of Cyprus, saw that the women lived very licentiously, and determined never to marry. Afterwards, as he was a famous statuary, he made an ivory statue of such perfection, that, falling in love with it, he prayed the goddess Venus to procure for him a wife as beautiful as the statue he had made. The goddess heard his prayer, and changed the statue into a fair damsel, by whom he had Paphus, the father of Cinyras. This Cinyras is said to have possessed immense riches, inasmuch that "The wealth of Cinyras" became proverbial, for expressing an over-grown estate. As the worship of Venus was first established in Cyprus by Paphus the father of Cinyras, both he and his descendants were buried in the temple of Venus at Paphos, an honour which was granted to no other family. The priesthood of Venus was likewise entailed on their race, a dignity which they preserved for many ages, after the throne was seized by others.

**CINYRIA**, in *Ancient Geography*, a town of the island of Cyprus, famous for the worship paid in it to Urania. It did not subsist in the time of Pliny.

**CINYRUS**, a mountain of Italy, placed in the Picenum.

**CINZANO**, in *Geography*, a town of Piedmont; five miles S. S. E. of Chivazzo.

**CIOLI**, **VALERIO**, in *Biography*, a sculptor of some eminence, who was born about the year 1530, at Settignano, a village near Florence, which, from its vicinity to some excellent quarries of stone, has at all times furnished a number of good sculptors. Valerio was, in his infancy, instructed by his father, Simone Cioli, a sculptor of some merit; but, at the age of 15, he was placed under Tribolo, an artist of considerable reputation, who at that time was employed in works of sculpture and architecture by the duke Cosimo, at one of his villas near Florence.

Having staid four years with Tribolo, he went to Rome, where he put himself under the tuition of Raffaello da Montelupo; one of the best imitators of the style of Michael Angelo; by whom he had indeed been employed in the execution of some of the statues for the celebrated monument of pope Julius II.

Having finished his studies, he was for some time employed to restore many of the ancient mutilated statues; but he was afterwards chosen for a work which allowed greater scope to his abilities; it is the figure of Sculpture, who is represented in a disconsolate attitude, weeping the loss of the great Michael Angelo Buonaroti, and is one of three statues which adorn his tomb in the church of St. Croce at Florence.

It is to be regretted, that a great part of the life of Cioli was sacrificed in the execution of the ridiculous grotesque figures in the gardens of Boboli, which, though intended to ornament, are alone calculated to call forth sentiments of pity or contempt, for the peurile and corrupt taste which gave them birth. He died, aged upwards of 70, and left a son, Simone Cioli, who followed the profession of his father, but who possessed small talents. Gherardo Silvani was likewise his disciple. Baldinuci, Dec. 1, della Par. 3, del. Sec. 4.

**CIION**, in *Anatomy*, is sometimes used for the uvula.

**CIION**, or **CYON**, in *Gardening*, a young shoot, sprout, or sprig, put forth by a tree.

Grafting is performed by the application of the cion of one plant upon the stock of another.

To produce a stock of scions for grafting, planting, &c. the gardeners sometimes cut off the bodies of trees, a little above the ground, and only leave a stump or root standing; in this case the redundant sap will not fail next spring to put forth a great number of shoots.

In dressing dwarf-trees, a great many scions are to be cut off. See **PRUNING**.

**CIONE**, **ORGAGNA** (da) **ANDREA**. See **ORGAGNA**.

**CIONES**, in *Antiquity*, a kind of idols very common, being only oblong stones, erected pillar-wise; whence also they had their name.

**CIOS**, **ESKER**, in *Ancient Geography*, a river of Thrace, the *Oeseus* of Pliny, and thus denominated by M. D'Anville, had its source in the N. W. part of mount Rhodope, in the country of the Pæonians. It passed by mount Hæmus, near its middle, and, pursuing its course through the western part of the Triballian plain, emptied itself into the Ister, near one of the two towns which bore the name of Oeseus.—Also, a river of Asia Minor, in Bithynia, which watered a town of the same name, according to Pliny. The town called Cios, was situated, says Pliny, in the place called Ascania of Phrygia. Pomponius Mela says, that it was seated at the bottom of a small gulf, formed by the Propontis; it is called in Greek, "Glio," in Turkish, "Kemlik."

The town of Cios had been built, according to Aristotle, by Cios, who conducted thither a colony of Milesians. Eustathius says, that Cios was one of the companions of Hercules. The town was destroyed by Philip, father of Perseus, and king of Macedonia, and its territory surrendered to Prusias, king of Bithynia, who rebuilt it, and gave to it his own name, Prusias.

**CIOTAT**, **LA**, in *Geography*, a sea-port town of France, in the department of the Mouths of the Rhone, and chief place of a canton, in the district of Marseilles, seated at the bottom of a bay in the Mediterranean, in a country which produces delicious fruit, oil, and excellent wine. The harbour is in the form of a horse-shoe, and defended with several forts; four leagues S. E. of Marseilles, and  $7\frac{1}{2}$  S. S. E. of Aix. The place contains 5770, and the canton 8738 inhabitants; the territory includes  $162\frac{1}{2}$  kilometres, and 4 communes. N. lat.  $45^{\circ} 10'$ . E. long.  $5^{\circ} 31'$ .

**CIPHER**, or **CYPHER**, in *Arithmetic*, one of the numerical characters called figures, and formed thus 0. The word *cipher* is probably derived from the Hebrew ספר *saphar*, to number. By the Italians it is written *Zifra*, by the French *Chiffre*, and by the low Latins *Ciphra*. It is, therefore, more properly spelt 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 serves to augment each of their values by tens; and in decimal arithmetic,

## CIPHER.

arithmetic, it lessens the value of each figure to the right thereof, in the same proportion. See the article ARITHMETIC.

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 moveables.

Formerly, when merchants and tradesmen were not allowed to use armorial bearings, they had ciphers thus artificially composed in their stead; which mostly consisted of the first letters of their names, curiously intertwined about a cross, &c. 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.

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 very 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 towards 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.

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.

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 by 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 endeavouring 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 serpent's teeth; and yet it was but a barbarous act of Thamus, 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* (*Departm. Diplom. tom. i, part ii, p. 538.*) mention is made of only three or four (and these not the principal) authors; so that we conceive 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

## CIPHER.

And again :

“ Sæpe tacens vocem, verbaque vultus habet.”

Schottus, in his “Steganographia,” exhibits an arthralphabetical alphabet in Latin and German; also Mr. Falconer, in his “Cryptomenysis Patefacta,” and Bp. 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 been often commended for its antiquity: since the ancients used to express any number under 100 by the fingers of the left hand; and above 100, and under 1000, by those of the right hand. Moreover, Pierius has particularly described their methods of reckoning from 1 to 9000: and hence Juvenal says,

“ Rex Pylius, magno si quicquam credis Homero,  
Exemplum vitæ fuit à cornice secundæ,  
Fælix nimirum, qui tot per sæcula vitam  
Distulit, 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 endeavour 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,” lib. vii, cap. 56, 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 apprized 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 on between the parties. See *Onosander's Strategicus*, cap. 25, 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 Tacticus*; 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 (Lib. x, cap. 45, p. 296, tom. iii, Lips. 1790, edit. *Joh. Schweighæuser*) attributes the invention to *Cleomenes* and *Democritus*, or

vol. VIII.

(more correctly) to *Cleoxenus* and *Democlitus*, in words thus rendered: “Postrema ratio, cujus auctores sunt *Cleoxenus* & *Democlitus*, sed quam nos correximus, certa definitaque est, adeo ut quidquid exortum fuerit negotiis, 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* shewed, how to correspond alphabetically, and to give or receive any species of intelligence, without this previous concert. The plans of *Æneas Tacticus* 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 *Polyb. L. 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 into 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. When the water is drawn off from any of these vessels, which must agree exactly in size, &c. it is evident that 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 Tacticus* 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 also 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 tubes, 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 (*παρπατερεχθαι*) ten feet broad,

G

and

## CIPHER.

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 the 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 αδ' ημων ηυλομολησαν.* 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 Φύλαξι or Πυρρεια 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 α, let κ be its substitute: Thus,

	1.	2.	3.	4.	5.	
a	i	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 towards 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 shews 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 .  
w e p e r i s h b y f a  
33 . 24 . 34 . 15 . 11 . 34 . 14 . 14 . 24 . 43 . 15 . 11 .  
m i n e a n d d i s e a  
43 . 15 .  
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 left hand. It is worthy of remark, that this very principle for 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.) But we have advanced enough to shew that the ancients, 2000 years ago, knew how to maintain secret correspondence by signals. We shall next prove that they were also acquaint-

ed 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 Lacedemon," endeavours to shew that the Spartans were the inventors of writing in cipher; and that their Scytalæ 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 Tacticus 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 *Scytale*, 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 keep 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 Lacedemonians, 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 shewed 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 scytale 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 seems to have assumed a more regular and systematic form; but the

## CIPHER.

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 Tacticus, and Polybius, are our principal guides; the former of whom was contemporary with Aristotle: (vide "*Æneæ Vetustissimi Tactici 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 he has 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 :: S P :: L C H · R, which signifies  
DIONYSIUS PULCHER.

H · R · C L : D · S V · 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 a 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 lie hidden in a piece of knotted thread. Bishop Wilkins has farther illustrated this device, in the 5th and 11th chapters of his "*Secret and Swift Messenger;*" and we have given a representation upon *Plate II, fig. 1*, of the graduated 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 *Poliorteticus*, § 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's little treatise!

He likewise describes several ways of fraudulently conveying intelligence into a besieged town, &c. For example, by the application of a manuscript to a sore leg, instead of a plaister 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 earrings, &c. 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 afterwards covering it over with melted wax;—to which are added some other singular proposals, shewing the fertility of invention exercised by the ancients on such occasions.

But the strangest contrivance was that of Hystæus, 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, Hystæus 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 cabbalism which the Jewish rabbies call *צירוף*, or combination. Bishop Wilkins has cited examples of this sort among the Hebrews; and it was also practised 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. &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 statesmen

## CIPHER.

in this respect, as there was formerly; but we are in possession of certain facts, which shew 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 labour of the decipherer; and yet remain commodious enough, so as to be readily wrote and read; but through the ignorance and unskillfulness 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 enlightened nations. The ancient Gauls, Saxons, Normans, &c. used more commonly to employ new and uncouth alphabetical characters for secret writing; many examples of which were collected by Trithemius, and the other systematic authors on polygraphy, in the 15th and 16th 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 *ταχυγραφία*, or *βραχυγραφία*, was not composed entirely at random, but according to some preconceived system.

The Tyronian *note*, 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 sigillæ, used to be chiefly inscribed on statues, arms, coins, public records, monuments, &c. for the sake of brevity, rather than of se-

crecy; 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 towards 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 them 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 this 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 towards 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 topic; *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; afterwards by \*Blaise de Vigenere, Walchius, Isaac Casaubon, \*Schottus, \*Gustavus Selenus, Gerrard Vossius, Herman Hugo, Schwenter *alias* \*Hercules à Sunde, Wecker, Nicéron, \*Lord Bacon, Caspi, Seeländer, \*J. Balthasar Friederici, Comiers, Basaccioni, La Fin, Dalgarno, Becher, Hiller, \*Bishop Wilkins, J. Nicholas, Buxtorff, Caramuel, Wolfgang, \*Falconer, Horsley, P. Crinitus, Ernest 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, \*Thickesse, 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. 2428. We have named the unedited works of these two Englishmen, because Dr. Wallis's papers have been often 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, § iv, ch. 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

## CIPHER.

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! That 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 this 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.

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 Punic wars, mention is often made of certain rude methods of correspondence; besides which, Ammianus Marcellinus speaks of the *vexillarii*, 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 cœlo constare sereno,  
Dat clarum è puppi signum."

Also in *Æneid* ii, 255, before quoted; which implies that Agamemnon from his ship, and Sinon 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 natives 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 representation 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 combination 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 lanthorns, blue-lights, false-fires, or rockets, with the occasional report of guns, in such a way as to keep up a regular correspondence. The lights displayed for signals in the dark, must always be arranged perpendicularly, to avoid any apparent change of their relative position, 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.*

Lights.	stands for	Fig.	Lights.	stands for	Fig.
0		1	0	}	7
0		2	0		
0			0		
0		3	0		
0			0		
0		4	0		
0			0		
0		5	0		
0			0		
0		6	0	}	9
0			0		
0			0		10
			A false fire		The







CIPHER.

⊙ h 2 ⊙ h 2 ⊙ h 2  
 ⊙ h 2 ⊙ h 2 ⊙ h 2  
 ⊙ h 2 ⊙ h 2 ⊙ h 2  
 ⊙ h 2 ⊙ h 2 ⊙ h 2

Solution.

Indien het voorvalt, dat die personen ons verblijft met hem te spelen, y welk men nimmermeer moet beginnen als na een uitgedrukt gebod, moet men geen driftigheid tot spelen noch yver om te winnen laten blyken.

No. VII.

87A 88†† 7d†L 7¶w6g†6A, 7d† 16AA 87A 8g6-  
 87sd†† 7†6¶w6A 18¶w6, 8AA 7d†L 8A OLT-  
 6†78†9†. d6w6A; 7d† 16AA 87A 7806A wog9†  
 u6A 11AA d6¶7¶7¶1616.

Solution.

Man muss also arbeiten, als wenn man niemahls sterben würde, und also in Gottesfurcht leben; als wenn man Augenblick den tod verewartete.

No. VIII.

מחשבת אמת צדק ומשפחה חסידים  
 חסידים ומשפחה חסידים ומשפחה חסידים

Solution.

Equidem non nego quod ex iis quos febris acutissima aggreditur, pauci ad sanitatem redeunt.

No. IX.

⊙ h 2 ⊙ h 2 ⊙ h 2  
 ⊙ h 2 ⊙ h 2 ⊙ h 2  
 ⊙ h 2 ⊙ h 2 ⊙ h 2  
 ⊙ h 2 ⊙ h 2 ⊙ h 2

Solution.

Ἰμεῖς ἔστε οἱ δικαιοῦντες ἑαυτοὺς ἐνάτιον τῶν ἀνθρώπων ὁ δὲ θεὸς γινώσκει τὰς καρδίας ὑμῶν ὅτι τὸ ἐν ἀνθρώποις ὑψιλὸν βδέλυμα ἐνάτιον τοῦ θεοῦ ἐστίν ὁ νόμος καὶ οἱ προφῆται ἐως ἰωάννου ἀπὸ τότε ἡ βασιλεία τοῦ θεοῦ ἐπαγγελῆται καὶ πᾶς εἰς αὐτὴν βιάζεται.

In the beginning of the fifth century of the Christian æra, Pharamond, and other reigning princes, invented characters of singular forms; and, during the eighth and ninth century, Charlemagne kept up a private correspondence with his agents in the north of Europe by similar modes of deception. Some of these alphabets, including that of Pharamond, are preserved by the noble duke Selenus, and by Trithemius. We have selected and exhibited (as a specimen of such inventions) one of those employed by Charlemagne, in *Plate I. figure 1*; under which is seen *fig. 2.* the form of another secret-alphabet, used in England during the reign of Alfred, copied from a MS. in the Bodleian library. (Vide "Aistle's Origin and Progress of Writing, chap. vi. 2d edit. Lond. 1803.") Rudolphus IV, archduke of Austria, who lived in the 14th 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 15th 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's curious book to the flames!!!

In *Plate I. fig. 6.* we have represented the cipher used by 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. N° 132, and 6988 Bibl. Harl.) We subjoin part of one of this unfortunate monarch's letters, dated Aug. 1st, 1648, as a specimen of that kind of cryptography; and, for an explanation of many more of them, we refer to Dr. Wallis's 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 : 245 : 339 : 363 : 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, (Nov. 7th, 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 24 short strokes, variously situated upon a line; and by which, April 5th, 1646, he wrote to the earl of Glamorgan, afterwards the marquis of Worcester. See Royal Letters, Bibl. Harl. vol. iii. 118, 119, &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 invention. (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. N° 2428.) 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 Sept. ye 21th, 1659."

We here extract the marquis's words regarding this 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 24 letters; and as ready to be made for the one letter as the other."

"This invention, so refined and so abbreviated, that a point

## CIPHER.

point only sheweth distinctly and significantly any of the 24 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 a 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 afterwards made touching the nature of this noble author's contrivance. We shall notice one of these guesses, before we proceed to give a farther description of it. See *Gent. Magazine*, vol. xviii. p. 55.) An anonymous gentleman proposes "to rule his paper with quaternions of lines, as if for music, and to let the points representing the letters be placed on, or 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 his 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. 2428, 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 cypher" 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 shewn in *fig. 5. Plate I.* An engraved page is given to write upon, in which are made horizontal rows of octangular squares or chequers; and a strait line is to be drawn from the centre towards 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

VOL. VIII.

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 of paper," he advises "to omit all needlesse 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 any thing 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 practiced."

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 24 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 natâ*, and no need of provision before hand; though much better if forseen, 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 French-man, Italian, Spaniard, Irish, Welsh, being scollars, yea, Grecian or Hebritian, shall as perfectly understand it in their owne 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 English."

No. 33. "To write with a needle and thred, white or any colour upon white, or any other colour; so that one stitch shall significantly shew any letter, and as readily and as easily shew 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 interrogation, 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 lattan 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. 45. "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."

## CIPHER.

fication 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 dispatch, 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 dispatch; 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  
 2      999 4 10      50 1000 14  
 unreasonableness 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 within 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 negociator 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 J. 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 J. 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 *ae*, not *a*, &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 labours: (Præf. ad Maximil. Imperatorem, Polygr. p. 100.) "In manibus jam habeo grande opus, quod si unquam fuerit publicatum, totus mundus mirabitur." See the article STENOGRAPHY.

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 proposal 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 kind of 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 also 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 cypher."

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

"There are several kinds of cyphers; as the *simple*; those mixed with non-significants; those consisting of two kinds of characters; *wheel-cyphers*, *key-cyphers*, *word-cyphers*, &c. There are three properties required in cyphers, viz. (1.) that they be easy to write and read; (2.) that they be trusty and undecypherable; and, (3.) if possible clear of suspicion. For, if a letter should come into the hands of such as have a power over the writer, or receiver, tho' the cypher itself be trusty, and impossible to decypher, '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 cypher, 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 cypher, 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 cypher of our own, which has the highest perfection of a cypher; that of signifying omnia per omnia; any thing by every thing; provided only the matter included be five times

## CIPHER.

times less than that which includes it; without any other condition or limitation. The invention is this; first let all the letters of the alphabet be resolved into two only, by repetition and transposition: for a transposition of two letters, thro' five places, or different arrangements, will denote two and thirty differences; and consequently fewer, or four and twenty, the number of letters in our alphabet; as in the the following example:

"A biliteral 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 an *A*, you write five *a*'s, or aaaaa; and to write a *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 shews a method of expressing, and signifying 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, cannon, &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 decyphered, by translating them into the letter *A*, only.

"The second, or Italic 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 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 me to you.*

"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 cyphers has introduced another, relative to it; *viz.* the art of decyphering, without the alphabet of the cypher, or knowing the rules whereby it was formed. This indeed is a work of labour and ingenuity, devoted, as well as the former, to the secret service of princes. Yet, by a diligent precaution, it may be render'd useless; tho', as matters now stand, 'tis highly serviceable. For, if the cyphers in use were good and trusty, several of them would absolutely elude the labour of the decypherer; and yet remain commodious enough, so as to be readily wrote and read: but through the ignorance and unskillfulness of secretaries and clerks, in the courts of princes, the most important affairs are generally committed to weak and treacherous cyphers."

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 labour 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 doubts, 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

## CIPHER.

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 especial 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 bilateral 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 threefold 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 shewn 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 pre-determined 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 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 Oettingen. 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 an harmonic alphabet, and several specimens of musical writing, in 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 5040 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 precise order and relation we should wish to use 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 pre-conceived 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**.

Having thus freely given our deliberate view of this subject, we lay before the reader some observations of Mr. Philip Thicknesse, who has laboured 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 amongst 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 soli* 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 endeavour 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,

## CIPHER.

guardians, by hearkening to his folly, impertinence, 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 "Deserted 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 any thing to do with the reading; so that the decypherer would not so readily know how to proceed, and many people there are, who will think it impossible to be made out without 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 cliff, 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 possession of the seven notes which express *a, b, c, d, e, f, g*; and know by ear exactly when either of those 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 quick, 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 common piece of 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  $\gamma$ , 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 Coventry's minuet implied, as it might, an assignation in Grosvenor-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 downwards, and all the nulls upwards; 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 careful 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 consideration 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 corded 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 least liable to suspicion; for who, that examined a suspected messenger, would think an old song, without words, in which perhaps the messenger's tobacco or snuff might be put contained the secret he was to convey? Nor could an ordinary messenger, either by bribes or threats, discover any thing more, than that the bearer was strictly charged to deliver that piece of music  
into



## CIPHER.

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 having 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 farther 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, without 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 language formed, as might be equally speakable by men of all nations, and so restore to us what we lost by the second general 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 constructing.

"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 the harmony: yet it is such a picture as must pass unsuspected by all who do not understand music perfectly, 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. Goldsmith's "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, conceal 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 upwards; and therefore, he passes over them, and takes down in order from the bass and treble cliff those only which are turned downwards, 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 suspicion

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 annexed 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 cyphers, *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 *bye-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 shew 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 *Pl. 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 characters.

"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 harmonic alphabets, might write two letters on different subjects, 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 repeating them, as is usual in singing songs, may sing those in due time, with the air which conveys them: and though I confess I see much harm might arise from it, yet it may be right to observe, by the bye, that an harmonic letter thus written could not easily be brought home with any degree of certainty (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

## CIPHER.

as it may be productive of much good, as well as of mischief; 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 cryptographic writing by the several princes and states in Europe. How often do we hear of a courier, being murdered, and his dispatches 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 endeavours 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 alterations 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 of conducting a correspondence in this way be so great, and the labour of composing it so considerable, we should rather give the preference to lord Bacon's idea of a bi-formed 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 *INK*.) 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 somewhat 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 shewn uncommon industry and acumen in this way, believed "that the most sure cipher, practicable in a current converse, may make a discovery;" and "if you once understand the rules for deciphering 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 out of 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 endeavour 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  
at,

## CIPHER.

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 labours 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 afterwards, 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 cypher, 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 Davys' 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 Deciffratoria*," 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 labour and time necessary to accomplish their design." (Letter to Leibnitz, Jan. 16, 1698.) We are therefore not to wonder that so few persons attain to a moderate degree of excellency, or even endeavour to cultivate this art, in any single 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 destined,—the person for whom 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, "*& 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 shew 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

VOL. VIII.

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 shewed 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," adds he, "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 endeavour 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 his 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.

Endeavour 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 *g* 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 than the latter, those characters stand for *gu*, which two, except in a few Scotch names, are always followed by a vowel. 6. That although every language has something peculiar in its structure, the fore-

## CIPHER.

going 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 spelt. It is probable the vowels *e* or *o*, are these; as *meet*, *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*, *n*, *r*, *s*, *t*; and next to those, *c*, *f*, *g*, *l*, *m*, *v*; 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*, *x*, *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 *thiss*; 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 *on*, 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*, *these*, *their*, *thirst*, *thwart*, &c. &c.

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

A B C D E F G H I K L M N O P Q R S T U  V W X Y Z	} Beginning a word is regularly followed by	most of the letters. a, e, i, l, o, r, u, y. a, e, h, i, l, o, r, u. a, e, i, o, r, u. most of the letters. a, e, i, l, o, r, u, and sometimes y. a, c, h, i, l, n, o, r, u, y. vowels only. most of the letters. a, e, i, n. vowels only. vowels only. vowels only. most of the letters. a, e, h, i, l, o, r, s, sometimes t, u, y. only by u, and QU by a, e, i, o. a, e, sometimes h, i, o, u, y. a, c, e, h, i, k, l, m, n, o, p, q, t, u, w, y. a, c, h, i, o, r, u, w, y. sometimes d, and g, l, m, n, p. sometimes r, s, t, x. vowels only. a, e, h, i, o, r, y. sometimes a, or e. e, sometimes i, o. 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, 8vo. Lug. Bat. 1739, and in the latter part of Breithaupt's "Ars Decifratoria, sive Scientia occultas 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, &c. 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

## CIPHER.

junction 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 Con-

spiracies 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>know</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 would have business very I possible of I send hear against my 'till what little upon *know 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 an of thought my and go you in or resolved so I intend he or them *our friends*, &c. &c. &c.

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.

2. 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 amongst the several characters. This admits of no particular rules; nor will the judicious need any.

3. 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 preheminance," there must be several alphabets framed for each of its letters in the manner following:

# CIPHER.

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

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 backwards 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 ztze ixt hdasytgh  
idcb wofr rihm obr rihm rxsh:  
dfaawi fd, zc espi getww cpfzwe ez  
cq nwxg bynmrtg. Qibcn.

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

*Solution.*

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 this for the first line:

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

## CIPHER.

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, 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 all 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 a-new, 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 qzcnpo cx mggr rfc lgdwbxkl  
 kcdc zriv hzyc hvl mewh puqf:  
 bdytyg hf, sw gvrl ylnn wizspy id  
 hws pypxi bynmrtg. Kcsvg.

#### Solution.

When the alphabet is changed at every word, you may either make suppositions 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 forwards as before, until you come to the end of the epistle.

4. Afterwards 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 1, you shall find the twentieth word *id* decipherable by its alphabet, *viz.*

A.P. and consequently *hws*, the one-and-twentieth word in the writing, but twentieth after *oa* the second word, to have one alphabet with it; and in the same order *pyfxi* to have one alphabet with *qzcnpo*; and *bynmrtg* and *cx* 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 *Lydwbxkl* are written by the same alphabet, but not the seventh from that, *viz.* *fyqf*, nor the seventh from *oa*, *viz.* *kcdc*, &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 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 oqptv yw oqnc yvg xdzorgpl  
 kgsn mmaq hhwc pbo qcpw saib:  
 xgyepl xx,df eqgw oyep, zigxyy gg  
 yxs pwgkq hgimhvtl. Mvnyh.

#### Solution.

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

1. Extracting out of it the monsyllables, &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 *yvg* 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 monsyllables, &c. in any part of the epistle; or you may consider what letters can follow *enc*: and thus *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 afterwards 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

## CIPHER.

great many. *E.g.* In the last example 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 continually 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; whereas 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 occasion 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 parts 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 Gronsfeld, 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.

4 3 6

a b c d e f g h i k l m n o p q r s t u v 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

The governor of the city is beyond corruption  
64 3643 64 364 36436436 43643 64 3643643 64  
so that we may conclude there is nothing of  
36436436 4364 36436 436 4364.  
bribery will 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 3; 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 eoxa ow dkbqsg etvtasworp yr  
wndw bh ofb etqeqyfk xkkvg ow ptxkoqi ti dxmdkvlk  
zlqo vkvxk 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. Endeavour 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  
xkk kqahtsr t i wnh eoxa ow dkbqsg etvtasworp  
31 2312 31 231 23123123 12312 31 2312312 31  
yr wndw bh ofb etqeqyfk xkkvg ow ptxkoqi t i  
23123123 1231 23123 123 1231.  
dxmdkvlk 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 forwards: 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 24 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 it 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 for all the rest, until you

come



## CIPHER.

come to an end, or rather the side of the epistle, towards 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, Sclavonic, &c.

At first the Greeks wrote from the left to the right hand, and again from the right 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	c	i	d	s
i	e	a	o	o	b	s	w	s	y
l	c	s	m	t	a	i	e	p	d
c	n	e	a	b	c	e	g	e	e

Here the rows are introduced instead of the lines. And if you begin at the first letter towards 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 supplie."

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 shew 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.)

Our calculation is, however, carried no higher than the number of changes in an alphabet consisting of 36 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 24 letters, if each of them completed 40 pages a day, and every page contained 40 permutations; and Mr. Falconer has shewn 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 36 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

*A Table of Changes in the relative Position of 36 Letters.*

1 =	1
2 =	2
3 =	6
4 =	24
5 =	120
6 =	720
7 =	5040
8 =	40320
9 =	362889
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:

371993	326789	901217	467999	448150	835200	000000
sextillions	quintillions	quadrillions	trillions	billions	millions	units

*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,

## CIPHER.

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 amongst themselves, the same way as letters. Therefore,

2. The order of the rows is agreed upon at 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 frame 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 combinations agreed upon is set down in a row, in the first column towards 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 written by the square key."

### Form of the Table for Writing.

Order of Positions,	A	B	C
1 CBA	<i>a t s a s k d e t</i>	<i>e c e h m a a l i y</i>	<i>w e h e r t e n r e</i>
2 CAB	<i>e t c w o n u y y</i>	<i>b i c h u f f p o t</i>	<i>r a u d y e y t b</i>
3 ACB	<i>i o e e h o o u h</i>	<i>w t s h v w o n s</i>	<i>g n s t a r n r e</i>
4 BCA	<i>h n u t n l a t a</i>	<i>i o y e e i c e g</i>	<i>t k o r u l c x u</i>
5 BAC	<i>x w a e e c i e e</i>	<i>e o h h d b s b r</i>	<i>p t v a r r o w k</i>

### A further Explanation of this Table.

CBA, 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.

CAB, 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.

ACB, 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 the 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 any thing to write.

The writing taken out of the table will stand thus:

$\Delta$  *A t s a s k d e t . e c e h m a a l i y . w e h e r t e n r e .*

*e t c w o n u y y . b i c h u f f p o t . r a u d y e y t b . i o e e h o o u h .*

*w t s h v w o n s . g n s t a r n r e . h n u t n l a t a . i o y e e i c e g .*

*t k o r u l c x u . x w a e e c i e e . e o h h d b s b r . p t v a r r o w k .*

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.

1. 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  $\Delta$  (which must be supposed to shew that three letters are combined); extract the three first letters from the three first 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 or other prime number, and the last quotient again by a prime number, and so go on until the last quotient of all be 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 help of them you will find all the rest of the divisors, *viz.*

By multiplying the first prime divisor, towards 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 towards 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,

## CIPHER.

and, 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, 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, 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	o	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	u	p	y	o	o	n	a	c	c	i	s	o
8.	e	l	n	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,

VOL. VIII.

1. Search in the several lines for some of the particles of that language you may suppose the epistle 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, *o* 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, 7, 8, 9.

<i>Rows</i>	5	7	9
	6.	<i>f</i>	<i>o</i>
	1.	<i>b</i>	<i>i</i>
	2.	<i>i</i>	<i>o</i>
	3.	<i>c</i>	<i>e</i>
	4.	<i>h</i>	<i>e</i>
	5.	<i>u</i>	<i>h</i>
	7.	<i>p</i>	<i>o</i>
	8.	<i>o</i>	<i>u</i>
	9.	<i>t</i>	<i>h</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:

4.	5.	7.	9.
1	<i>e</i>	<i>b</i>	<i>i</i>
2	<i>t</i>	<i>i</i>	<i>o</i>
3	<i>c</i>	<i>c</i>	<i>e</i>
4	<i>w</i>	<i>h</i>	<i>e</i>
5	<i>o</i>	<i>u</i>	<i>h</i>
6	<i>n</i>	<i>f</i>	<i>o</i>
7	<i>u</i>	<i>p</i>	<i>o</i>
8	<i>y</i>	<i>o</i>	<i>u</i>
9	<i>y</i>	<i>t</i>	<i>h</i>

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	<i>r</i>	<i>e</i>	<i>b</i>	<i>i</i>
2	<i>a</i>	<i>t</i>	<i>i</i>	<i>o</i>
3	<i>u</i>	<i>c</i>	<i>c</i>	<i>e</i>
4	<i>d</i>	<i>w</i>	<i>h</i>	<i>e</i>
5	<i>y</i>	<i>o</i>	<i>u</i>	<i>h</i>
6	<i>e</i>	<i>n</i>	<i>f</i>	<i>o</i>
7	<i>y</i>	<i>u</i>	<i>p</i>	<i>o</i>
8	<i>t</i>	<i>y</i>	<i>o</i>	<i>u</i>
9	<i>b</i>	<i>y</i>	<i>t</i>	<i>h</i>

## CIPHER.

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  
 c 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 c 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 c 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. eechmaaliy, or wehertour.* 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 adventure at all, once next 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 b x y f q.

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 towards the left hand, and 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 towards the right hand, &c. *Diagonal* is a mathematical term, from *dià,* 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 e n c r h l s . a 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 n 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 may 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, h,* 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. By inserting nulls before the epistle.

As to the first, if they begin at the lower angle towards the left hand, the words will discover themselves as before. Only the order of the lines will be reversed in the operation, *viz.* The first line is last in the true order, &c.

2. If they begin at the upper angle of the parallelogram towards the right hand, the lines will be in their true order, but the writing must be read backwards. 3. If, at the lower angle towards the right hand, the order of lines will be reversed, and the writing must also be read backwards. This holds true by the ordinary operation; but you may frame your figure for discovery, according to these three suppositions, *viz.* beginning it at any corner, &c. Yet, we think, the ordinary operation will give the speediest resolution.

*Note.* From beginning at the lower corner towards the right hand, you are not to expect words or syllables in the beginning of the first line by your operation, seeing it is last in the true order; and mutes, perhaps, may be inserted to fill up the void places in the figure, so that you must observe the other lines.

As

## CIPHER.

As to the second method, by inserting nulls before the epistle, they may, in process of time, be discovered thus :

When, upon trial, you find the writing in the epistle will make nothing of sense, lay aside the first letter, and make a new supposition with those remaining ; if nothing yet appear, lay aside two letters, and proceed as before ; then leave out three, four, &c. until you perceive words.

We next shall analyse that kind of writing in which *more letters are used than are requisite*. The first remarkable, and very ordinary, contrivance in secret writing, by more letters than usually go to the framing of words, is that insisted on by Schottus, (in his "Scholia Steganographia,") viz.

1. The confidants at parting frame an alphabet of figures to write by ; *e.g.*

A	b	c	d	e	f	g	h	i	k	l	m	n	o	p	q	r	s	t		
4	22	10	9	1	11	13	18	3	19	12	8	20	2	21	23	7	6	5		
v	w	x	y	z.																
15	14	16	17	24.																

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	20	3	13	18	5	4	5	
I	s	h	a	l	l	s	e	e	y	o	u	t	h	i	s	n	i	g	h	t	a	t
16	2	15	7	12	2	9	13	3	20	13	6											
y	o	u	r	L	o	d	g	i	n	g	s.											

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 of hazard 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."

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 6th letter from *v*, viz. under *d* ; and 18 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 dipt in water, &c.

### *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 afterwards 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 endeavour 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.

### POST-SCRIPT.

Pray  
expose not yourself to  
imminent danger.

A K Q

Now

## CIPHER.

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

This measure is not in danger; to all it is as yet secret; there is now no thing in view to threaten our safety, but by flight we should ruin all our designs. Do not fail to meet me by six in the usual manner: half an hour hence, I intend to be at the council. Let the next meeting be where they will, I'll have notice: just without the gate was the governor this morning (if my sense are sound) secure as we could wish him; we may conclude to have hit right on the means, and more clear infallible evidence is not on this side conjuration: the snare is prepared, they are misted, and see not 'tis effectually to entrap them, and on their ruin to raise you and

Your, &c.

### POST-SCRIPT.

Pray throw off those vain fears: expose not yourself to scorn, when there is not any imminent danger.

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 *a*, a second to stand for *b*, and if there be a third, let it be supposed *c*. Afterwards 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 way 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 a word: for when two letters go to the composition of the alphabet, they must have five places; and the words will consist of 5, 10, 15, 20, or 25, letters, &c. If three letters are in three places, you will find 3, 6, 9, 15, or 18 characters, &c. in each word: if five letters in two places, the words shall have 2, 4, 6, 8, 10, or 12 characters, &c. a piece.

2. From the number of the 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 3 characters: *e. g.* *a, b, c*; and if 5 in a rank, you will possibly have but 2 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 (whether 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 *more 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 labour 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 the 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 menchette an butter; an mi sistre (a joli nymphe) tu chat tu yeux, & sing yeux an ode, tu 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 tu the rude Squire:—but pardon mi long lettre, pré doux comme tu us about mai, if yeux canne: mi service tu ure niece: hoüe 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 colours, (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;

## CIPHER.

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 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 pedlar's toys, without the slightest suspicion of its insidious contents. If only three colours 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 matrem, qui nunquam novit verbum Latini sermonis, in duabus horis docere scribere, legere, et intelligere Latinum satis ornatè et disertè, quantumcunque voluerit; ita ut quicumque viderint ejus literas, laudent verba, intelligent 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 ornatè 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,

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

2. These alphabets require a more than 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 freely 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 before 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 upwards 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 into each 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," endeavours 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 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 endeavoured to shew 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 shew how puerile any common endeavour 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 practised by letters and figures, or words, or by all mingled together, without any apparent difference in its form. The reader will never discover any thing 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

state's

# CIPHER.

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 engraven 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.

152618035466693599507192735855362202836931217327  
 245920645394011183947056667685756342011439314394  
 706595077377993219296977788565806653544536151393  
 294785046353641935574079616392439375896198162891  
 963401283797466464393112515532259472106664630615  
 316495968670125532261892940717273752693373561630  
 111839470223534599324251116177507163064696146047  
 396196849394786382053824306637295903546799396818  
 814241505284652207565474849424546691116180271131  
 181215172736480949922450654401526391403546450585  
 938016351127572159689409599920342824626514355849  
 750765645670655704298943235151226059520112556686  
 749471813940832326185713035464507483150566895445  
 512171836151643044352858374468160666509554768388  
 035938598941227616384439371726374934581971417363  
 934937173772693947584872425162776569386776645475  
 849593693533642939977726384949353464593385293948  
 775729335036291525573993869407799931118017363534  
 144948678911546393959992032465312151775790458112  
 182458936847344546061634743933239122516173546075  
 738412872248587874759694930001118484942455693717  
 298756400667263932218363946355455774393839400748  
 924261846569335464500075651432544581938674850858  
 995445512251615937799071574958459398823246652465  
 8477283736933585993152618174693987447572812357443

bawmkarupfoy.ujozaruhsnyffaxmopets.jhupe.awadzmyg  
 lrert.puhv.kn.usscoxzpewanohjkffyqpd.ubcdp.jsydfkwz  
 elqgrufxglvjrpmcdlw.t.foi.elcyzjfxpablvpdwqozk.ugrjldr  
 u.ng.dhyerpwpwyzjvplsizfhkj.j.smbwebzoaykr.c.ekt.piqe  
 flxmgjyvdu.ucsgfanzjvzgtmhyw.mbrpfxglkzpecfpdx.r.  
 hveh.uwqbwgdgldqkvlwzjhsmlchbtglrpglxvbe.pesvjw.x.j  
 tmgzjd.ugkovcbslqaharuhcw.rulyqjlsvp.pjllcwrzmzprdp  
 pruaucdp.jelgljfvvrjquoyh.rp.lobj.symdeezykqh.zifequle  
 whjudw.fhg.cbseu.rplqbspdfwqhwiuwpjezyrp.kifgtcnzjf.  
 qmeltekfsdru.gfwi.rpanq.rzayfjcbghzmhua.yeafvawezkzp  
 vkcfzm.uuyshtdfklqgtuffxgwxwazjxhlwnozyrplqfh.jnafqalj

gquvlhaeyzu.r.scstfavl.yhj.kxzyefveekw.zmcpzpa.ahw.zj  
 yljoxq.uaceiyyaabgsisoxmhwwmdu.uyduak.veldddwlfqrpq  
 ofrzpdfadvwoqzwpv.uox.lihaealcsnyldj.uhcigiuyw.uxonb  
 quysshiyw.kt.jhcafeljh.pzdiqodlnjgtaclefie.dzuuqaoihoxo  
 mlvaqpkwrul.dijyrj.reljhdqcp.jg.qhj.rub.qm.pqvhewqey.  
 jt.zpuelpfbagfaih.rjolae.uieea.ucs.j.zjmnulm.pdckbhkxvkw  
 rebblnorj.a.rfh.jgdkvpfbmqnmoia.l.ui.nshfdatywizjcoyuk  
 yqdl.plbluodkj.pmp.iappfkaqfjderjwqzooybglnsvvfxl.k  
 hiaj.ae.uccococucikccnec.jhbitwuiawmzpiiij.rjmsvujlyaiof  
 dflfodu.uxuqm.uqy.tytedqdlehrje.aip.zuifeltgjmseh.nc.pg  
 .yhuk.jktk.kkzfo.haoislqn.jqoq.rjhcycaqap.zpafdw.pptyee  
 agyjofhfozmmushb.yhrjvwz.zjqoedyabi.t.uy.dhaxahy.ift.k  
 uru

Great care has been taken, in a former part of this article, to exhibit the peculiarities of the English language, and to point out the most approved means of deciphering any secret writing composed alphabetically: and, "such is the craft of man," says a modern author, "that it is scarcely possible for a letter in cipher to be 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 trifomed 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 towards 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



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 deep; and it will be observed, that the 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 analysing 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, Rasc quema Lovazig arodi; Moxati Ho hyka Fagiva myne quipaxo Aukava in Onfa yani moxarico, Pangdo Spulzi Jorixa mugaro ya zangor Alsiva yival ponbine Kazeb re lynthvath.

CIPHERING, or *CYPHERING*, is popularly used for the art of accounting; properly called *arithmetic*; which see.

CIPIERES, in *Geography*, a town of France, in the department of the Var; 10 miles N. of Grasse.

CIPOLI, a considerable town of Asia, in the kingdom of Nepal, containing about 8000 houses, and very populous. This, and other towns of the same country, both great and small, are well-built; the houses are constructed of brick, and are three or four stories high; but their apartments are not lofty; they have doors and windows of wood, well worked and very regularly arranged. The streets of all these towns are paved with brick or stone, so laid as to afford a regular declivity for carrying off the water. In almost every street of the capital towns there are good wells made of stone, from which the water passes through several stone canals for the public benefit. In every town there are large square verandas, well built, for the accommodation of travellers and the public; and on the outside of the great towns are small square reservoirs of water, faced with brick, having a good road to walk upon, and a large flight of steps for the convenience of those who choose to bathe. *Asiatic Researches*, vol. ii, p. 308, 8vo.

CIPONIMA, in *Botany*, Aubl. Juss. See *SYMPLOCOS ciphonima*.

CIPPUS, in *Antiquity*, a little low column sometimes without base or capital, but generally bearing an inscription. The cippi served for various uses among the ancients: placed in roads with distances engraved upon them they became military columns, or served the purpose of indicatory hermas. They were used for land-marks, and when the circuit of a new city was traced with the plough, cippi were placed at equal distances, on which sacrifices were offered, and which marked the situation of the towers.

The cippi found in sepulchres have been often taken for altars, on account of their form and ornaments, espe-

cially when the inscription has not contained an epitaph, properly speaking. The distinction is, however, very slight, as these cippi were consecrated to the infernal deities, and to the manes in particular; and they are even sometimes excavated in the upper part, in the form of a basin or crater. Fabretti mentions a number of cippi perforated from top to bottom, to receive libations in the manner of some altars. Hottinger has an express treatise of the cippi of the Jews, "*De Cippis Hebræorum*;" wherein he takes cippus for the tombstone of a defunct.

CIPPUS was also used in antiquity for a wooden instrument wherewith criminals and slaves were punished; being a kind of clog, or stocks for the feet.

CIPPUS, in *Entomology*, a species of *PHALÆNA-Bombyx*, with brown wings and three green spots, found in Surinam.

CIPRANDI of Milan, in *Biography*, a serious tenor singer, with much taste and feeling, arrived here in 1755, during the high favour and opera regency of Mingotti. He remained here a considerable time, for we find his name in the dramatic personæ of our lyric theatre in 1764, and 1765, with Manzoli, when, in the opera of Ezio, he was deservedly very much applauded in Bach's charming air, "*Non so dondi victre*," originally composed for the celebrated tenor Raaf. And at Milan, in 1770, it has been recorded by travellers, that he sung in the churches on great festivals, in a manner far superior to the rest of the choral performers. Indeed his cast of parts has seldom been better filled by subsequent tenor singers.

CIPRIAN RORE, or, as the Italians call him, *Cipriano di Rore*, one of the most voluminous and renowned composers of the sixteenth century, was born at Mechlin, in Flanders, 1516. In the title page of a book, published at Venice, 1549, he is called the scholar of Adrian Willaert. In the preface to the *Canti Carnascaleschi*, published at Florence, 1559, he is called *Cantore*; as if he had been merely a singer in the service of the house of Medicis. However, he seems to have spent the greatest part of his life in Italy, as a composer; in which character he is mentioned with great respect by Zarlino, Vincenzo Galilei, Pietro Pontio, and almost every Italian musical-writer of his time. And after having been successively maestro di capella to the duke of Ferrara, the republic of Venice, where he was the immediate predecessor of Zarlino, and the duke of Parma, he died at the court of that prince, 1565, aged forty-nine. His motets and madrigals were first published at Venice, 1544, and again, together with his masses, and many other works, after his decease, in 1562 and 1565. His *Cantiones Sacras*, or motets, were likewise published at Lovain, 1573.

CIPRIANI, GIOVANNI BAPTISTA, was of a Pistoiese family, but born in Florence, according to Heineken, in 1732. At a very early period of life he evinced great facility and taste in his drawings, many of which, in the manner of Gabbiani, are still to be met with at Florence. Lanzi mentions two juvenile performances of Cipriani in oil, in the abbey church of St. Michele near Pistoia; one representing St. Tesauro, the other St. Gregory the 7th, observing at the same time, that though he drew much he painted but little.

In 1750, he went to Rome to complete his studies, and soon afterwards came to England, where he was chosen a member of the Royal Academy, and lived much respected during the remainder of his life. Amongst the first works which Cipriani painted after his arrival in this country, was a room decorated with poetical subjects, in the house of the late sir William Young, at Standlynch in Wiltshire.

THE  
CYCLOPÆDIA;

OR,

UNIVERSAL DICTIONARY

OF

Arts, Sciences, and Literature.

BY

ABRAHAM REES, D.D. F.R.S. F.L.S. *S. Amer. Soc.*

WITH THE ASSISTANCE OF

EMINENT PROFESSIONAL GENTLEMEN.

---

ILLUSTRATED WITH NUMEROUS ENGRAVINGS,

*BY THE MOST DISTINGUISHED ARTISTS.*

---

PLATES. VOL. IV.

NAVIGATION — WRITING BY CIPHER.

---

LONDON:

PRINTED FOR LONGMAN, HURST, REES, ORME, & BROWN, PATERNOSTER-ROW,  
F.C. AND J. RIVINGTON, A. STRAHAN, PAYNE AND FOSS, SCATCHERD AND LETTERMAN, J. CUTHELL,  
CLARKE AND SONS, LACKINGTON HUGHES HARDING MAJOR AND JONES, J. AND A. ARCH,  
CADELL AND DAVIES, S. BAGSTER, J. MAWMAN, BLACK KINGSBURY PARBURY AND ALLEN,  
R. SCHOLEY, J. BOOTH, J. BOOKER, SUTTABY EVANCE AND FOX, BALDWIN CRADOCK AND JOY,  
SHERWOOD NEELY AND JONES, OGLE DUNCAN AND CO., R. SAUNDERS, HURST ROBINSON AND CO.,  
J. DICKINSON, J. PATERSON, E. WHITESIDE, WILSON AND SONS, AND BRODIE AND DOWDING.

1820.



# WRITING BY CIPHER.

I

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

2

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

3

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

# WRITING BY CIPHER.

Alphabet and Key.

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

H. Blair's Copy.

Handwriting practice lines for cipher writing. Each line consists of a top line, a middle line, and a bottom line, with small dots placed along these lines to guide letter height and placement. The page contains 20 such sets of lines, with the first three sets corresponding to the cipher key table above.

31 31 12 23 n 32 33 43 12 33 21 23 n 22 33 43 23 22 21 21 20

# A Better Copy of William Blair's *ALPHABET AND KEY*

*ALPHABET AND KEY*

	1	2	3	4	5	6	7	8	9
1	B	C	S	M	T	L	I	E	O
2	G	M	T	P	U	H	O	I	A
3	J	P	U	D	A	N	H	O	E
4	K	D	Y	F	E	R	N	S	I
5	Q	F	A	L	I	S	R	T	O
6	V	L	E	H	O	T	S	U	A
7	W	H	I	N	C	U	T	A	E
8	X	N	O	R	D	A	U	E	I
9	Z	R	.	S	F	E	A	I	O