CRYPTOGRAPHY

OR

THE HISTORY, PRINCIPLES, AND PRACTICE OF CIPHER-WRITING

CRYPTOGRAPHY

OR

The History, Principles, and Practice

OF

CIPHER-WRITING

BY

FREDERICK EDWARD HULME, F.L.S., F.S.A

AUTHOR OF "FAMILIAR WILD FLOWERS," "MYTHLAND," "NATURAL HISTORY LORE AND LEGEND," "THE BIRTH AND DEVELOPMENT OF ORNAMENT," "WAYSIDE SKETCHES," ETC

"*Here's now mystery and hieroglyphic.*"
BEN JONSON—*The Alchemyst.*

LONDON
WARD, LOCK AND CO. LIMITED
WARWICK HOUSE, SALISBURY SQUARE, E.C
NEW YORK AND MELBOURNE

CONTENTS

CHAPTER I

CHAPTER II

CHAPTER III

ILLUSTRATIONS

CHAPTER I

Meaning of cryptography—Objections to its study—Its legitimate use and value—Historic examples of its employment—Delight in the mysterious—Many other ways of conveying secret information—Symbolism of action—The spoken word imprisoned and dispatched—A matter not necessarily secret because one cannot understand it—Egyptian hieroglyphics—Chinese characters—Indian mutiny Greek—Ancient Biblical cryptogram—Sheshach of Jeremiah—Sir Henry Rawlinson thereon—Statements for and against—Julius Cæsar's secret code—The waxed tablet of Demaratus—Difference between hidden and secret writing—The shaven head a writing tablet—Charlemagne and Alfred the Great as cryptographic experts—Mediæval authorities—Trithemius the Benedictine—"Steganographia"—Dabbling in the black art—Dr. Dee—Batista Porta's book on "Natural Majick"—Invisible writing—Chemical methods by vitriol, alum, etc.—Writing on glass or crystal—Papal Inquisition—Disappearing writing—Messages wrapped round rollers—Two methods—A slave's back the writing surface—Chemical methods of no great value ordinarily—Disadvantages of use—Action of light and heat—Chloride of cobalt, sulphate of copper, etc.—Often impossible to procure the materials.

THE word Cryptography is derived from the two Greek words *kryptos* and *grapho*, the first signifying that which is concealed

or hidden, and the second meaning to write or describe, and it is in brief the conveying in a secret manner of any intelligence we may desire to communicate.

It may at once occur to our readers as an objection to the study of cryptography that it is an art that may palpably be very readily adapted to evil purpose, and that in doing anything to facilitate its study we are placing a weapon in the hands of the ill-disposed. This is an argument, however, that applies equally to many studies that nevertheless are of great value. Astronomy may in evil hands become astrology, and the glorious stars themselves mere counters for the fortune-teller; while from the researches of chemistry may be derived the valuable dye, the healing medicine, or other beneficent discovery, or it, equally readily, may be perverted to supply the arsenal of the *dynamitard* or the subtle potion of the secret poisoner. Moreover, even if we regard cryptography as affording means

for clandestine or treasonable communications, it is clearly a double-edged sword, and a knowledge of its principles and practice may at least equally well be used to unmask deceit and to unravel the tangled skein of the traitor.

It is sufficiently evident, on a moment's reflection, that this art of cryptography has a most legitimate use in the world. There are times of stress and danger in the history of a nation when it is absolutely impossible that vital operations in the field could be conducted to a successful issue if all the world at their inception had to be taken into confidence, and every step became at once a matter of common knowledge and discussion. In the same way the labours of the diplomatist could scarcely fructify to the national benefit or turn aside a national danger if every step had to be laid bare to the eye and the well-meant or acrimonious criticism of friend or foe, and become at once the property of every tattler who could

read a letter or any traitor who could copy a dispatch.

During the stormy closing years of the reign of Charles I., we find this art of secret writing assiduously cultivated both by Royalist and Parliamentarian, as the multitudinous records preserved in the British Museum and our other national archives abundantly testify. Previously to this, in the stirring times of Queen Elizabeth much use had been made of it, and during the troublous days of the French Revolution, when no man of any mark or influence was safe any hour from denunciation, we find an immense use of this cipher-writing, when treachery was at its deadly work, or when the love that was stronger than death sought to shield the victim from the impending blow, and give the warning that might yet secure safety by timely flight.

That which is secret and mysterious, calling for acute intelligence to penetrate its meaning, has always exercised a great fascination on

the human mind. Hence at one end of the scale we have the denunciations of the Hebrew prophets clothed in mystic language or figured in strange symbolic action,[1] and at the other the delight in puzzledom that finds its pabulum in missing-word competitions, conundrums, and such-like stimulants to the ingenuity of the reader. This love of the mysterious, this delight in setting one's wits to work to excel others or to save oneself from checkmate, is one great influence the more in the fascination that cipher-writing has undoubtedly at all times possessed.

Secrecy of communication may of course take many forms. The scarcely perceptible movement of the eye may convey a very definite warning, or the talking on the fingers,

[1] This symbolism has always exercised a very marked influence amongst Eastern peoples. Our readers will recall, as an example, the sending of a bird, mouse, frog, and arrow by the Scythians to the Persians, as a gentle hint to them that unless they could escape as a bird by flight, could swim as frogs, or conceal themselves as mice, they were hastening to swift destruction.

learnedly called dactylology or cheirology, may serve as a means of conveying a message. The significance of flowers may make a bouquet eloquent, or the gift of a ring may, in the initials of the stones that enrich it, spell out words of sympathy and tender feeling. The Romans had a code of communication based on touching various parts of the person; thus the finger to the forehead meant F, while the touching of the beard signified B. Watch-fires, waving torches, flashing mirrors, jangling bells, have all been utilized; but all these are mentioned but to dismiss them, since our present purpose is to deal only with such methods of communication as are possible by means of writing. Before, however, doing so we cannot forbear reference to a quaint suggestion that we encountered in an old authority on the subject, whereby the human voice was made the medium of transmission. The person desiring to send the message was gravely instructed to breathe his

words slowly and distinctly into a long tube that was carefully and securely closed at the other end. So soon as he had finished all he had to say, the end into which he had spoken was promptly fastened up, and the message was then dispatched to the receiver. This latter, on obtaining possession of the tube, was careful to open it at the end last sealed, as of course it was of great importance that the words should come out distinctly and in the order spoken. If by inadvertence the wrong end were opened, the operator was warned that the message would come out in inverted order. On thinking out this valuable idea we cannot help deciding that the directions given would lead to just the result deprecated. If we, for instance, plugged up the farther end of a railway tunnel, ran a train into it, and then fastened up the near end, we should, on presently re-opening this end, find that the train would come out backwards. However, this is a mere detail, and a very little

experience would soon decide which end of the tube it was best to open. Baron Munchausen seems to have quite accidentally hit upon another curious property of sound, when the melodies that he had apparently hopelessly in hard frost endeavoured to get out of his bugle flowed from it of themselves quite easily when the instrument was brought into a well-warmed room at his journey's end.

A matter is not necessarily secret, of course, just because we or some other people fail to understand it. This seems the barest of truisms when once stated, but it needs enunciation nevertheless. People, for instance, constantly speak of the Egyptian hieroglyphics, as Ben Jonson does on our title-page, as though they had some reserved and occult significance, whereas they were but the recognised symbols for conveying ideas, recording history, and so forth, of the whole educated caste of the nation. In the days not so very long ago when three-fourths of the people of England

could neither read nor write, the epistles that passed between the "quality," and written in legible enough characters for those who were sufficiently "scollerds" to read them, could scarcely be considered examples of cryptography. The queer characters on a Chinese tea-chest are to most of us Western people merely meaningless lines and dabs of colour, but the sole reason of their being put there was that they might convey a meaning. The Cantonese or Amoy man who painted them was adding information, and had no thought or intention of bewildering the outer barbarian whose Rugby, Harrow, or board-school training had in this matter failed him. The outward form of the communication has very little to do with it, but the intention has almost everything to do with it. If we, for instance, from a laudable desire to keep up our French, often talk it in the family circle, that is one thing; but if we drop into it because the servant is in the room, and it

is not quite convenient that the details of our approaching bankruptcy should also be discussed ten minutes afterwards in the kitchen, that is quite another. If an English officer at Aldershot chose to write out any little message to a brother officer in English words, but with Greek characters, he would be considered eccentric or silly; but such communications passed in hundreds between British officers during the Indian Mutiny. An intercepted message written in English could have been read easily enough in every camp of the mutineers, and they would thus have become possessed of valuable military information; but this cryptogamic use of the Greek letters rendered such communications entirely valueless to them.

It has been freely stated by divers authorities that the earliest examples of cipher-writing may be seen in the use of the word Sheshach by Jeremiah. He is the only writer who uses it, and while a Hebrew scholar

assures us that the term is meaningless in itself, it is undoubtedly made up by reversing the letters that spell the Hebrew word for Babylon. If a modern writer denouncing the wickedness of London thought it prudent to refer to it as Nodnol, those who detected the transposition of the letters would have no doubt of the meaning. Yet one cannot help feeling a little hesitation in accepting the Sheshach as an archaic cryptogram. One authority we questioned said that there might have been a good reason for disguising the name; but on going to the fountain-head and reading the verse itself that the prophet wrote over six hundred years before the Christian era, we find, "How is Sheshach taken! and how is the praise of the whole earth surprised! How is Babylon become an astonishment among the nations!" There seems but little reason for any concealment in the first half of the verse when the second half effectually lays all open. Sir Henry Rawlinson, no mean

authority, does not feel the accepted explanation so entirely satisfactory as to render any other superfluous. He states that Ur, the city of Abraham, "might have been read in one of the ancient dialects of Babylon as Shishaki," and if this be so the transposition of letters becomes merely a remarkable coincidence. Sheshach then stands for Ur, the ancient capital, and Babel or Babylon for the then modern one, and the prophet may thus be taken as referring to the whole national life from its birth in lowly Ur of the Chaldees to the day when he wrote of the great city of Babylon his words of warning and reproof; but here again on going to the fountain head, we find the whole reference to be in the present tense. Rawlinson, too, only tells of what "might have been," and we certainly seem to need a firmer foundation than this possibility. The two alternatives before us are equally perplexing. Would any writer be so cautious and reticent one moment,

so plainly outspoken the next, if his object all through was prudent suppression of a name? On the other hand, if the two names refer to two entirely different places—as, for example, Winchester and London—is it not a most extraordinary coincidence that the letters in the name of each city are precisely the same, and that while the one has them in one order, the other has them exactly reversed? What proportion, according to the law of chances, of millions to one would be necessary to express the likelihood of such a transposition occurring? It was absolutely necessary to refer to this Sheshach question, since, as we have stated, this passage in the Bible is claimed by some enthusiastic cryptologists and commentators as the earliest example of a cipher, and now, perforce, we can but leave it to the reader to derive such benefit and comfort from the matter as he may.

This simple reversal of the alphabet, A

representing Z, B being the equivalent of Y, etc., is far too evident to have any cryptogrammic value, as the changed value of the letters is very quickly perceived. The historian Suetonius tells us that Julius Cæsar, in forwarding his dispatches, changed the positions of the letters by four places, making D stand for A, P for M, and so on; but this, though a trifle better, was still the most elementary work. Scaliger, we see, in referring to it, styles it a "pure absurdity"; yet one repeatedly finds in the "agony column" communications based on this or some equally simple shifting on of the letters.

Polybius tells us that Æneas Tacitus had collected together twenty different kinds of secret writing, some of them having been in use before his time, while others he devised himself. Herodotus mentions that one Demaratus, a commander of the forces, wrote his communications on wooden tablets, and then had them smoothly coated over

with wax, as though they were merely blank surfaces for the stylus. Those who received them, and who were in the secret, removed this upper coating, and the message stood revealed. But this, it will be noted, was scarcely secret writing, any more than a letter fastened down in an envelope to-day becomes secret writing by the process. It is but hidden writing, and when the wax of the tablet or the covering surface of the envelope are removed the writing has lost all its secrecy. Most of the ancient methods of secret communication were of this nature. One plan gravely commended was to shave a slave's head, and then to write upon it any message one might wish to send. When the hair was sufficiently grown to conceal the matter, the man was dispatched to the person with whom it was desired to communicate, and he in turn shaved the victim and read off the message. In these days when fifty miles an hour is considered far too slow for business,

and when we read at breakfast in our newspaper the details of the insurrection that broke out yesterday in Central Africa, such a method of communication would be voted altogether too dilatory, and we cannot help feeling—such is the force of nineteenth-century habit—that even in those good old times, when nobody seemed to be at all in a hurry, the message that could afford to wait while a new crop of hair was growing could not have been of any great urgency, or they would surely have found a less leisurely way of dispatching it.

Charlemagne kept up a private correspondence in cipher-writing, and the secret alphabet used by Alfred the Great may still be seen in the Bodleian Library. We also, during the fifth century, find Pharamond and other reigning princes utilising various more or less satisfactory systems of cryptography, but in those early days those who could either write or read with any ease were but few in

number. When we come to the Middle Ages a perfect epidemic ran round Europe, and cryptographia, or, as it was sometimes termed, polygraphia or steganographia, had its enthusiastic votaries in every land. Those who care for the archæological side of the subject may refer to the writings of Palatino, dating 1540, of Bellaso in 1553, and of Glanburg in 1560. Should this not have damped their ardour, they may next take a course of Porta, Trithemius, Cardanus, Walchius, Bibliander, Schottus, Selenus, Herman Hugo, Niceron, Caspi, Tridenci, Comiers, La Fin, Dalgarno, Buxtorff, Wolfgang, and Falconer. Even then, if they so wish it, are open to them the writings of Eidel, Soro, Amman, Breitkampt, Conradus, De Vaines, Lucatello, Kircher, and not a few others; while for those who do not care to dig their knowledge out of such dusty worm-eaten tomes William Blair is the very thing, though we would fain hope that ere we, and they, reach the last of these present

pages they will feel that they have derived thence as much enlightenment as they need.

As many of these mediæval authors had a great knack of conveying, with scant or no acknowledgment, the labour of others into their own store, there would be little profit in referring at any length to their works; we will therefore select but two, Trithemius and Porta, for any comment.

Trithemius, the first in time of these two old writers, was an able Benedictine. He was Abbot of Spanheim, and his was the first really elaborate treatise on cryptogrammic writing. The first printed edition was published in Frankfort in the year 1606, and a copy of this is preserved in the Bodleian Library; a second edition was issued from the same press two years later. Its title is of the elaborate character that is characteristic of books of that period. "*Steganographia: hoc est ars per occvltam Scriptvram animi svi voluntatem absentibvs aperiendi certa: avthore*

reverendissimo et clarissimo viro Joanne Trithemio, Abbate Spanheimensi et Magiæ Naturalis Magistro perfectissimo." His method was a somewhat curious one, as he compiled many folios full of devout sentences through the use of which quite other and mundane matters could be conveyed. The result was a vast mass of misdirected energy. Unfortunately, to these he added a number of extraordinary characters, which he designated spiritus diurni and spiritus nocturni, the result being that he was accused of dabbling in the black art and holding converse with demons. He was therefore brought to trial for these magical incantations, and had a very narrow escape of being burnt. He had also the misfortune to incur the lavish abuse of Jerome Cardan, himself the author of a system of cryptography, and was by him relentlessly attacked and hounded down.

Dr. Dee, who was himself under the ban as a follower of divers uncanny arts that were

supposed to bring him into closer relation with demons than was held to be at all justifiable, was a great admirer of the work of Trithemius. He was often sent abroad on more or less secret service by the Ministers of Queen Elizabeth, and we find him writing from Antwerp on February 16, 1563, to Sir William Cecil for permission to extend his stay in that city. He was mainly desirous of doing so, as he was arranging for the publication at Antwerp of a book of his own, the *Monas Hieroglyphica*, issued in the following year; but as his private affairs were scarcely a sufficiently good reason why he should be maintained there at the expense of the State, he adds that he is there able to gather much together that would be of gain to the nation.[1] Amongst other reasons for staying on, he writes: "Allready I have purchased one boke, for wch a Thowsand Crownes have

[1] In reference to this appeal of Dr. Dee, Cecil's memorandum is extant stating that the applicant's time beyond the sea had been well spent.

been by others offred and yet could not be obteyned. A boke for which many a lerned man hath long sowght and dayley yet doth seeke: Whose use is greater than the fame therof is spred: The name therof to you is not unknowne: The title is on this Wise— Steganographia Joannis Tritemij: wherof in both the editions of his Polygraphia mention is made, and in his epistles, and in sundry other mens bokes: A boke for your honor, or a Prince, so meet, so needfull and commodious, as in humayne knowledge none can be meeter or more behopefull. Of this boke the one half, with contynuall Labor and watch the most part of X dayes have I copyed oute: And now I stand at the Courtesye of a nobleman of Hungarie for writing furth the rest: who hath promised me leave therto after he shall perceyve that I may remayne by him longer (with the leave of my prince) to pleasure him also with such points of Science as at my hands he requireth. Thys boke,

eyther as I now have yt, or hereafter shall have yt, fully whole and p'fit (yf it pleas you to accept my present) I give unto your honor as the most precyous juell that I have yet of other mens travailes recovered."

The account is not quite a clear one, as he declares that he has bought the book, though he does not say that he himself gave a thousand crowns for it, and yet he appears to have copied it by the courtesy of the nobleman possessing it, and who certainly does not seem to have sold it to him. From the price Dee puts on the book, it is evident that it was a manuscript copy. The book was long kept from the knowledge of the general public, the first printed copy not being issued until forty-three years after this letter of Dee to Cecil. The direct gift to Cecil we may perhaps, without being wanting in charity, regard as a gentle bribe to be allowed to stay on at Antwerp for the advancement of his private business ends.

Batista Porta, a Neapolitan writer, compiled five books on ciphers, "*Les Notes occultes des lettres*," that were published in Strasbourg in the year 1606, and he also devotes one of the "Bookes" of his "Natural Majick" to the art of invisible writing. The edition before us as we write is dated 1658, the title page stating that the book was "printed by Thomas Young and Samuel Speed, and are to be sold at the Three Pigeons, and at the Angel in St. Paul's Churchyard." In this volume, divided into twenty sections, or books as he calls them, are "set forth all the Riches and Delights of the Natural Sciences," and the result is a strange medley indeed. His first book deals with "the Causes of Wonderful things," a sufficiently extensive subject in itself and including "the Nature of Magick," the influence of the stars, and so forth. Other sections deal with the transmutation of metals, the wonders of the load-stone, the beauti-

fying of women, etc., and the sixteenth concerns itself with "invisible writing." His last book is "of the Chaos," and here we find a promiscuous mass of matter that either would not fit in happily in any of the other books, or which he happened to have overlooked, or upon which he had gained fuller information than when dealt with in its original position. This chaotic section includes such diverse matters as how to make foul water drinkable, and how to distil it from the air, the art of altering one's face so that one's friends are deceived, how to make stones grow of themselves, how to make an instrument whereby we may hear sounds at a great distance, how to detect frauds in impostors, and much else of more or less chaotic interest and value.

The sixteenth book, "wherein are handled secrets and undiscovered notes," commences with the statement that "there are two sorts of secret marks, which they vulgarly call

syfers: one of visible marks, and is worthy of a treatise by itself; another of secret marks, whereof I have attempted to say something in this present Volume, and what are the consequents thereof, for the use of great Men and Princes, that take care for things absent, and write to some man that knows the invention. I shall set down some examples plainly: but these things and the consequences of them must be faithfully concealed, lest by growing common amongst ordinary people they be disrespected." Our old author here clearly felt the difficulty of the position he had got himself into; on the one hand thinking to impart much curious and useful knowledge, and on the other hand in the act of doing so feeling its publication a contradiction vitiating all his labour. Even Natural Magick fails to show how the frank exposition and the careful concealment of secret matters can be simultaneously accomplished. This doubtless, too, was one potent reason why the folios of Tri-

themius remained in manuscript some fifty years.

Porta's division of his subject into visible and secret marks looks at first sight a little puzzling, for unless visible marks carry a secret significance they are in this connexion valueless. We soon find, however, on reading his book, that what he means by visible marks is the use of letters, figures, or other signs that are evident enough to all beholders though their significance is unknown, and these, as he says, are worthy of a treatise to themselves. In the present work he deals almost entirely with communications that are secret through their invisibility, until some chemical application, the action of heat or of light, or other external cause, bring them to view. He, in fact, begins his first chapter with the words: "There are many and almost infinite ways to write things of necessity, that the Characters shall not be seen, unless you dip them into waters, or put them near the

fire, or rub them with dust, or smeer them over."

His first recipe is a double-barrelled one. It is to be employed "if you desire that letters not seen may be read, or such as are seen may be hid." This is a very artful state of things to bring about. The enemy or other unauthorized person into whose hands the paper fell would be put off the scent by reading a communication that was of no value or significance to them, while the person to whom it was really sent would take steps first to remove the visible writing, and then to make a second communication, written between the lines of the first, tell out its story by the application of a second preparation. The procedure is as follows: "Let Vitriol soak in Boyling water: when it is dissolved, strain it so long till the water grow clear: with that liquor write upon paper: when they are dry they are not seen. Moreover, grinde burnt straw with Vinegar: and what you will write

in the spaces between the former lines, describe at large. Then boyl sowre Galls in white Wine, wet a spunge in the liquor: and when you have need, wipe it upon the paper gently, and wet the letters so long until the native black colour disappear, but the former colour, that was not seen, may be made apparent. Now I will show in what liquors paper must be soaked to make letters to be seen. As I said, Dissolve Vitriol in water: then powder Galls finely, and soak them in water: let them stay there twenty-four hours: filtre them through a linen cloth, or something else, that may make the water clear, and make letters upon the paper that you desire to have concealed: send it to your Friend absent: when you would have them appear, dip them in the first liquor, and the letters will presently be seen." The materials, it may be noted, are fairly readily procurable: an important point to consider.

Porta also suggests that we may dissolve

alum in water and write with it upon linen and the like, declaring that when this writing is dry it will be invisible. When you would render it visible, it will suffice to soak the sheet or napkin in water. The fabric will appear darker where it has not been touched by the alum solution, so that the message will appear in letters of white. After divers other prescriptions, in which litharge, citron-juice, goat's fat, juniper, and various other ingredients figure, he winds up his first section, "On how a writing dip'd in divers Liquors may be read," by the assertion, "there are many such arts, too tedious to relate," and he then proceeds to his next section, how letters may be made visible by the action of heat.

"If you write," he tells us, "with the juice of Citrons, Oranges, Onyons, or almost any sharp things, if you make it hot at the fire, their acrimony is presently discovered: for they are undigested juices, whereas they are detected by the heat of the fire, and then they

show forth those colours that they would show if they were ripe. If you write with a sowre Grape that would be black, or with Cervices:[1] when you hold them to the fire they are concocted, and will give the same colour they would in due time give upon the tree, when they were ripe. Juice of Cherries, added to Calamus, will make a green: to sowbread a red: so divers juices of Fruits will show divers colours by the fire. By these means Maids sending and receiving love-letters, escape from those that have charge of them. There is also a kind of Salt called Ammoniac: this powdred and mingled with water, will write white letters, and can hardly be distinguished from the paper, but hold them to the fire, and they will shew black."

Porta has also a suggestion for making communications that cannot be read until

[1] The fruits of the Service-tree, *Pyrus torminalis*, of a greenish-brown colour, and of rough acid flavour until they are mellowed by frost.

the paper be burnt upon which they are made. He arrives at this in the following fashion: "Take the sharpest Vinegar and the white of an Egg: in these steep Quick-silver and stir it well: and with that mixture make Letters upon the paper: burn the paper in the fire, and the letters will remain unburnt." The result of this will be that the paper will be black and the letters white. This sounds better in theory than it would probably work out in practice. We are all familiar with the fact that even when a letter written in ordinary ink is burnt, we may often still be able to read on its charred surface portions of the writing, but we know also that the act of burning twists and curls the paper up so that much of the writing is out of our sight, while the whole thing is so brittle that a touch may break it up, and any attempt at straightening out the sheet would be wholly futile.

Porta has various ideas as to developing invisible writing by means of dust or soot; by

writing with vinegar, gum solution, the milk of the fig tree and various other ingredients, and then rendering the message visible by rubbing these substances upon it. The milk of the fig tree was not readily accessible as we were writing these lines, so of its efficacy we can say nothing, but a letter which we forthwith proceeded to write with vinegar at once became clearly legible when soot was rubbed gently over its surface. Our author tells us that "there is also an Art that one would not imagine to write upon Chrystal; for being all transparent no man will dream of it, and the letters may lie hid therein. Do it thus. Dissolve Gum Arabick in water, or Gum Tragacanth, that it may be cleer; and when it is well dissolved, it will not foul the Chrystal if you write upon it or upon a Cup or Glass, for when the letters are dry they are invisible. No man will imagine it, if a cup be sent to one in prison, or a Glass full of wine: when he would see the letters, rub burnt straw or paper upon it, and the letters

will presently be seen." This also we brought to the test of experiment, writing upon a glass bottle with a solution of gum-arabic. The writing when dry was absolutely invisible. On rubbing burnt paper over the writing we were unable to get any satisfactory result, but on wiping this off and using soot instead we at once got the wording very sharply defined in black on the transparent glass, the experiment being entirely successful. At the same time there seem to be practical difficulties; one can hardly imagine a prisoner saying, "Would you kindly oblige me with a pinch of soot or a handful of straw and a match?" At all events we can hardly imagine his getting them.

A curious side-light and reference to "the good old days" is shown again in Porta's instructions as to how secret messages may be sent by means of eggs, for he tells us that "Eggs are not stopt by the Papal Inquisition, and no fraud is suspected to be in them."

Hence prisoners might perchance receive eggs from their friends, and with them messages from the outside world. However this may be, it is at least a pleasant picture. One has always so imagined the victims of the Inquisition going melancholy mad in dripping dungeons, or shrieking at each turn of the rack and thumb-screw, that the idea of the man sitting down in peace to his lunch, and having a new-laid egg with it, comes as quite a welcome surprise.

Porta is also great on the subject of devising means whereby written characters, freely legible at first, might presently disappear; but one can scarcely imagine such a thing as being of any great value. It might at times be an advantage if promises made on the eve of an election, the former sentiments of recreant and turncoat politicians, or the fervent protestations of the lover lavishly poured out ere the breach of promise action had even been deemed a possibility, could somehow be forgotten; and

there might of course be occasions when some damning document might be laid up in the archives of the enemy for use at some critical moment, and when its production after all as a blank sheet of paper might well be the difference between a traitor's death and safe deliverance from the noose, the firing party at ten paces, or the convict hulk. Ordinarily, however, when one has mastered the meaning of a communication, there are many safer and more expeditious ways of disposing of it than trusting to the corroding or paling action of any chemical to obliterate its secrets. In the seclusion of the diplomatist's study the glowing hearth, or in the bustle of the bivouac the roaring camp fire, will expeditiously enough reduce to ashes any paper that has fulfilled its purpose.

In like spirit of adverse criticism we would deal with the reverse of this, "that invisible letters after some time shall become visible and show themselves." We are told that "if one

write with juice of Citrons or Oranges on Copper or Brass, and leave this on for twenty days the letters will appear green upon the place; the same may be done many other ways, namely, by dissolving Salt Ammoniac in water, and writing with it upon Brass, the place will sooner appear of verdigreese colour." It is sufficiently evident that it is rarely indeed that a delay of twenty or any other number of days is a desideratum. One ordinarily desires to

Fig. 1.

know at once any communication that any one sees fit to make to us, and should especially desire to do so if we knew that the secrecy and mystery attaching to it was an indication of its grave importance.

The two or three examples that Porta gives "of letters on divers things which, though

they be visible yet the Reader will be deceived by their secret device," are of no great value. One of his hints is to write on parchment, and then put it to the fire or candle, when it will crumple up and in the contorted state of the parchment the written matter will be so twisted about that it will be unreadable. The harshness of the fire-tried material upon which it is inscribed will resist any attempt at forcible flattening out, so that even if we detect the presence of a communication it is not get-at-able. But "if one desires to read what is in it let him lay it on moyst places or sprinkle it gently with water, and it will be dilated again and all the wrinkles will be gone, and it will appear as it did at first, that you may read the letters upon it without any hindrance."

Porta also refers to the ancient expedient, ascribed to Archimedes and mentioned by Plutarch and other ancient authors, of writing on a strip of paper wrapped round a stick. Two sticks of equal diameters must be sup-

plied, one being held by the one correspondent and the second by the other. A long thin strip of paper must now be wrapped spirally

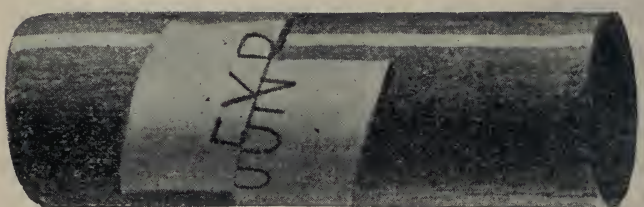


Fig. 2.

round one of these cylinders so that the edges are just in contact throughout its length, and on these edges, so that a portion of each letter

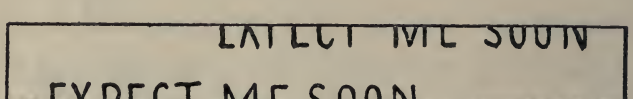


Fig. 3.

comes on each side, the required communication is written. The paper is then unrolled and forwarded to the holder of the second stick, and he, on rolling the strip around this,

is able to read the message with great facility. The theory is that no one would take any notice of these marks on the edges of the paper, but on putting the matter to the test of experiment we found no difficulty, without any wrapping round stick or ruler, in reading the message that we had previously written. Half of each letter is seen, and that is quite sufficient to serve as a clue. If any of our readers like to test this statement for themselves, they will readily find that if they place a piece of blank paper along any of the lines of

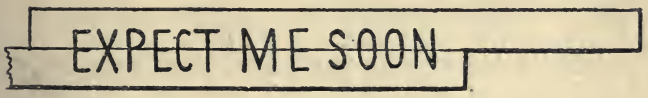


FIG. 4.

this printed page so that half of each letter is hidden the remaining half quite suffices for its identification.

The message we wrote was, "Expect me soon." Fig. 1 shows the spirally wrapped

strip of paper and the message written on its edges. Fig. 3 represents the strip when unrolled from the pencil and flattened out ready for dispatch; while Fig. 2 shows how the message would look if the receiver, not knowing that a pencil had to be employed, tried wrapping it round a ruler. Fig. 3 has a

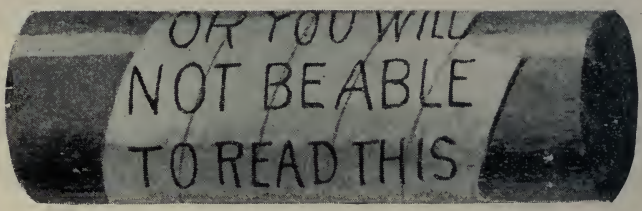


Fig. 5.

decidedly tell-tale appearance, anyway; but if any unauthorized person into whose hands this strip came would just take the trouble to divide it in half lengthwise, and place, as in Fig. 4, the two lettered edges together, the message is at once as legible as any orthodox rewinding round a pencil could make it.

A very much better way of working this spiral paper method is to write the message, not along the edges, but right across the strips themselves. Having wound our strip of paper round our ruler, we wrote as follows upon it: "Get another roller the same size, or you will not be able to read this communication." The appearance of our message-bearing staff may be seen in Fig. 5, while Fig. 6 shows a portion of the strip as it looked when unwound and ready for sending off to our correspondent. It will at once be seen how far more puzzling this is than the strip shown in Fig. 3.

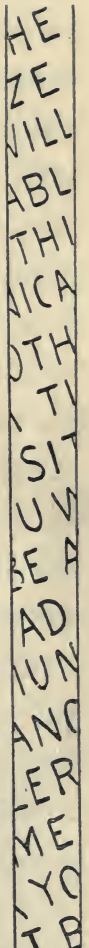


FIG. 6.

Some of the material we find in Porta's chapters can scarcely be considered to come within the category of "invisible writing" at all, since the methods he adopts are akin to

the ordinary letter put in an envelope that we have already cited. He tells, for instance, how a communication was once sent within a loaf, and in another case in the interior of a dead hare; how others, again, have safely brought letters concealed in their girdles, beneath the soles of their feet, or in their scabbards or quivers; how pigeons may be used as messengers,[1] or intelligence shot into camp or fortress by arrows or guns. He quotes numerous instances of this sort of thing from ancient writers; from Theophrastus, Africanus, Herodotus, Ovid, Cæsar, Pliny, and others.

He does not forget to refer to the slave with shaven head, but he also recognises that it may oftentimes be desirable that an underling conveying a message should be in ignorance of the fact that he is being thus

[1] A great use was made of pigeons as messengers during the Franco-German war, and the pigeon-loft of to-day is as much an item of war strength as a Maxim gun.

employed. Had he this knowledge, he might possibly desert to the enemy, or be filled with such exaltation of spirit at the importance of his mission as to betray himself and awaken suspicion. If he fell into the hands of the enemy, he might be tempted by fair promises, or affrighted by threats, to reveal his mission; whereas, if he were unconscious of it, his whole manner would be so frankly guileless as to avert suspicion, and he would much more probably pass on his way unchallenged. He was, therefore, given no letter to conceal; nothing was handed to him to excite his interest or awaken his suspicions; but his food was drugged, and, while he was under the influence of an opiate, his own broad back was the surface utilised as the sheet whereon to inscribe the message required to be transmitted. This method is referred to by Porta, but it dates back far into ancient history,—Ovid, for instance, alluding to it.

Speaking in a general way, but at the same time as the outcome of considerable experiment, we should be inclined to say that the various compounds suggested by Porta and many other writers as inks, invisible until developed by the action of light, or of heat, or the washing over of another solution, are of no great practical value; while the materials, though in most cases common enough, may not always be forthcoming. The commander of an advanced post in a hostile land, who was desirous of communicating with the base of operations, or with the leader of a relief party, might be a thousand miles from the nearest place where chloride of cobalt, for example, was procurable.

A great practical disadvantage in the use of such materials is that, as they flow from the pen as clear and colourless as pure water, it is very difficult to see what one is writing; and so soon as the writing dries, as it very

quickly does, any chance of correction or reconsideration is gone, and one can only trust to memory as to what was really put down at all. Such a message, too, on its receipt, might easily be mislaid or torn up as a piece of valueless paper; while, on the other hand, any special solicitude for its preservation would at once excite comment and suspicion. Any person who entertained such suspicion would probably be well aware that heat was one of the most effectual means of rendering a secret message visible, and on its application the message would stand forth revealed to quite other eyes than those for whom it was intended.

Some few of these simple preparations we may refer to; as those who are curious in such matters might, when once put on the track, very naturally desire to test them for themselves. Any one so doing should be careful to use a clean quill pen; and as some, at least, of the materials are poisonous,

some little discretion. Any one, for instance, who leaves a clear, colourless solution in a teacup or tumbler for an hour or two in kitchen or dining-room may very possibly be called upon by the coroner to explain; while attendance at the funeral would be another grievous break in the time devoted to this interesting study.

As a familiar example of the chemicals affected by light we may mention nitrate of silver. Any communication made by a solution of this would remain invisible until such time as exposed to daylight. On this exposure, the writing would reveal itself in dark chocolate-brown, and, once made visible, remains so. The writing should, of course, be done by artificial light; and we have found that a proportion of one of nitrate to fifteen of distilled water makes about the most satisfactory mixture. If, instead of placing the paper in the daylight we hold it over a vessel containing sulphate of ammonia the

writing will appear with a metallic and silvery brilliancy.

If we make a solution of chloride of cobalt, it will be of a pale pink in tint; but the colour is so slight that in writing with the fluid it appears colourless on the paper, and there is absolutely no trace of anything to be seen. On warming the paper before a good strong fire the characters appear of a clear bluish-green; but they disappear again as the paper cools, a matter of some five minutes or so. The effect can, of course, be reproduced as often as we choose to apply the necessary heat. If we use acetate of cobalt instead, the warming of the paper brings out the communication in a clear and beautiful blue colour.

Equal parts of sulphate of copper and sal-ammoniac dissolved in water give a solution of a beautiful turquoise-blue tint. This, if applied at all strongly, dries on the paper of a pale greenish colour, a tint too weak

to be legible, though not too weak to be noticeable on a scrutiny. On warming the paper on which any communication has been made by this agency the writing appears of a clear yellow, but on the cooling of the paper it disappears. The juice from an onion that has been macerated in a mortar will also produce the same effect, the characters written by means of it being at first invisible, but afterwards clearly legible and of a yellow colour.

If we wish to have a message that will remain indelible when once developed, we have the materials ready to hand by dissolving oil of vitriol in soft water in the proportion of a fluid ounce of the former to a pint of the latter. Strong chemical action is set up, and great heat evolved. The solution should be well stirred, and then allowed to cool, and it is then ready for use. Anything written by this agency is in theory supposed to be quite invisible until warming at the fire brings

it out a clear black, but in practice we found, with solutions of varying strengths, that the writing, though at first invisible, became on drying quite perceptible, and looking as though written with whitewash or Chinese white on the paper. On a very cursory examination it might escape notice, but the slightest scrutiny reveals it. The difficulty is that if we use a strong solution the writing can be read in the white characters, though it, on the application of heat, develops into a clear and excellently legible black; while if we use a solution so weak as to escape notice when applied to the paper, it also develops a very weak colour on the application of warmth. The proportions we have given are perhaps the best, but the result in any case is hardly satisfactory if absolute invisibility is our object, and of course nothing short of this is worth anything.

Many other chemical methods might be mentioned, but their value after all does not

appear to be very great. Nothing but personal investigation is of any real use. One finds over and over again things commended by various writers that entirely break down when brought to the vital test of actual experiment.

CHAPTER II

Ancient use of arbitrary symbols—Tyronian abbreviations—Early works on shorthand—Excessive abbreviation of inscriptions on coins, etc.—Telegram-English—Mason-marks—Rise of cipher-writing in England—Clarendon's "History of the Rebellion"—Battle of Naseby—Royal correspondence captured and deciphered—Published by Parliament—Weighted naval signal-codes—Charles I. a great expert in cryptography—Use of nulles or non-significants—Numerical ciphers—Mediæval inscription without vowels—Ciphers of Queen Henrietta and Sir Ralph Verney—Great use of cipher at troublous periods of history—The "Century of Inventions" of the Marquis of Worcester—Birth of the steam-engine—Dedication of his labours to the nation—His numerous suggestions for cryptograms—The "disk" cryptogram—Principle modified to sliding strip—Bead alphabet—Heraldic representation of colours in black and white—The "string" cipher—Bacon a cryptographic enthusiast—His essentials of a good cipher——His highest perfection of a cipher—His plan cumbrous and unsatisfactory—A Trithemian example—Elizabethan arbitrary mark ciphers—No real mystery in them.

A METHOD adopted by the ancient writers of representing words by arbitrary marks was said to have been first introduced by the

old poet Ennius. Mæcenas, Cicero, Seneca the elder, Philargirus, Tyro, and many other writers commended and employed these marks. By the time of Seneca thirteen thousand of these characters were in use. They are ordinarily termed Tyronian. Thousands of these Tyronian abbreviations and symbols may be seen in the writings of Valerius Probus, Paulus Diaconus, Goltzius, and other authors. So completely during the Middle Ages did they answer the purpose of secret writing that an old copy of a psalter found inscribed in these characters was ignorantly entitled, "*Psalterium in Lingua Armenica*"; and Pope Julius the Second employed several learned men without success to decipher it. This was originally but a system of shorthand, and it only grew into a mystery when the key that unlocked it was lost.

The "*Ars Scribendi characteris*," written about the year 1412, is the oldest system of shorthand extant, while the first English

book on the subject did not appear until 1588. It was written by one Timothy Bright, and entitled "Characterie, or the Art of Short, Swift, and Secret Writing." The notion of cryptography is present in this title. If a man employs a system of abbreviated writing because it is short or swift, it is to him but a matter of convenience and a gain of time; but if he adopts it because it is secret, an entirely different motive comes in. A man who writes in Pitman or any other widely-known system of shorthand, or who adopts any of the modern telegraph code-books that compress a long sentence into a single arbitrary word, is no disciple of cryptography therein; but if he, like Pepys in his famous diary, adopts a secret code because on the whole he prefers to keep his affairs private, his shorthand stands on quite a different footing to that of the first man. Such codes have their dangers. Not only is one exposed, like Pepys, to the risk of having all one's

matters laid bare, but there is also the probability of such a fiasco as occurred within our own knowledge, where a man kept his business and family memoranda by a shorthand system that he himself devised, the result being that at his death his affairs got at once into a state of utter confusion that they never rallied from, and there can be but little doubt that much property was lost to the family from want of all clue to it.

An ancient form of writing employed amongst the Romans was the excessive abbreviation of words in inscriptions on statues, coins, and so forth; but this was not for secrecy. Any one caring for examples of the sort of thing will find abundant illustrations in such old tomes as the "*Lexicon Diplomaticum*" of Walther or the "*Siglarium Romanum*" of Gerrard. In fact, the D.G. and Fid. Def. on our present money supplies us with a good example of the curtailment necessary where one desires to get a good deal of

material in a very circumscribed space. A still better example may be seen in the coinage of George III., where we may find such concentrated information as the following: M · B · F · ET · H · REX · F · D · B · ET · L · D · S · R · I · A · T · ET · E ·. This suggests a sort of mince or hash of the alphabet, but with due amplification and clothing of these bare letters, we arrive at last at "*Magnæ Britanniæ, Franciæ et Hiberniæ Rex, Fidei Defensor, Brunnovici et Lunebergi Dux, Sacri Romani Imperii Archithesaurarius et Elector.*"

We may say parenthetically that in all cryptogrammic communications the message or other matter should be abbreviated as far as is consistent with intelligibility. One should cultivate for this purpose the style of telegram-English. It makes less labour and less chance of error creeping in for the sender, less time in unravelling for the receiver, and less handle for any unauthorized reader to lay hold of. This last, as we shall

see when we come presently to consider the decipherment of a mysterious message, is a point of very considerable importance.

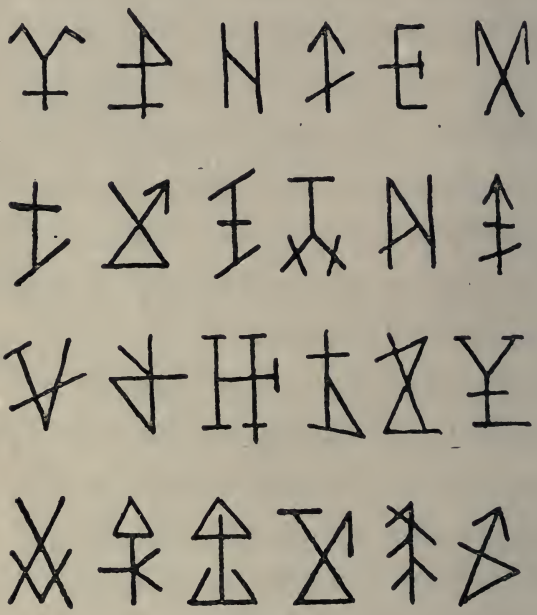


Fig. 7.

On old buildings we may sometimes see what are called mason-marks cut upon the stones. It has been suggested that these had originally a symbolic meaning known

only to those initiated in the ancient craft of freemasonry. Some authorities tell us that they are almost as old as the human race, that they probably had in early times a meaning that is now lost, that they were long regarded with a certain reverence, and that an essential rule for their formation was that they should contain at least one angle. We have reprinted in Fig. 7 divers examples of these marks from various ancient buildings. There is no doubt that all of them contain at least one angle! The more prosaic explanation of these marks is that they served to denote the work of each mason employed on any important building, that if the payment was by piecework such marking prevented dispute, and that if the work were badly done or any error made it was at once seen where blame should be imputed. Each mason had his distinctive mark, and many ancient registers of these are extant. The enthusiasts who see in these marks some mystic cult claim

as one proof that they may be found even on the blocks of stone that complete the Pyramids; but the more prosaic student might point out that this after all only indicates very ancient usage, and that it was as necessary in the time of Chofo to detect careless workmanship as when Salisbury or Amiens cathedrals were being erected. Whatever may be the exact truth, we are, we think, at all events justified in giving them a paragraph and an illustration in the space at our disposal.

Cipher-writing scarcely makes any real appearance in English archives until the reign of Queen Elizabeth. There had been divers isolated examples, as, for instance, as far back as Alfred the Great; but it was scarcely until the days of the Tudors that we find it really in vogue. Many examples of this period are preserved in the British Museum, and in the troublous days of the first Charles we find an immense use of it.

Amidst the historical documents preserved in the House of Lords, and brought to light by the Royal Commission on historical MSS., is the correspondence of King Charles captured by the Roundheads at Naseby—a correspondence which Dr. John Wallis, a distinguished mathematician of those days, analysed and finally deciphered, and which ultimately cost the defeated monarch his head.

In Lord Clarendon's "History of the Rebellion" (Book IX. vol. ii. p. 508) we read: "In the end the King was compelled to quit the field, and to leave Fairfax master of all his foot, cannons, and baggage, amongst which was his own cabinet, where his most secret letters were,[1] and letters between the Queen

[1] One scarcely sees how, in the turmoil of battle and the sudden realization of defeat, an incident so untoward could well be prevented. On board a man-of-war the code of signals is always kept in a leaden case, perforated with holes, so that when surrender is imperative the whole thing is dropped overboard, that it may not fall into the hands of the enemy. Even this, however, owing to the death of the responsible officer, or other cause (for in the

and him, of which they shortly after made that barbarous use as was agreable to their natures, and published them in print: that is, so much of them as they thought would asperse either of their Majesties, and improve the prejudice they had raised up against them; and concealed other parts that would have vindicated them from many particulars with which they had aspersed them." The battle of Naseby occurred on Saturday, June 14th, 1645. On June 23rd the House of Commons resolved "that the several letters and papers taken at Naseby Field should be referred to the Committee, to translate the French letters, decipher those that are not deciphered, and to sort them." It was also resolved that these letters and papers should be communicated to the Committee of both Kingdoms, "to the

heat of action a man may lose his head, though to outward appearance without a scar), is not always an efficient safeguard. Within a mile of Charing Cross, in the Royal United Service Museum, may be seen the weighted signal code of the United States ship *Chesapeake*, captured on board that vessel by the British ship *Shannon*.

intent that they may take copies to transmit into Scotland and to foreign parts, and that the said letters and papers shall be put in a safe and public hand and place, to the end that such as desire it may peruse the originals." Some sixty letters were captured. Many on receipt had been already deciphered by the King or Queen, and the translation appended to them for greater ease of reading.

Charles I. during the course of the war composed a great many ciphers, and some of them of very abstruse character. His celebrated letter to the Earl of Glamorgan, in which some very suspicious concessions to the Catholic party in Ireland were mooted, was composed entirely of short strokes in different directions; but his favourite idea was the use of numbers, and the Naseby letters were of this latter type. A good many "dummy" numbers are introduced, in addition to those that stand for letters or words. Such dummies are of course intended to throw those

who are unauthorized to read the letters off the scent, and some such arrangement is very common as a cryptographic expedient. They are known as nulles or non-significants also, and we shall come across numerous examples of their use ere our book is finished. Various people are also numbered, and the names of places that are likely to frequently recur. This is clearly a great saving of time, as instead of having to spell out Prince Rupert or Oxford in full a couple of numbers will at once express all we want, and of course the same principle is applied to such constantly wanted words as artillery, regiment, provisions, and the like. Where words are of more immaterial and non-betrayal character, they are often written in full; thus, for instance, we find the Queen writing to the King as follows: "Mr. Capell *nous a fait voir que cy* 27 · 23 · 52 · 62 · 28 · 45 · 9 · 66 · 4 · 48 · 31 · 10 · 50 · 35 · 33 · 47 · 31 · 8 · 50 *que ce* 34 · 8 · 27 · 28 · 23 · 17 · 16 · 3 *est tout* 33 · 8 · 50

·5·62 *cest pour quoy si* 66·4·46·189·18·69·2·70 *intantion de donner* 62·40·11·."

In one letter of the sorely troubled Queen she writes that matters have so harassed her, "*que je suis extremement tourmantee du mal de teete qui fait que je mesteray en syfre par un autre qui jovois fait moy mesme.*"[1] The trusted new hand then comes and finishes the letter in English. We give the commencement, and place over the symbols their significance: "Theer beeing hear

s o n n e o f KD
a 47·35·39·40·7·35·16·192· that

h a t h g r e a t c r
31·17·46·31·21·51·7·17·45·11·50·

d i t w i t h h i s f
5·27·45·58·27·45·31·31·27·47·15·

a t h e r f r o
17·45·31·7·50 goeing now 16·51·32·

m Ho
42·164," and so forth. The rest of the

[1] "Which causes me to be extreamly troubled with the headach and to make use of another for the writing in cypher which J should have done else myselfe."—Parliament translation.

letter goes on in the same manner, but we need not repeat the figuring. The translation of it is that "260 thought fitt to speake to him to solicit KD at his arriuall for to dispatch of 6000 armes to be sent to N to arme the Scottch or to imploy any other way 189 shall thinke good. WM being returned hath aduertised 260 that some Englishe Catholiques in F haue layed their purses together for supply of armes for 189. 260 doth therefore desire 189 to aduertise WM of the place where they are to be sent. 189 may write to WM in the cipher 189 hath with 260." This was clearly a document to be veiled in cipher. The publication of these letters by the Parliamentarians caused great excitement, we are told—a matter to be scarcely wondered at,—and we can well imagine that KD and WM, 189 and 260, would take uncommonly good care to keep the Channel between themselves and the victorious Puritans.

It will not have escaped the notice of the careful reader that, while some of the letters in the little extract we have given are each time they occur represented by the same number,—H, for instance, being always 31,—others vary, so that N is represented by 39 or 40, T is 45 or 46, and R is 50 or 51. This changing of the symbol is frequently resorted to in cryptography, or a little patient analysis of a communication would presently throw light upon it. First a small clue would be gained, and then more and more would follow. E, for instance, is the letter that occurs most commonly in English; therefore, unless the symbols are changed, the one that occurs oftenest will mean E.[1]

[1] A curious old inscription over the decalogue in a country church runs as follows:—

PRSVRYPRFCTMNVRKPTHSPRCPTSTN.

It is said that the meaning of this was not discovered for two hundred years; but if our readers will add to these letters a sufficient sprinkling of one more letter—"E"—they will have no difficulty in converting it into "Persevere, ye perfect men; ever keep these precepts ten."

Double L is a common final, so if we find two similar symbols recurring at ends of words we may at least think them to be LL. Of course they may be double SS, another common termination; but if we assume them for the time being to be LL, then we may look up ELL. That means very little, but it is at all events something to build a theory on. Then we think of sell, well, fell, and maybe add another letter to our store. All this of course is very speculative and tentative, but it is in this direction that he who would decipher a cryptogram must proceed.

As another illustration of the number cipher we may instance that used by Sir Ralph Verney. An example of it may be found in the "Notes of Proceedings of the Long Parliament," that may be seen in the valuable reproductions issued by the Camden Society. The editor makes the following note: "The following numerals written

in pencil by the hand of Sir Ralph Verney look like an attempt to take notes in a cipher. The numbers range from 1 to 28. I add them here in the hope that the ingenuity of some reader may discover their meaning." As they evidently entirely nonplussed him, one hardly sees why he should somewhat slightingly have called them "an attempt" to "take notes." If we come across a slab in the British Museum covered with arrow-head forms, we may scarcely legitimately regard it with supercilious indifference, or, at best, contemptuous toleration, as the quaint attempt of some poor Assyrian ignoramus to record something or other; nor should we lament from our higher level the vainglorious conceit of some Chinaman who evidently thinks that his queer characters mean something.

A Mr. Cooper, in the year 1853, succeeded in deciphering the figures, and they proved to be rough notes of matters referred to

in Parliament. Though there can be no doubt of the correctness of the key that has unlocked their significance, the fact is patent that Sir Ralph, writing probably against time and in the midst of many distractions, was not entirely at home in the cipher he employed, wrong characters being at times introduced. The following are examples of the cipher used by Sir Ralph Verney in making his memoranda: "28 · 17—15 · 22 · 5 · 3 · 14 · 10 · 5 · 8—17 · 2—20 · 15 · 5 · 5 · 15 · 3 · 8—5 · 17—6 · 15—14 · 20 · 17 · 18 · 15 · 13—16 · 28—5 · 7 · 16 · 8—7 · 17 · 18 · 8 · 15." This deciphers into: "No extracts of letters to be aloued in this House." Another one reads: "5 · 7 · 15—12 · 3 · 16 · 28 · 10 · 15—16 · 8—28 · 17 · 7—10 · 17 · 27 · 15 · 5 · 17—11 · 3 · 15 · 15 · 28 · 7 · 16 · 10 · 7," signifying "The prince is noh come to Greenhich." For the fourth word here we should probably read either now or not, the difference in sense being considerable,

the direct contrast between an affirmative and a negative. "Come to" is in the cipher run together into "cometo," but this was probably carelessness rather than craft.

The ingenious and painstaking Mr. Cooper presently determined that the same numeral always stands for the same letter, and that is always a very helpful state of things for the decipherer. Of course A is not 1, and B 2, and C 3, and so forth in regular sequence, as that would be a great deal too easy an arrangement, so that it remains to find out what arbitrary arrangement has been made. On analysis it is found that the letters are represented by numerals as follows :—

2 = F	8 = S	14 = A	22 = X
3 = R	9 = W	15 = E	25 = Y
4 = K	10 = C	16 = I	27 = M
5 = T	11 = G	17 = O	28 = N
6 = B	12 = P	18 = U	
7 = H	13 = D	20 = L	

In the memoranda that have come to light we find no use of 1, 19, 21, 23, 24 or 26, but on the other hand we find that by chance Verney had no necessity to use in anything he wanted the less-commonly employed letters J, Q, V, or Z; we may therefore fairly assume that four of the missing numbers would be the equivalents of the four missing letters.

For facility of reading anything already written, the table we have given, numbers and then letters, is the most useful; but if we desired to write anything ourselves, a table having first letters and then numbers is of more service. If we want to translate a good stiff piece of Russian, we turn to the Russian-English half of our dictionary; but if we desire to translate our own tongue into Russian, then we seek help from the English-Russian portion of our book. In the same way the sender of a cryptogram uses "ordinary letter-cryptogrammic,"

while the receiver employs to translate it the "cryptogrammic-ordinary letter" table. For the purpose of the sender the Verney table should be as follows :—

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

We have assigned values to the *J*, *Q*, *V*, and *Z*, the letters missing in Verney's notes. If, therefore, we had desired to pass a little note across the House to Sir Verney, "Why do you use cipher?" we should have sent him the following: "9 · 7 · 25—13 · 17—25 · 17 · 18—18 · 8 · 15—10 · 16 · 12 · 7 · 15 · 3." His supposititious reply to this supposititious message we leave to our readers to translate. It ran as follows: "27 · 16 · 28 · 13—

25 · 17 · 18 3—17 · 9 · 28—6 · 18 · 8 · 16 · 28 · 15 · 8 · 8," a remark that shows that while he felt our note an intrusion, also shows that we had succeeded in mastering the cipher he was employing.

We also find a great revival of cryptology during the stormy period that has its central point in the flight of James II. and the landing of William III., when plot and counter-plot sought safety in the use of cryptograms. The adherents of Mary Queen of Scots and the followers of the Pretender were naturally also very proficient in their use.

Edward Somerset, Marquis of Worcester, published in the year 1633 a little book called the "Century of Inventions." This nobleman was greatly addicted to scientific pursuits, and at the same time was in command of a large body of troops under Charles I. He afterwards attached himself to the suite of Charles II. in exile in

France, and being sent over by him to London to procure intelligence and supplies, was speedily detected and put under lock and key in the Tower. He was set at liberty at the Restoration. His enforced leisure in the Tower gave him abundant leisure for study, while his position as a man of affairs at so stormy a period explains how it is that amongst his hundred inventions not a few deal with the various methods of secret communication.

It is of course beside our present mark to deal with the book as a whole. Suffice it to say that the majority of his inventions are of an entirely practical character, and the germ of the steam engine of to-day in all its mighty force and pervading utility is to be found in his observations. The closely fitting cover of a vessel in which he was preparing food in his apartment of the Tower was suddenly forced off by the pressure of the confined steam, and he drew

from this the suggestion that such a force might be turned to useful account.

That he himself believed in the value of his work is quaintly evident, for in the dedication of his book to the King's most excellent Majesty, plus Lords and Commons, on the sensible principle of having more than one string to his bow, he writes: "The Treasures buried under these heads, both for War, Peace, and Pleasure, being inexhaustible I beseech you pardon if I say so: it seems a Vanity but comprehends a Truth: since no good Spring but becomes the more plentiful by how much more it is drawn: and the Spinner to weave his web is never stinted, but further inforc'd. The more then that you shall be pleased to make use of my Inventions the more Inventive shall you find me, one Invention begetting still another, and more and more improving my ability. And as to my heartiness therein there needs no addition, nor to my readi-

ness and spur. Therefore be pleased to begin, and desist not from commanding me till I flag in my obedience and endeavours to Serve my King and Country.

> For certainly you'l find me breathless first t'expire
> Before my hands grow weary, or my legs do tire."

No. 1 on his list is "Several Sorts of Seals, some shewing by scrues, others by gages, fastening or unfastening all the marks at once. Upon any of these Seals a man may keep Accompts of Receipts and Disbursements from one Farthing to an hundred Millions. By these Seals likewise any Letter, though written but in English may be read and understood in eight several languages, and in English itself to clean contrary and different sense, unknown to any but the Correspondent, and not to be read or understood either, if opened before it arrive unto him, so that neither Threats, nor hopes of Reward, can make him reveal the secret, the letter having been intercepted by the Enemy."

No. 2 is a further development, showing how ten thousand people may use these wonderful seals and yet keep their secrets intact. No. 3 is "a Cypher or Character so contrived, that one line, without returns or circumflexes, stands for each and every of the 24 letters, and as ready to be made for one letter as the other," while the inventive faculty in him, growing, as he declared it would, by use. No. 4 is "this Invention refined and so abbreviated that a point onely showeth 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: 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." One almost wonders that he did not

hit upon the idea of dipping his fingers in the ink and so making four or five points at once instead of being content with two. His fifth invention is "a way by a Circular motion either along a Rule or Ring wise, to vary any Alphabet, 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."

We were first made acquainted with the labours of the Marquis by a reference to them in an educational work, but preferring always, where at all practicable, to go to the original, we turned it up in the magnificent Library—the students' Paradise—at the British Museum. We note with great regret that the author gives no further clue to his inventions than such

short sketch as we have already quoted in the case of one or two of them. This fifth invention of his, the constant shifting

Fig. 8.

of significance of letters rule or ring-wise, is very descriptive, however, of two methods, or rather perhaps one method in two forms, that was largely in use in the middle ages. Fig.

8 is an illustration. We draw a circle on a fairly stout piece of cardboard and divide its circumference into twenty-six equal parts, and in these divisions we place the letters of the alphabet in the regular A B C sequence of ordinary usage. We then cut out a somewhat smaller circle from one card and divide the edge of this also into twenty-six equal parts, and in these we place the alphabet letters in any haphazard fashion we choose. We next cut this out and place it in the centre of the first and drive a good strong pin through the centre, the result being that the upper card revolves freely on the under one, enabling us to bring any letter of the one in a line with any letter of the other. The person with whom we are corresponding has a similar arrangement, and we arrange together that, as in Fig. 8, J shall be adjusted to A. We then spell the words out, the true letters being those of the outer circle, but representing them by those of the inner. If

then we desire by means of this diagram to write the word February, it would come out as DZOXEJXT. The sender reads from the outer circle to the inner one, while the receiver reads the characters from inner to outer, a glance at the two circles showing him that D is really F, that Z is E, and so on. This may be used, as set, for a time; but if we want to circumvent the ingenious meddler who begins to think that he has got a clue through our continuous use of the same equivalents, all that is necessary is to give the upper card a gentle push and A, B, C, etc., are now represented on the inner circle by entirely different letters, and the too ingenious onlooker is at once thrown off the scent. Our correspondent must of course know of this and give his card a similar turn, but this may easily be arranged. It might, for instance, be that two similar letters followed by a different one should convey the hint; thus, KKQ would mean that at this point we

shift our inner alphabet till the letter within A should be Q; and if we like in the course of a page or two to change again, then BBX would convey the hint to spin the circle round until X became the new equivalent of A.

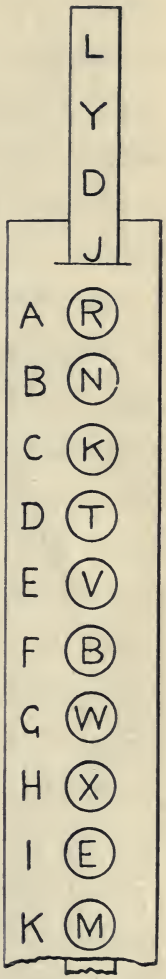


Fig. 9.

This combination of the fixed and revolving circles is a most excellent one, its only drawback being that it is perhaps a little difficult to read the radiating letters, as while only one is absolutely straight up the others begin to lean away at gradually increasing angles, till we get at last to one that is absolutely upside-down. After all, however, a little practice should make the reading of them a very easy matter; but to those who feel a difficulty Fig. 9

should come as a boon and a blessing where the "Ring-wise" arrangement is changed for that "along a Rule." We must confess ourselves that the compactness of No. 8 more than compensates to our mind for any topsy-turvydom, Fig. 9 being a long rambling sort of thing to keep in one's desk, and possessing great possibilities of being torn when turned over amongst other papers. We have only drawn a portion, less than half—the proportion in fact that AK, the part we have shown, bears to AZ. To make this key a somewhat broad strip of card has twenty-six openings cut or punched in it, and opposite to these, in regular sequence, are placed the letters of the alphabet. A slit is then cut at top and bottom, and a narrower strip of card is inserted so that it will slip, not too easily, up and down. All along this, at the same distances apart as the openings on the broader strip, are placed the letters of

the alphabet in any irregular order. When the whole twenty-six letters have found a resting place, the strip should still be so long as to admit of the repetition of the first six or eight, as what we want is not only a letter to appear opposite the A, B, C, down to the end, but also some little surplus, so that the slip can be moved up and down so as to bring other combinations in. Of course the reader, on inspection of our figure, sees that in principle it is identical with the circular card method already shown, that "head" would be XVRT, and that we could at once vary the equivalents by sliding the narrow strip upwards or downwards. If we slipped it down until D came opposite to A, then "head" would no longer be XVRT, but BKDN. Our correspondent must clearly be informed of any such shifting, and of course any accidental shifting of the sliding piece must be guarded against. The merest glance that the proper key letter is still opposite to

A will suffice to show whether any movement has taken place.

To revert now to our ingenious Marquis. After devoting the first five of his "Century" to cryptography, he remembers that after all there are other matters that may be dealt with too; but cryptography crops up again at No. 33, and this and Nos. 34, 35, 36, 37, 38, 39, 40, 41, 42, and 43 are all devoted to suggestions for secret communication, though some of them are of a very forced character and having nothing to do with writing at all. Fig. 40, for instance, is to be worked by the sense of smell, pegs of sandal-wood, cedar, rosewood, and so forth being so arranged and grouped that even in the dark a message could be composed or discriminated; while another method trusts to the taste, pegs being dipped in alum, salt, aloes, etc., and distinguished by touching them with the tongue. It is scarcely to be imagined that even amongst the blind such a sensitiveness to smell or taste could be developed as

would make these fancies workable realities. We should imagine that some sixty or eighty applications of the tongue would end in a complete dulling of the perception, while one could scarcely imagine anything much more nauseous than a course of peg-tasting for half an hour of alum, castor oil, saccharine, turpentine, cod-liver oil, lavender water, salt, and as many more strongly flavoured ingredients as would build up an alphabet. One of his methods is by a knotted string, and another he calls a bracelet alphabet. After No. 43 he devises a new tinder box, an artificial bird, and so on; but at No. 52 we find him harping on the old string again, if devising an alphabet by the "jangling the Bells of any parish church" can be so termed, and at No. 75 we are instructed "how a tape or ribbon weaver may set down a whole discourse without knowing a letter, or interweaving anything suspicious of other secret than a new-fashioned ribbon."

It is certainly very remarkable that when

the Marquis had the whole field of possible inventions open to him, he should have devoted so large a proportion of his book to the thinking out of so many schemes in this one narrow field of investigation.

The bracelet alphabet idea has been utilised, and cryptographic messages may readily be conveyed by means of any coloured objects such as beads or precious stones. If we take, for example, some red, green, yellow, black, blue, and white beads, we can so arrange them in pairs, each pair representing one letter of the alphabet, as to be able to spell out any communication. Such a bracelet or string of beads could be worn on the person, or sent amongst other trinkets without exciting any special observation. Receiver and sender would mutually arrange a scheme of lettering by this aid of colours, and if at any time this were discovered a re-arrangement of the colours would alone be necessary for a fresh departure, and these variations could be made

in an immense number of ways. By way of a start we would suggest the following key:—

A = red and green
B = yellow and green
C = red and yellow
D = yellow and black
E = red and black
F = black and yellow
G = green and black
H = yellow and red
I J = green and yellow
K = green and red
L = black and red
M = red and white
N = white and red
O = green and white
P = black and green
Q = white and green
R = white and black
S = yellow and white
T = white and yellow
U V = green and green
W = black and white
X = red and red
Y = yellow and yellow
Z = black and black

Beads of turquoise blue colour can be used to divide words, or they may be inserted anywhere as non-significants. If the beads themselves are not available, the initials of the colours will suffice; thus, if we cannot actually express A by a red and a green bead, we can by RG. As B is already required for black, the blue must be T for turquoise. Ignoring T wherever it comes, the letters must always be read in pairs, as it takes two of these to signify the real letters of

the message, and, knowing this, any number of accidental breaks, as misleaders, may be introduced. "Mind see Cecil" would therefore read RWGYWRYBYWRBTRBRYTRTBRY-GYBRT or RWTGY WRYBT YWRB TRBRBT RTBRYG YBRTT, or any other arbitrary breaking-up of these particular let-

Fig. 10.

ters into sham words to mislead investigators that we chose to make.

In Fig. 10 we have strung the actual beads, marking their colours by the signs used in heraldic work.[1] Their message is the beginning of "Mind see Cecil."

[1] Should any of our readers not know these, they would find it useful to learn them, as they come in very serviceably not only in finding from these signs the actual colours of arms engraved in illustrations, book plates, and the like, but they are also very useful as a shorthand way of expressing colours for any purpose, as, for example,

A curious form of early cipher may be seen in Fig. 11. Each of the persons desirous of communicating with each other was provided with a similar strip of board or stout card. Along the top of this was placed the alphabet, either according to the common order of the letters or in any irregular fashion, so long only as they all made their appearance somewhere in the series. A knot was then tied at the end of a piece of string, and by it, through a hole made at the top of the strip, the string was held in its place. The sides of the strip of wood or cardboard were notched, and the string was wound round tightly and was held in these teeth or notches and secured at the bottom by being inserted in a cut. On this string the person

our beads. Gold or yellow are indicated by dots, while silver or white are left quite plain. Red is shown by a series of upright lines and blue by horizontal ones, while black is known by being marked in plaid by lines both horizontally and vertically disposed. Green is indicated by inclined lines downwards from right to left.

sending the message made a mark with ink or colour in a line with any desired letter. The message being thus spelt out, the string was unfastened and then wrapped round a package or in some such inconspicuous way got into the hands of the receiver. He, on its receipt, wound it round his counterpart board and was

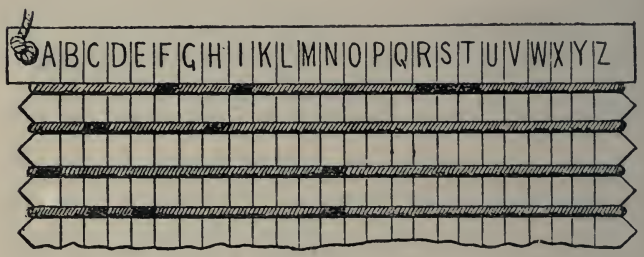


Fig. 11.

enabled, readily enough, to read off the communication. Fig. 11 is only a small portion of such a board, though sufficient to indicate its use. We have commenced upon it the message "First chance not till May," but our space enables us to show but a very limited portion of this. The first line gives us FIRST,

but the second line only gives CH, as the A we want next comes before C and H in the alphabet and must therefore come on the next row. If we marked it on the same row, we should get ACH, and this is no use to us. The only drawback to this method of communication is that, unless each party stretches the string with equal tension all through, the marks will not in the second winding come in quite the right places. A slip along of only one letter space would turn FIRST into GJSTU, to the great bewilderment of the receiver of this enigmatical message.

Lord Chancellor Bacon was an enthusiast in cryptology. He laid down the law in quite Johnsonian style in this and many other matters. The three essentials of a good cipher, he very justly declared, were facility in execution, difficulty in solution, clearness from suspicion. This latter item is perhaps not very clearly put; his meaning is safety from the decipherment of those for whom the com-

munication was not intended. A method that he himself devised, he with calm assurance introduced as "a cypher of our own which has the highest perfection of a cypher, that of signifying *omnia par omnia*, anything by everything." This sounds most convincing and awe-inspiring. It is ordinarily said that people will accept a man pretty much at the valuation he sets on himself; but when one presently re-reads this Baconian dictum, and asks what it means, perhaps the truest answer would be "very little."

As a cipher it is not of any great merit, and it sins grievously against his own first rule, since it is by no means facile in use. He employs only the letters A and B, and arranges these in groups of five for the different letters. If then we desire to send a message of fifty letters, it would be necessary to use two hundred and fifty. It is therefore far too slow in operation; even if one had the various formulæ at one's finger's ends, it would involve

five times the labour of ordinary writing. When we once know that each group of five stands for a single letter, it is as liable of discovery, on the same principles of decipherment, as a simpler arrangement. Of course, if Bacon had not published this clue, the task would have been immensely more difficult, and it is only just to his method to frankly and fully say so.

The cipher was composed as follows:—

A=AAAAA	I =ABAAA	R =BAAAA
B=AAAAB	K=ABAAB	S =BAAAB
C=AAABA	L=ABABA	T =BAABA
D=AAABB	M=ABABB	U =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

We shall the better see the cumbrous nature of this cipher if we endeavour to apply it. Such a word, for instance, as cryptogram would become by this code—

AAABABAAAABABBAABBBABAABAABBAB
AABBABAAAAAAAAAABABB

In the same cumbrous fashion, and based on the same lines as that of Bacon, is the following, which we extract from an old encyclopædia:—

A = 11111	J = 12112	S = 21122
B = 11112	K = 12122	T = 21211
C = 11121	L = 12211	U = 21212
D = 11122	M = 12212	V = 21221
E = 11211	N = 12221	W = 12121
F = 11212	O = 12222	X = 22212
G = 11221	P = 21111	Y = 22221
H = 11222	Q = 21112	Z = 22122
I = 12111	R = 21121	

The intervals between the words were to be marked by 333. If we wished to ask our correspondent to "come soon now," we should have to set forth the following unwieldy arrangement:—

11121122221221211211333211221222212222212221
333122211222212121

Another plan that has been sometimes adopted may be illustrated by the following cumbersome example from Trithemius, where

only the second letter in each word counts, and all the rest is mere padding: "Baldach abasar lemai clamech abrach misach abrai disaria athanas." This, after all, only signifies "Abel bibit," and it has taken fifty-six letters to give nine!

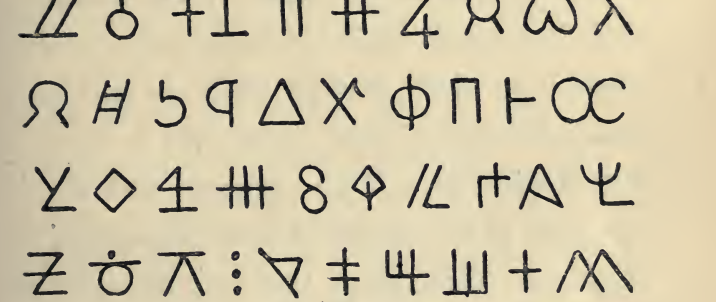


Fig. 12.

In some of the Elizabethan ciphers neither letters nor figures are used; but in place of them we find merely arbitrary forms, such as those we have represented in Fig. 12. But this, though it looks at first sight very mysterious, has no more real element of difficulty in it than the use of the letters of the alphabet.

It is really immaterial whether we spell cat with a curved line (that we have learnt to call C), and two sloping lines coming to a point and a horizontal line across their centre (that we have got used to as A), and a third symbol made up of an upright line and then a horizontal line across its top (a form that we are accustomed to call T), or whether we decide that C instead shall be made of two lines crossing at their centres, while A shall be a thing made up of two circles, like a figure 8 turned sideways. If we recognise that a certain form is the symbol of a certain letter, we soon learn to recognise this form when we see it, and its shape is a matter that is absolutely indifferent to us. If the letters of our present alphabet had not been the shapes we know them, but something entirely different, it would still have been our alphabet, and it is as easy to write dog in Greek or German letters, or in these grotesque forms of Fig. 12, as in the letters in which this page before us is printed.

Why should not the ten upper forms in Fig. 12 spell cryptogram just as well as CRYPTOGRAM does? In the one case we are used to the forms employed, and in the other case we are not. That is really the only difference.

CHAPTER III

Is an undecipherable cryptogram possible?—The art of deciphering—Keys for the analysis of a cryptogram—Oft recurring letters—Great repetition of vowels—Patient perseverance—Papers on the subject in *Gentleman's Magazine* of 1742—Value of general knowledge—Conrad's rules—The letter E—"Noughts and crosses" cryptogram—Its construction—Ciphers from agony columns of *Standard* and *Times*—Prying busybodies—Alternate letters significant—Ciphers based on divers shiftings of the letters—Cryptogram in Cocker's "Arithmetick"—Inventor in 1761 of supposed absolutely secret system—His hopes and fears thereon—Illegal to publish Parliamentary debates—Evasion of the law—Poe's use of cryptogram in story—Secret marks made by tramps and vagrants—Shop ciphers for marking prices on goods—Cryptogrammic trade advertisements—Examples of cipher construction—The "grill" cipher—The "revolving grill"—The "slip-card"—Forms of numerical cipher—The "Mirabeau"—Count Grousfield's cipher—Communication by use of a dictionary—The "Newark"—The "Clock-hands"—The "two-word" cipher—Conclusion.

THE question as to whether a cipher has ever been devised that could for all time successfully defy patient investigation will naturally occur to our readers. Some would have it that as all the advantages are in favour

of the ingenious cryptographist, it should not be impossible to build up a monument of ingenuity that should be safe from all assault, and certainly this is an opinion that commends itself to us as a very reasonable one. Others would tell us that nothing that the wit of man could devise is safe from the wit of some other man to search out. However this may be,—and the point, of course, can never be settled,—we must bear in mind that what to the ordinary man is hopeless may not prove so to the deftly-trained ingenuity of the expert. A cryptogram in Paris that was deciphered some few years ago for the French Government took accomplished experts just six months to lay bare, and the ordinary amateur would scarcely attack any problem with such dogged determination as that.

In the art of deciphering it is emphatically the case that "practice makes perfect." There are certain very definite rules, too, that prove of immense assistance in the analysis of a

cryptogram. There are special conditions, however, for each language, "O," for example, being a much more freely used letter in Spanish or Italian than in English. In the English language "E" is the letter that occurs with the greatest frequency. The easiest cipher to translate is that where each letter in it always stands for some other individual letter, where K, for instance, always means F, or P may be recognised as L all through. Where too the symbols, puzzling though they be, are always arranged as in an ordinary communication, and broken up into words. A cipher at once becomes immensely more difficult if the letters change their significance, so that, as in the revolving card we have already illustrated, E, for instance, may be sometimes written as J, at others as S, or M, or X. We at once add greatly, too, to the puzzle if the words are all joined into one, or are arbitrarily broken up. Non-significants also add to the difficulties of analysis, and it is a good plan

to cut out every "and" and "the" and such-like common words that can at all be spared. The English tongue abounds in monosyllables.

Of course the letters that necessarily occur most commonly are the vowels, and in words of two letters, such as am, in, of, or we, one of them is necessarily a vowel. E is not only the commonest letter in use in English, but it also very frequently occurs in couples; been, seen, feet, sweet, agreed, speed, are examples. EA and OU are the double vowels that most commonly go together, as in pear, early, and ease, or our, cloud, or rough. A single letter will be A, or I, or O. Of all English words "the" is the one that most commonly occurs, and "and" runs it very closely. If, therefore, we have determined that the commonest symbol of all in our mysterious cryptogram is E, then if a very constantly recurring word of three letters ends with this same symbol, we may begin to hope that we have found out H and T. EE, OO, LL, SS, are the doubled letters

of most usual occurrence; see, feet, tool, shall, well, miss, and loss are illustrations. A begins three very common two-letters, an, as, and at, and O begins of, on, or, and ends do, go, no, so, to. In by far the great majority of words the first or second letter is a vowel. Q always has U after it. No English word terminates with I. It is on such bases as these, vague as some of them may seem, that the decipherer works. There is no royal road; nothing but delicate discrimination and unlimited patience will achieve success.

When certain equivalents are determined, they should at once be written down. We may now take any word in which any one or more of them occur, and substitute them for the symbols standing for them, and then just put dots for the others until more light dawns. Very often this proceeding at once suggests the whole word, and if so we have at once gained a knowledge of other charac-

ters and soon get a long way towards building up our key. If, for instance, we have discovered by analysis that X, L, and P are really A, I, and T, and we come across the words FXLTNXO JPXPLER, we set them down as follows: ·AI··A· ·TATI··, and it presently begins to dawn upon us that the words "railway station" would just fit in. We at all events accept this tentatively. If we are right we have added largely to our store, for we now see that F must really be R, T must be L, N must be W, O will be Y, J is S, E must be O, while R represents N. Our knowledge of three letters has thus given us seven others. If we presently find in the cryptogram the group of letters JQXTT, we remember that we know X to be really A, and our railway station guess has led us to believe that J is really S, and T is L; we try how it looks if we turn JQXTT into S·ALL. This suggests to us small, stall, and shall, so Q is

either M or H; we know that the word is not stall, because T we already know is shown by P. One or two endeavours at words containing Q will determine for us whether we shall read it as M or H. Z, the commonest symbol of all, we have decided at once to be E, and PQZ often recurs. T·E is evidently THE, so Q is not M,—for there is no word TME,—but H. JQXTT is therefore SHALL. So by patient analysis, sometimes by success, sometimes by failure, sometimes by guessing what it might be, sometimes by seeing what it could not be, we step by step press on. The man who would pull down a wall finds it difficult to make a start, but when he has once got his pick fairly into a joint the first brick is presently got out, and then all the others follow, every brick removed making the work easier. The first insertion of the quarryman's wedge wants considerable skill; blow after blow of the swinging hammers fall swiftly then upon it, and each tells,

until presently the great block of many tons in weight is riven in twain.

In the *Gentleman's Magazine* for the year 1742 will be found an interesting series of papers on the art of deciphering, entitled "*Cryptographia denudata*," the author being David Arnold Conradus. After a general introduction he first proceeds, curiously enough, in an English magazine, to an exposition of the German language, pointing out the characteristic recurrences of letters, terminations of words, and so forth, by which one may attack a cryptogram in that language. He then proceeds with equal thoroughness to analyse the Dutch language, then the Latin, English, French, Italian, and Greek. He writes: "The Art of Deciphering being an abstruse Subject I purpose in this Attempt to explain it with Accuracy and Perspicuity, and I doubt not by this Undertaking both of gratifying the Curiosity of the Inquisitive, and of convinc-

ing those of the Certainty of the Art who have hitherto questioned it. There are to be found Men of uncommon Capacity who are ready to assert with great Confidence that no Success is to be expected from Enquiries so doubtful and uncertain in their Nature. There are these whose Credulity and Superstition set them almost below Mention, who pronounce no less positively that the Interpretation of private Characters, if it ever can be attained, is the effect of Magic. The Art of Deciphering is the Practice of interpreting Writings composed of Secret Characters, so that the true sense and words of the Writer shall be exactly known. This Art, however difficult it may appear, will be admired for its Simplicity and the Ease with which it may be attained, when the Theory of it is understood, which depends upon many certain and a few probable Propositions. The Usefulness of Arts by which suspected and dangerous Correspondences may be detected cannot be

denied, nor is it a small Incitement to the Study of it that those who profess it are employed by Princes, in time of War particularly, and rewarded with the utmost Liberality.

"He that engages in this Study is supposed to be previously furnished with various kinds of Knowledge. He must be in the first Place Master of Orthography, that we may know what Letters are required for each Word. He should be acquainted with several Languages, and particularly Latin, which is most frequently made use of in secret Writings; and he will be a greater Master of this Art in proportion as his Knowledge of Languages is more extensive; for the Decipherer has to determine what the Language is, in which the secret Writing is composed, whether Latin, French, or any other; and by this Art are to be discovered the peculiar Characteristics of each Language.

"It is likewise necessary to understand at least the Elements of various Sciences, that

the Sense of any Passage may be more easily discovered, and one word contribute to the Explication of another. Cryptography, or the Art of writing in Ciphers, must likewise be understood, by which so many Artifices are practiced, so many intricate Alphabets formed, and so many Expedients for Secrecy produced as requires the utmost Acuteness to detect and explain. Upon the whole as a Man advances in Learning he becomes better qualified for a Decipherer.

"By Accuracy of Method and a just Deduction of Particulars from Generals, is our Art exalted into a Science, consisting of certain and indubitable Propositions, from whence the Rules are drawn, which are to be used as Clues in the Labyrinth of Cryptography."

Truly our author magnifies his subject! He who would shine in it would be a man who might have been Solicitor-General or Primate of all England had he not chosen the path of the cryptographic expert!

His rules spring rather quaintly from his propositions. Thus the proposition says "In a Writing of any Length the same Letters recur several times." Then the rule says "Writings of Length are most easy to decipher, because there are more Opportunities of remarking the Combination, Frequency, etc., of the Letters." One would have thought the proposition sufficiently clear to a man of ordinary intelligence, without need of what is practically a repetition of it: merely old matter under a new name. Another proposition says that "The Vowels are four times outnumbered by the Consonants, the Vowels must therefore recur most frequently." The rule that is based on this is as follows: "The Letters that recur most frequently are Vowels."

Some of his suggestions are very good, while others do not seem so very helpful after all. Thus we are gravely told, if the writing be in Dutch any three-letter word must

either be aal or aap, aan, aen, als, amt, arm, arg, ast, bad, baf, bak, bal, ban, bas, bed, bef, bek, bel, ben, bes, bid, bik, bil, bit, bly, bok, bol, bon, bos, bot, bry, bul, bus, dag, dam, dan, das, dat, dek, den, der, des, die, dik, dis, dit, doe, dog, dol, dop, dor, dun, dur, dyk, een, eer, eet, elf, elk, end, erf, eva, fyn, gal, gat, gek, git, plus one hundred and eighty-two more right away through the alphabet till we pull up finally at zyn. Whether this list of all three-letter words be at all exhaustive, our ignorance of Dutch forbids us to say; but in the English section he roundly declares that any three-letter word in that language must, at all events, be one out of the list of one hundred and eight that he gives. On looking over this list, however, one quickly notes many omissions. The words, for instance, beginning with M that he gives are mad, man, may, and men; but to these we may at once add mar, mat, map, maw, met, mew, mid, mob,

mop, mow, mud, and mug. As we have thus readily amplified his four words under only one initial letter into sixteen, it will readily be seen that the same treatment all through the alphabet would prodigiously increase his grand total of one hundred and eight. His formula to be of practical use should therefore be extended into—"Any word of three letters will be found to be one of the following one hundred and eight, unless, perchance, it may be one out of the many scores of other three-letter words that we have omitted to include in our list." Besides, in any case, the list is utterly useless. If it were possible to say that any three-letter word must necessarily decipher into "and," or "the," or "but," the hint would be a most valuable one; but when one can go no further than to say that it is either one of those three, or, more probably, one out of a list of four or five hundred other words, the help given is, after all, not of great

value. Setting up as some little authority on the matter ourselves, we may add to these rules of Conrad's one which he seems to have overlooked: that all words beginning with H will be found to be either horse or hallelujah, or else one of the hundreds of other words that commence with that letter.

The letter E is the commonest in use of all the letters, not only in English but in all of the European languages. Statistical enthusiasts assert that out of every thousand letters in any ordinary page of prose, one hundred and thirty-seven of them will in English be this letter. This is a matter that our readers, who are statistic and enthusiastic, can at once check from the page before them, if, indeed, we may assume it to fulfil the conditions named, and not sink beneath even ordinary prose. In a French book the letter E should occur about one hundred and eighty-four times per thousand, a

much larger proportion than in English; while the German language runs the French very close, being one hundred and seventy-eight per thousand. Spanish and Italian are about the same in this respect as English; one hundred and thirty-one per thousand being assigned to Italian, while in Spanish the letter E occurs one hundred and forty-five times. Of course, all these numbers are necessarily only approximate. The only letters of which more than ten per cent. occur are the I, N, and O; the former coming out in Italian at about one hundred and three per thousand, the N at about one hundred and ten in German, and the O at about one hundred and seven in each thousand letters used in Italian and Spanish writing and printing.

An old fellow we once met, and who prided himself on being rather clever at this art or science of decipherment, told us that he had, for the fun of the thing, joined in

some of the "agony-column" advertisements in the newspapers, to the great perplexity of the original correspondents, and he

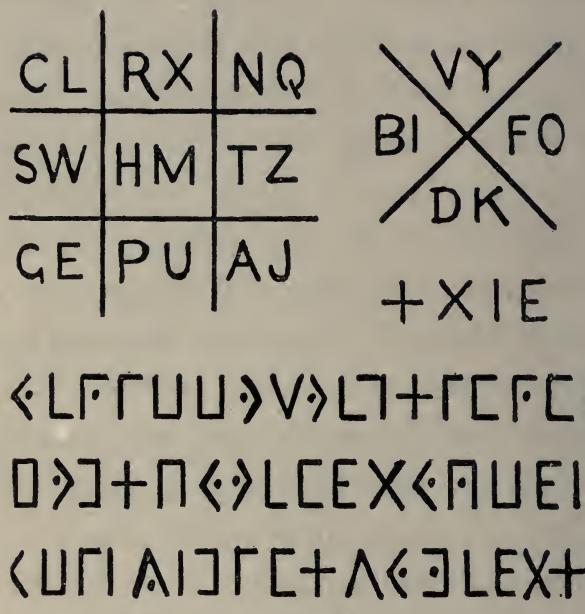


Fig. 13.

further ventured the rather rash remark to us that he could unravel any cryptogram. On this we sent him a message that had not a single E in it, as we knew that this letter was the first he would

endeavour to get hold of; and the final outcome might be considered a confession that he was beaten—at least, he never replied to our communication. The form of cryptogram we employed is rather a good one, and we have often used it on postcards, etc. Probably most of our readers in their school-days have played "noughts and crosses" when they ought to have been devoting their time instead to one of the subjects set down in the curriculum. Set out, then, two horizontal and two vertical lines, as shown in the upper part of Fig. 13, and place in the spaces made by them the various letters of the alphabet in pairs, so far as they will go. As a matter of fact, it will use up eighteen of them. Then place two other lines X-wise, as we may see, to the right of the previous arrangement, and in the four intervening spaces that these make place, also in pairs, the remaining eight letters. These letters may be arranged in

any order. Should it at any time appear that some unauthorized person has penetrated the mystery, it would merely be necessary to shift the letters and start happily again. This shifting would be ar-

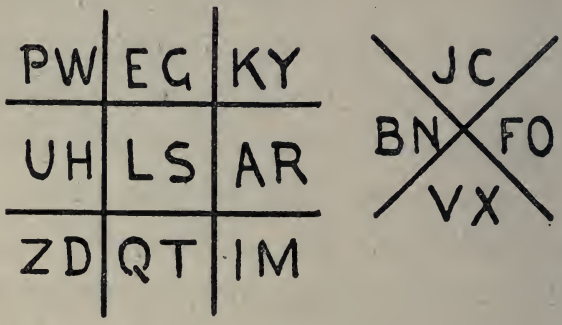


Fig. 14.

ranged as follows:—On counting the pairs of letters, we find, of course, that there are thirteen. Two in the first space, two in the second, and so on. Our present arrangement is 1 C L 2 R X 3 N Q, and so forth. It

is evident that if we merely sent our correspondent the new formula, as 1P W2 EG 3KY, any unauthorized person into whose hands it fell might reconstruct it. To avoid this, we should not place our figures in the ordinary numerical order, and we should use others beyond the thirteen. These would be non-significants, and any letters that followed them we should, on receipt, merely run our pens through. We have in the upper part of Fig. 14 given the new combination, and the formula for it might run as follows: 12FO37CJ5LS91ORA9IM4UH, and so forth. We should, on getting this, draw out the skeleton lines and lightly number the spaces, and then proceed to construct our key, putting FO in the twelfth space, LS in the fifth, taking no notice of the CJ, as we have no thirty-seventh space to put it in.

To use this cryptogram, we must note the shapes the lines make. The central space in the upper left-hand diagram in Fig. 13 is

clearly a square; the space above would be a square, except that it has no top line; the space to right of it is also a three-line figure, the square being incomplete for want of the right-hand line; and the same applies to the space below, to the left and so on all round. The X-like figure gives us a V-like form at top, a reversed V at base, and two other V's that are turned sideways. For the first letter in each space we merely draw that space; thus H is a square, and the second letter we represent by a dot in the space. Below the X-like cross we have placed four forms that are merely dummies for use where we please; and such little-used forms as those for J, X, or Z may be also thus employed, as any one receiving and reading off the message would readily detect their non-essential character. In the lower half of Fig. 13 is the message we send by it—"On arriving at this point our Frank sat down." Below the

second combination, Fig. 14, we place another communication; but this our readers, with the key before them, should find no difficulty in deciphering for themselves, so we leave it to them.

The following is from an advertisement in one of the London daily papers, the *Standard* of April 14th, 1892:—

> SN NADX.—H vhkk mns rzx vgzs h gzud sgntfgs,—Nq vgzs rvdds sghmfr lzx qhrd tmrntfgs.—He h bntkc nmkx ad pthsd rtqd,—H sghmj h'c cqno tonm sgd ektqd!—AKZQMDX.

It is of very easy construction, each letter being merely one forward in reality from the one here given, so that what is B is really A, what is Y is really W, and so on. It is the poetic effusion of one "Blarney" (AKZQMDX). It read as follows:—

> "I will not say what I have thought,
> Or what sweet things may rise unsought.
> If I could only be quite sure,
> I think I'd drop upon the flure."

In the following from the *Times*, two letters

ahead of the real one are used:—"Ngv og mpqy aqw ctg uchg cpf gcug oa vqtvwtgf okpf," meaning, "Let me know you are safe, and ease my tortured mind."

In another *Times* notice F was substituted for A, G for B, etc. The story involved must have been a very sad one, and much sickness of heart was evident in its appeal. Three days later appeared in the same cipher the intimation, "I know you," evidently the work of some third person, and the correspondence at once came to an end. That this penetration into matters deemed secret must often take place is evident from intimations that one not unfrequently sees that a certain advertisement referred to was not inserted by the person whose name or other sign it bore. We may perhaps be allowed to say here that the illustrations of decipherment we have here given are published examples,[1] that

[1] From an American book of the "Curiosities of Literature" type.

in the case of the third we have foreborne to give the details, and that our strong feeling is that while those who make use of cryptography do it at their own risk, and in some measure may be thought to be issuing a challenge to busybodies,[1] that nevertheless to pry into matters that do not concern one is a base and ungenerous thing to do; that to decipher a communication not intended for ourselves is on a par with reading a letter that may be lying about, listening to a conversation not intended for us, or any other such meanness.

Some advertisements are so abbreviated, as so much business or sentiment has to be got into so narrow a space, that they verge on the cryptographic without any such intention —as, for instance, "so hpy in nw hme, so thnkf an mre hpfl fr yr ftre."

[1] A term a little wanting in accuracy, as used generally to define those who have no proper work to busy themselves with, or who, having it, neglect it to attend to that of others.

Several forms of cryptographic writing may readily be devised, not by changing the various letters into others, but retaining them as they are, a being a, b remaining b, and simply mixing them up with other letters that are merely blinds. Thus we may determine that alternate letters, say the second, fourth, sixth, and so on, shall be the significants, the carriers of the message. For instance, if we desire to send the following communication, "Get away at once," it would read as "Lgpestra rwnapyi astro eniciel." We could break it up into any arbitrary groups of letters or run it all into one; thus it might read, Rgoentlavwxalyvaft Polnjcien. In either case all we should need to do to decipher it would be to run our pen through all the odd numbers and then read off what was left, or put, as done here, a dot under each letter that is to count. It just doubles the length of the communication, a message of thirty letters requiring another thirty to conceal it.

In substitution for this we may make the first letter of the first word, the second of the second, and the third of the third, the significant letters, beginning again at the first of the next, then the second of the following one, and so on. "Get away at once" would then read, "go pey rst al lwn afa yon ta sft of pn loc ei." By this means we have to employ a considerable number of non-significants. This is certainly a drawback, and it would in an especial degree be felt to be so if the message to be conveyed were at all a lengthy one. Such devices, however, have the advantage that the letters employed to spell out the communication are the real letters. There is no need to learn a code of substituted characters, and one is also spared the chance of error that may spring from the use of such a code.

In the far-famed Cocker's [1] "Decimal, Loga-

[1] "According to Cocker," *i.e.*, an accuracy of statement entirely beyond question. The phrase occurs in a farce called *The Apprentice*, and hit the popular fancy.

rithmical, and Algebraical Arithmetick," published in the year 1684, we find, following the preface, a letter in cipher. All the vowels in this remain unchanged; A is A, and E is E, neither more nor less; and if we replace B.C.D.F.G.H.K.L.M.N.P.R.S.T.W.X.Z. by Z.X.W.T.S.R.P.N.M.L.K.H.G.F.D.C.B.— a mere reversal of the ordinary arrangement of the consonants,—we shall find no difficulty in reading the letter. By this code Constantinople would be XOLGFALFILOKNE.

In the *Gentleman's Magazine* for 1761 we find a rather interesting letter from a man who flatters himself that he has devised an absolutely safe cryptogram. He declares that "when the present war was ready to break out, a gentleman, not versed in secret alphabets, but chancing to think upon the subject, happened to hit upon a kind of cipher, the properties of which appeared very extraordinary, not only to him but also to some of his friends not apt to make

rash conclusions. He therefore without delay endeavoured to convey notice of his invention to his late Majesty: judging it might prove advantageous to the Royal Measures during a great and critical war to be waged at once in so many and so removed parts of the world. But this attempt, and likewise a second, had no effect.

"In the meantime some of his friends, solicitous to know the real merits of this cipher, procured that different specimens of it should, together with a brief detail of its properties, be laid before his Majesty's chief decipherer (esteemed the best in the world), requesting that he would be pleased to let them know whether he could or could not read those specimens, and begging his opinion upon the whole affair. The candid artist, having taken due time to peruse those writings, made answer that he could not read them, and that if they actually possessed the properties ascribed to them there could be no doubt

about the importance of such an art. But it was not his business to meddle further in it.

"It occurred to the author, when he had failed of making this art advantageous to the British dominions, that he could easily sell it upon the Continent; and, probably, for a sum not inferior to a large Parliamentary reward, to which many thought it entitled. But upon consulting his principles he found that no crowned head of Europe was rich enough to purchase from him an advantage over the monarch of his own country.

"Thus disappointed both at home and abroad, and reflecting that this secret may happen, by lying by, to be buried with him, he set himself to consider what to do with it, and hath now at length he thinks hit upon the best means of making it useful, and this method is, to publish it to all the world."

A century later, we may parenthetically presume that had the matter got so far as

this, he would have pocketed a handsome sum in promotion money, and been entitled to a seat on the directorate, while the rest of us would have been inundated with prospectuses of the Universal Cryptogram Company, Limited.

He goes on to say that "at first he saw several objections to this step, but they disappeared as soon as the following reasons presented themselves, viz.: First, that the Supreme Wisdom hath locked up every man's secrets, good and bad, in his own breast. Secondly, that human wisdom hath imitated the Supreme, by inflicting punishment on those who unlawfully break open secrets or letters. Thirdly, that after the publication of this art Governments will still have it as much in their power as ever to suppress all suspected writings, while every man's business and private concerns shall be no further exposed in what he writes than he chuses. And this, the inventor imagines, will prove

of singular convenience and advantage to mankind, who daily suffer from the insidious practice of intercepting and counteracting not only private instructions upon lawful business, but even the most important dispatches of nations.[1]

"These are the principal reasons that determined the author to publish this art; but, still diffident of his own judgment, he hath made the two following observations, viz.: First, that in case a true representation of this cipher should speedily be laid before the king; and that his Majesty should thereupon be pleased to command the author to appear and demonstrate the properties he attributes to it, then will the author cheerfully obey, and rejoice in the honour of arming his Majesty's hand with so advantageous a weapon. And he would much rather chuse thus to devote this art to the particular service of his country

[1] Surely in the breast of a patriot these two should be transposed, and the national interest placed first.

than to that of his fellow-creatures in general; For, he is not (as some style themselves) a citizen of the world, nor ever will be, till the world becomes one city. Again, he will never publish this secret till he hath given six months' notice previously of his intention to do so. And, if during those six months gentlemen of sense and knowledge will be so good as to publish reasons proving that more evil than good will result from the publication of this secret, then will the author resolve that it shall be buried with him. For he detests the thought of extending the catalogue of human ills. But, if no sufficient reasons to the contrary shall appear, he will then think it his duty to publish it without further delay. Query then, whether more evil or more good will result from such a publication?

"The properties of the said Cipher. Firstly, it can be wrote offhand in the common characters. Secondly, it can be read at sight.

Thirdly, the secrets both of writing and reading it are so simple that they can, in five minutes' time, be so perfectly communicated that the person instructed shall be able, without further help or any previous practice, to write offhand and read at sight as above set forth. Fourthly, though all the men in the world were perfect masters of the art of reading and writing this cipher, yet could any two of them, by agreement upon a small variation (to be made at will), correspond with impenetrable secrecy, though their letters were to pass open through the hands of all the rest. Fifthly, it is strictly impossible for all the art of man to read it except the reader be in confidence with the writer. N.B.—That the author thinks it may be demonstrated that there never hath been invented, and that it is impossible to invent, another cipher that shall not be inferior to this by many degrees.

"An invaluable advantage of this cipher, in

the hands of a prince, is that he can with ease and expedition write his own letters in it, with no necessity of exposing their contents to ciphering and deciphering clerks, first at home, and next abroad; or to any person whatever, except the individual to whom he writes. Another advantage is, that a prince, master of it, can himself change his cipher every day at will, and make, at the same time, every variation a new cipher, absolutely impenetrable even to those who are masters of this art, and to all human sagacity.

"This art, if judged useful to the crown of these realms, should be first communicated to the king only: that he may be the sole possessor of it, and so have it in his power to disperse it to such of his ministers abroad only as his Majesty shall have occasion to intrust with his most important communications. And the use of it ought to be reserved for such occasions, that it may be communicated to as few as possible, and so be kept

for an arcanum imperii. It should be made death and total confiscation for any man to betray this secret communicated to them by the king; and to the author also, should he betray it after he hath given it up to his Majesty.

"The toil and delays attending the best ciphers hitherto invented are an intolerable clog upon the dispatches of Courts. And we see, by most of the letters taken this war, that it hath been resolved rather to pen them in plain writing than to subject them to such ruinous delays. This cipher is exempt from all such toil and delay. The best ciphers hitherto invented and found fit for business are held, by the best authorities upon the subject, legible by an able artist. And this must be true: For, otherwise, princes would not, at a great expense, keep able decipherers. This cipher is, in every variation of it, impervious to all human penetration. The author hath never yet communicated the art of this

cipher to any mortal; nor indeed ever will, except to the king only, or to mankind in general; unless a dangerous sickness should happen to oblige him to reveal them to a select friend, in order to prevent them being lost for ever."

Whether this were so all potent an instrument as the inventor thought must for ever remain a moot point, as the king evidently did not respond to the advances made, Parliament did not give the large reward hinted at, nor was the Limited Company ever started whereby the secret should be kept inviolate, as he himself suggested, by the whole world being told it. Perhaps the dangerous sickness was too rapid in its progress to allow the summons to the select friend, or in view of the realities of Eternity all mundane objects, even the great cipher itself, may have shrunk into insignificance, or a sudden accident may have befallen him and at once made all notification of his secret a thing impossible.

However this may have been, we have the sufficient fact that all clue to the wondrous cryptogram is for ever lost.

It was long illegal to publish the debates of Parliament. In the various series of the *Gentleman's Magazine* we find "Proceedings in the Senate of great Lilliput" running at considerable length all through the volumes. The names of the speakers are veiled, but at the end of the volume we have an "Analysis of the Names of the Hurgoes, Climabs, etc., of Lilliput," in which both the assumed and real names are given. Hurgo is a Lord, and Climab is a member of the House of Commons; a debate therefore in which Hurgoes Castroflet, Shomlug, Toblat, Adonbring, and Guadrert spoke was really carried on by Lords Chesterfield, Cholmondeley, Talbot, Abingdon, and Cartaret. One can only wonder that such a very palpable evasion of the law should have been thus winked at.

Readers of the weird tales of Edgar Allen

Poe will recall the great use of cryptography in the story of "The Gold Bug," where a Mr. Legrand of South Carolina becomes possessed of an enormous treasure [1] of gold coins of antique date, and great variety, one hundred and ten exceedingly fine diamonds, eighteen rubies of remarkable brilliancy, three hundred and ten emeralds, besides sapphires, opals uncountable, and all by means of an old parchment with some mysterious writing thereon. Should any of our readers up to this point have applied the *cui bono* argument to our book, this good fortune of Mr. Legrand should be a convincing proof of the value of a knowledge of cryptography!

The treasure in question was supposed to be a part of the plunderings of the notorious pirate Kidd. Half buried in the sea sand, in close proximity to a wreck, a piece

[1] "We estimated the entire contents of the chest at a million and a half of dollars, and upon the subsequent disposal of the trinkets and jewels it was found that we had greatly undervalued the treasure."

of parchment was found, and on this some few mysterious markings were noted. On the application of heat this parchment revealed some three or four lines of cryptogram, and the hero of the story sets himself to the task of its decipherment. It proves to be the clue to the burial place of a treasure. The directions, duly followed, bring Legrand and two helpers to a particular tree in the tropic forest, and then at a certain distance and direction from this conspicuous tree a vigorous digging presently brings to light the massive chest which holds this ill-gotten wealth. The piratical vessel was lost and the scoundrels that manned it drowned, and the memorandum found by a mere chance on the desolate shore of Sullivan's Island was the means of bringing to knowledge the hidden booty. The story itself, with its weird accompaniments of skeletons, its midnight delvings, and so forth, can be read at length by those who care to hunt it up in any collection of Poe's works; all that now

concerns us is the cryptograph round which the story turns. This also we need not set out in detail, as it is given in full length in the story. The weak point in it is that it is not at all the sort of cipher that a pirate captain would concoct, while it is exactly what a literary man, with an eye to the possibilities of the printing press, would put together. Thus we find the dagger (†) representing D, the asterisk (*) standing for N, the double dagger (‡) being O. The parenthesis mark, (, is R, and the semicolon (;) is representative of T. The interrogation mark (?), the ¶, and the colon also appear. The message commences in this fashion—

53‡‡†305))6*;4826)4‡

The decipherment of this abstruse memorandum is very well worked out in the story.

That some people still believe in a present and future for cryptography is seen in the fact that so lately as the year 1860 was patented a machine for carrying on secret correspondence.

Probably all our readers must have noticed on their gate-posts or door-steps certain mysterious chalk-marks, the cryptographic symbols of the great begging fraternity, telling their successors what fate their appeal for alms may be likely to meet with. The soft-hearted, and perhaps a little soft-headed, householder who dispenses liberally and without enquiry to the bearers of every harrowing tale need never fear any falling off in the stream of applicants, since the little white mark on his premises will always suffice to bring on a fresh inundation, while the man who finds (or puts) a square mark on his door will be free, for it is an intimation that he is regarded as an unfavourable subject. A circle with a dot in the centre guarantees complete immunity from these uninvited visitors, the immunity that naturally attaches to a man who is prepared to hand any sturdy vagrant over to the police and follow this up with a prosecution.

Business people often employ a kind of cipher for marking prices on their goods and samples when for some occult and mysterious reason it is desirable that the customer should be kept in the dark on the matter. We should have thought that when a man was prepared to sell a proper article at a fair price and profit,—five shillings, for instance,—he would not feel any difficulty whatever in legibly marking it with a good wholesome five that need not be ashamed to look the whole world in the face. If for some reason more or less legitimate, he is unable to do this, all that is needful for him is to hunt up some ten-letter word or combination, such as smoking-cap, in which all the letters are different, and then the letters seriatim will stand for the numerals 1 2 3 4 5 6 7 8 9 0. With this key before us we see that an article marked MG/N will cost us 27/6.

We occasionally find the pushing business man breaking out as a follower of the crypto-

graphic art with the idea of more effectually calling attention to his goods. An energetic dealer in potatoes largely circulated the following offer of a bag of the very best tubers to all who could successfully read its terms. As he was prepared to sell the potatoes at the same price to all comers, whether they read his cryptogram or not, the generosity of the offer is not quite so clear as any one labouring through his circular might have anticipated. The result would probably amuse some and irritate others; but any way it would call attention to the goods, and the dealer evidently concluded that the balance of feeling would be in his favour:—

"Eht otatop nam skniht retfa gnidaer siht, uoy lliw leef taht sih llams elzzup dna ytisoreneg si levon fi ton gnitseretni. Ti sekat emit dna ecneitap ot daer, yltneuqesnoc eht stcaf dluohs eb erom ylmrif detoor no ruoy yromem; siht si eht tcejbo ni gnitirw eseht wef senil. Ew hsiw uoy ot evah a gab fo ruo

seotatop, os taht uoy yam wonk eht eurt eulav fo meht, dna retfa ecno gniyrt meht, i leef erus uoy lliw taeper ruoy redro morf emit ot emit. Sa i wonk eht seotatop era doog i evah on noitatiseh ni gnittup erofeb uoy ym suoreneg reffo: yldnik drawrof xis sgnillihs dna ecnepxis dna i lliw ta ecno dnes uoy eno derdnuh dna evlewt sdnuop fo ym tseb seotatop!!!"

It will be seen at a glance that this cipher is merely the ordinary words reversed in their spelling, and with a very little practice of reading the reverse way one makes it out very readily: "The potato man thinks after reading this, you will feel that his small puzzle and generosity is novel if not interesting. It takes time and patience to read, consequently the facts should be more firmly rooted on your memory: this is the object in writing these few lines. We wish you to have a bag of our potatoes, so that you may know the true value of them, and after once trying them I feel sure you will repeat your order from time to

time. As I know the potatoes are good, I have no hesitation in putting before you my generous offer: kindly forward six shillings and sixpence, and I will at once send you one hundred and twelve pounds of my best potatoes!!!"

We may add parenthetically that the potatoes supplied are excellent in quality, that we had pleasant experience of them long before and after the issue of this cryptogram,[1] and that they are well able to stand on their merits even without any adventitious aid; and the same remark may be made of the excellent "stick-fast paste," which nevertheless is advertised, amongst other ways, as follows: "STI CKPH AST PAS T EST ICKS." As one more illustration of this commercial use of cryptography, we may quote the following advertisement: "My darling, Rof tobacco og ot Nospmoht, ytrof evif, Kciredorf Teerts, Daetspmah Daor."

[1] And that we did not write or suggest this cryptogram!

The process again is simple reversal, and from it the reader will readily learn where, if he be a smoker, he may find due replenishment of his pouch. Such trade uses of the cryptogram are naturally of the simplest nature, and present no difficulty, as the great object is that the person whose eye it catches should be able to readily read the advertisement; to puzzle and baulk him would frustrate the whole intention of the thing.

We have now travelled throughout the centuries from Julius Cæsar and Herodotus to the vendors of potatoes and the makers of paste in this present year of grace; from the victors of Naseby, the fugitives of Culloden, to the shopkeeper of the Hampstead Road. Our rapid review of these hundreds of years has not been, we trust, without interest, and it will at least have shown that the subject has been held of great importance, that it has taken its part in making history, and in the rise and fall of great causes, and that it is something more

and better than a mere shield to the knave or the veiled appeal of the love-struck swain in the columns of the newspaper.

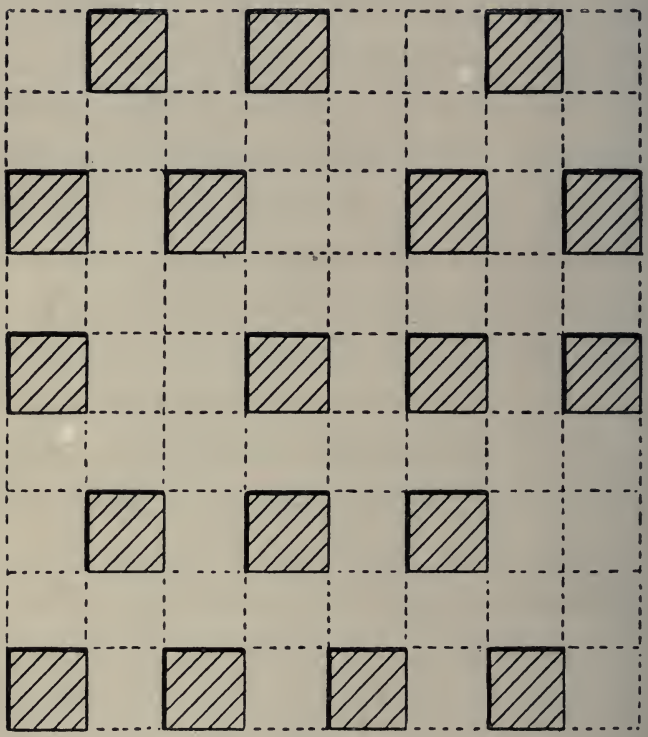


Fig. 15.

We turn now to the practical consideration of divers systems of cryptographic communication, and the first of these is that known as

the "grille." It is a very good method for short communications. The sender and receiver are each in possession of a similar piece of cardboard, and this cardboard is pierced with openings at irregular intervals. The sender then writes his message through these openings on to a piece of plain paper that is placed beneath. He then removes the grille,[1] and fills up the rest of the paper with any other letters or words that occur to him as being calculated to throw any unauthorized third person off the scent. The receiver merely places on the communication his duplicate grille, and reads the message, all superfluous material being to him no distraction, since it is hidden by the unpierced portion of his card. Sometimes the essential message is veiled by the addition to it of other words that transform it into an entirely innocent-looking affair; but this is very difficult to do properly. Any indication

[1] In France, *Le chassis* or *la grille*; in Germany, *Netz* or *Gitten*.

of halting composition or the introduction of any conspicuous word at once attracts attention

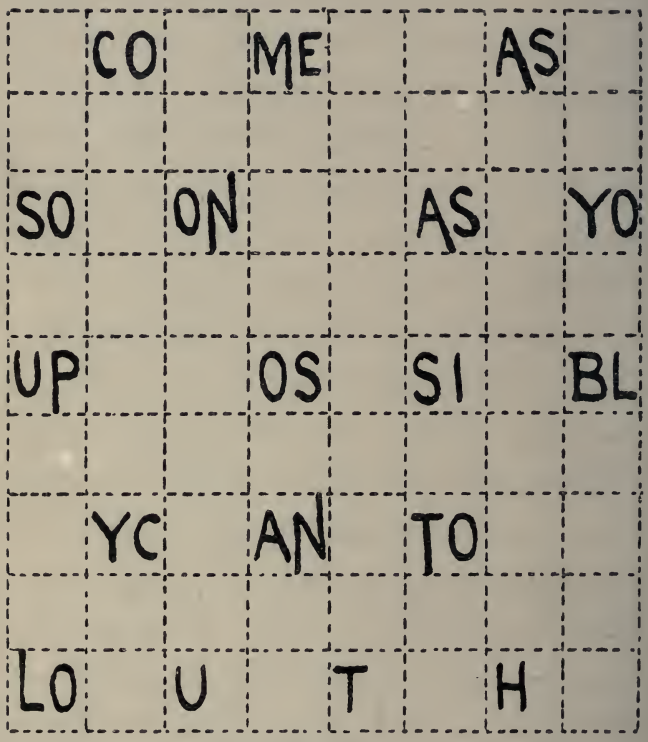


FIG. 16.

and arouses suspicion. "I" and "for" and "with" are easy enough; but if the message runs, "I send five hundred rifles for immediate

distribution, with necessary ammunition," it would require an enormous amount of ingenuity to so wrap round "rifles" and "ammunition" with innocent padding as to make the message read as though it were merely an invitation for lunch and lawn tennis. It is, therefore, better to face the fact boldly that the message is undoubtedly of a secret nature, and then leave the objectionable third person to get such comfort as he can out of it. Fig. 15 shows the pierced card that the sender uses, and of which the receiver holds an exact duplicate. Fig. 16 represents the message, "Come as soon as you possibly can to Louth," as it appears to the receiver when the grille is placed upon it; while Fig. 17 is how it looks when dispatched, and how it reads to any unauthorized and grille-less person. The dotted lines on Figs. 15 and 16 are of course only put that the reader may trace more readily the connection between the different squares: they are of no use in the actual transmission.

If, however, we did not care to risk sending the grille by post or messenger, the second person in the transaction could readily make one

VICOR MERI CASTO

SOREONIC PASYLYO

UPTINNOSP SINEBL

RLYC KANL TOLOIC

LOFTU EST RVH IE

FIG. 17.

for himself or herself, as it would only be necessary to know which squares in each row were pierced. In the top row of the pre-

sent arrangement we see that these are the second, fourth, and seventh. If then we take the first figure to indicate the number of the row, and the others to be the openings, a nought indicating the end of each row, it would be easy to send a formula by which five hundred miles away a duplicate grille, could be made. It would in the present case run as follows: 1247031468021368042460513 57. We have not taken the rows in regular sequence, as the following of 1, 2, 3, 4 and 5 in order after the noughts might suggest an idea to this troublesome third person; but this is entirely immaterial; the different rows are there all the same.

If we have a suspicion that our grille, is known, all that would be necessary would be to turn it upside down, the old bottom edge being now the top one. This at once throws the squares into a new sequence, and gives us a fresh start.

In Figs. 18, 19, and 20 we have a somewhat

similar contrivance, the "revolving grille," though it is perhaps still more puzzling. The grille this time has certain openings made in it

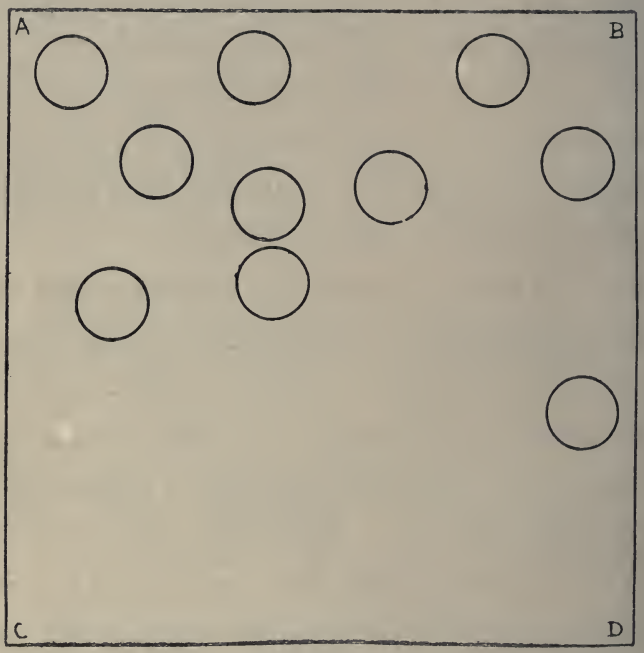


Fig. 18.

(of course we need scarcely pause to say that their shape, round or square, is a very minor point. Sometimes it would be easier to cut a square hole, and sometimes to punch a

round one); but these openings do not, as in the previous example, at once suffice for the whole message. To use this grille, we first

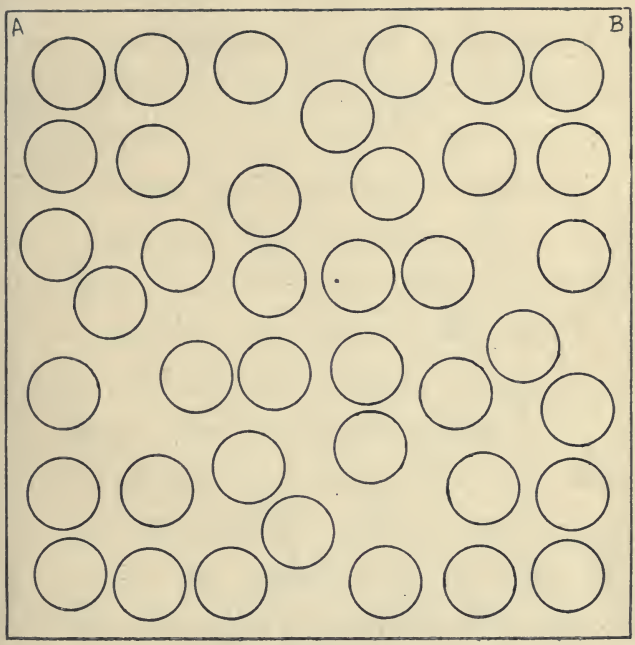


Fig. 19.

place the card so that the edge AB is uppermost, and in these openings we place as many letters as they will take. We then, still keeping our under paper in the same position

turn the grille so that BD is the upper edge, and in these new blanks go on writing our message until these in turn are filled. We then turn the card until DC is the upper edge, and proceed as before, and finally we give it one more turn and bring the edge CA to the top. The ten openings of Fig. 18 thus give us in rotation forty openings, as we see in Fig. 19. The result is a very hopeless-looking mixture of letters, the effect we get in Fig. 20. This Fig. 20 is the communication as the sender dispatches it, as the receiver gets it, and as it appears to all who may see it. To reduce this chaos to full legibility, the receiver takes his duplicate grille and places it, AB uppermost, on the message, and through its ten openings he reads "urgent need." He then turns the grill until BD is the top edge, and the openings now read "only hold ou." The next turn, DC, tells him "t another we," and the final shift of the card to CA as its upper edge reveals now "ck at most JP," and

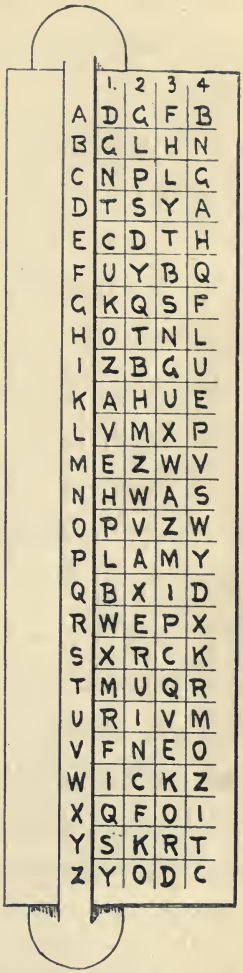
the whole warning stands clearly before him: "Urgent need, only hold out another week at most.—J.P." Fig. 19 is merely added to show how the forty openings made by the revolution

FIG. 20.

of the ten group themselves: the essential figures are Figs. 18 and 20, being the grille used for the message, and the resulting message itself.

We have already in Fig. 9 shown what is technically called the "ladder" cipher, a form made by slipping a card along, and we now have in Fig. 21 another arrangement based on much the same principle, though it works out somewhat differently. To make this form, the "slip-card," we take a long thin slip of cardboard, and then we cut two long longitudinal slits in it, so as to about divide the card into three equal portions. On the centre portion we place the letters of the alphabet in their regular everyday sequence. We then get a broader piece of card and slip this in the slits on the first strip. This second card is divided into squares, and in these squares we place the letters in any irregular way we choose, being only careful that every letter shall appear somewhere in the length of column one, and ditto in the case of all the other columns. About four of these columns will suffice. We now slip the paper along, and place any one of these columns alongside

the alphabet on the thin strip. If we continued to use this column, it might gradually become evident to any outsider what letter stood for A or E, and so on; but we can shift the card as often as we like during the making up of our message, so that E is no longer always C, for example, but at the next shift will be D, and then presently it is T, and so on. The shifting must be intimated to the receiver, or the message will all at once go chaotic to him, so that at the changing point we must indicate by its proper number what column we



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

FIG. 21.

have changed to. These numbers would be 1, 2, 3, and 4, the others, 5, 6, 7, 8, 9, being used as blinds and non-significants, or to separate words.

If then we desired to send the warning, "If you do not return at once it will be too late," it might read, ZU6SPR9TP6HPM2EDUIEW8G U6VWPD3GQ8KGXX6HT5QZZXFQT. The message here begins with column one, at two changes to the second column, and at three to the third.

Figures are at times employed in lieu of letters. It would, of course, be a great deal too obvious that A should be 1, and B 2, and so on; but we may make matters a little more complicated by letting the figures run in the reverse direction, A being 26, B being 25, and so forth, but still this too presents very little difficulty. The following message appeared in the *Times* of September 7th, 1866 :—

"1. 2. 9.—15 22 7, 14 22, 8 22 13 23, 24 12 9 9 22 8 11 12 13 23 22 13 24 22, 4 18 7 19, 9 22 24 7 12 9, 12 21, 24

12 15 15 22 20 22, 11 7, 4 18 15 15, 22 3 11 15 26 18 13, 19 12 4, 7 19 18 13 20 8, 8 7 26 13 23, 18, 20 12, 26 25 9 12 26 23, 13 22 3 7, 14 12 13 7 19."

As the matter is now over thirty years old there can be no objection to pointing out that if we practise this simple reversal, the result stands forth as "X Y R. Let me send correspondence with rector of College; it will explain how things stand. I go abroad next month." Apart from the simplicity of its construction, this cipher is faulty in having always the same equivalent for each letter, and in being cut up by commas into words. These are points that greatly aid decipherment. The numbers too, never running beyond twenty-six, naturally suggest that they are the letters of the alphabet.

Figure alphabets were very commonly used, as we have seen, in the Stuart times. The best arrangement is where each consonant is represented by two combinations of figures, and the vowels by still more. It is better, too,

not to employ single figures, such as 3 or 5 or 8, but to always take doubles, like 22 or 57. The message then runs continuously: there is no need to comma off the words, and every pair of figures stands for one letter. Should it at any time be suspected that the clue is found, an almost impossible thing, a re-shifting of the numbers is readily effected.

The following may be taken as an illustration:—

A. 21, 63, 95, 70.	J. 37, 46.	S. 48, 35.
B. 26, 27.	K. 90, 64.	T. 82, 58.
C. 31, 52.	L. 32, 36.	U. 43, 71, 93, 51.
D. 83, 65.	M. 72, 98.	V. 61, 76.
E. 41, 80, 34, 25.	N. 77, 66.	W. 33, 81.
F. 68, 28.	O. 42, 49, 56, 23.	X. 67, 96.
G. 29, 40.	P. 47, 50.	Y. 89, 97.
H. 22, 30.	Q. 33, 57.	Z. 24, 45.
I. 62, 91, 86, 92.	R. 69, 39.	

This is the sender's list; the receiver's key would have the figures first, and then the figures they represent. This latter would be as follows:—

21. A.	30. H.	39. R.	49. O.	63. A.	72. M.	90. K.
22. H.	31. C.	40. G.	50. P.	64. K.	76. V.	91. I.
23. O.	32. L.	41. E	51. U.	65. D.	77. N.	92. I.
24. Z.	33. W.	42. O.	52. C.	66. N.	80. E.	93. U.
25. E.	34. E.	43. U.	56. O.	67. X.	81. W.	95. A.
26. B.	35. S.	45. Z.	57. Q.	68. F.	82. T.	96. X.
27. B.	36. L.	46. J.	58. T.	69. R.	83. D.	97. Y.
28. F.	37. J.	47. P.	61. V.	70. A.	86. I.	98. M.
29. G.	38. Q.	48. S.	62. I.	71. U.	89. Y.	

This, it will be noted, sets free 11, 12, 13, 14, 15, 16, 17, 18, 19, 20, 44, 53, 54, 55, 59, 60, 73, 74, 75, 78, 79, 84, 85, 87, 88, 94, and 99 for use for any special purpose, such as names of people and places, or anything of such constant occurrence that it would be an advantage to be able to express it by two figures instead of the twelve that would otherwise be necessary to spell out London, or the twenty that Parliament would require. Twenty-seven pairs of figures are thus set free as symbols for anything that may be decided upon between sender and receiver.

Any one sending a dispatch by this code uses any figures he likes from those standing to the

letter he wants; L, for instance, being either 32 or 36, while the receiver, glancing down his key-list, sees that either 32 or 36 are equally L. The prying would-be decipherer is thus at once thrown off the scent. He knows, for instance, that double L is a rather common termination; but when the same letter is represented sometimes by one pair of figures and sometimes by another, he cannot find this double L. "Shall," for example, would read 48223236 or 35303632. He knows, too, that E is the commonest of all the letters; but when it may be 41, or 80, or 34, or 25, his chance of detecting it is but small.

As our readers have the key before them, we hand over to them the following message for decipherment: 22424741268062776923983482304333965218933344190.

By the old method called the "Mirabeau" the alphabet is divided into five rows of five letters each, marked from one to five, and each letter of these rows is also thus

marked. C, for instance, would be the third letter in the first five, and would therefore be $\frac{1}{3}$, while I would be the fourth letter of the second group of five, and would therefore be $\frac{2}{4}$. In practice, however, this regular alphabetical arrangement would be discarded as being too tell-tale. The figures 6, 7, 8, 9, 0 are all non-significants, and the receiver of the message would merely run his pen through them. The number of the row is written as the numerator of these fraction-like symbols, while the lower number is the position of the particular letter in the row. A good workable code would be as follows:— 1 QGALV; 2 DHNRX; 3 BIMSY; 4 PKFUZ; 5 EOTWC. "Constantinople" by this code would read as follows:—

$$\begin{array}{cccccccccccccc} 5 & 75 & 2 & 3 & 5 & 1 & 2 & 58 & 3 & 2 & 5 & 4 & 1 & 5 \\ 5 & 2 & 3 & 49 & 3 & 3 & 83 & 390 & 1 & 38 & 2 & 10 & 4 & 17 \end{array}$$

This is a very good system. It will be seen that it gives good scope for varying the symbols of individual letters; thus the thrice

occurring N of this word is each time represented by a quite different symbol. As an exercise in the same key we hand over the following to the consideration of our students of cryptography :—

$$\frac{3}{4}\ \frac{5}{29}\ \frac{4}{4}\ \frac{5}{38}\ \frac{2}{27}\ \frac{36}{47}\ \frac{5}{18}\ \frac{1}{3}\ \frac{4}{17}\ \frac{3}{1}\ \frac{5}{19}\ \frac{2}{4}.$$

Yet another numerical method is that of Count Grousfield. For this any three figures are taken, as, for example, 431. The message is then written out roughly by the sender, and these figures placed over each letter in the following way: $\overset{4}{C}\ \overset{3}{o}\ \overset{1}{m}\ \overset{4}{e}\ \overset{3}{a}\ \overset{1}{t}\ \overset{4}{o}\ \overset{3}{n}\ \overset{1}{c}\ \overset{4}{e}\ \overset{3}{t}\ \overset{1}{o}\ \overset{4}{u}\ \overset{3}{s}$ We now proceed to write out our message for dispatch, but instead of using C we use the fourth letter from it; instead of O we employ the third letter from it, and instead of M the first letter from it, while for E we recommence by taking in its stead the fourth letter in the alphabet from it. Our message would therefore read GRNI DU SQDI WP YV. Here again it will be seen that the same symbol is

not always associated with the same letter. Thus the twice recurring C is in one part of our communication represented by G, and in another by D, while the threefold O is R, or S, or P, in different parts of the message. Of course, if we took 513 as the recurring number, the letters we introduced into our cryptogram would be in regular sequence the fifth, first, and third from the true ones, and there is, we need scarcely say, no special virtue in grouping the figures in threes, the key might as readily be composed of four or five. Thus we might, for example, use 31042, and our message would then read, C o m e a t o n c e t o u s, the cryptogram based on this key being, FPMI CW PNGG WP UW. The following statement, based on the key of 2130, we pass on to our readers: KM-HSV-FQCQSH-CJFC-LWJ. The system is a very simple and good one, the key being of so easy a nature to remember or to transmit.

In some ciphers the real letters are em-

ployed, but they only reveal their meaning when read in some special way: left to right, and then the next right to left, upwards, or downwards, or diagonally. They are ordinarily, however, not difficult of detec-

T	I	C	E	F	S	P	E	C	N	C	E	P	S	F	E	C	I	T
I	C	E	F	S	P	E	C	N	I	N	C	E	P	S	F	E	C	I
C	E	F	S	P	E	C	N	I	R	I	N	C	E	P	S	F	E	C
E	F	S	P	E	C	N	I	R	P	R	I	N	C	E	P	S	F	E
F	S	P	E	C	N	I	R	P	O	P	R	I	N	C	E	P	S	F
S	P	E	C	N	I	R	P	O	L	O	P	R	I	N	C	E	P	S
P	E	C	N	I	R	P	O	L	I	L	O	P	R	I	N	C	E	P
E	C	N	I	R	P	O	L	I	S	I	L	O	P	R	I	N	C	E
P	E	C	N	I	R	P	O	L	I	L	O	P	R	I	N	C	E	P
S	P	E	C	N	I	R	P	O	L	O	P	R	I	N	C	E	P	S
F	S	P	E	C	N	I	R	P	O	P	R	I	N	C	E	P	S	F
E	F	S	P	E	C	N	I	R	P	R	I	N	C	E	P	S	F	E
C	E	F	S	P	E	C	N	I	R	I	N	C	E	P	S	F	E	C
I	C	E	F	S	P	E	C	N	I	N	C	E	P	S	F	E	C	I
T	I	C	E	F	S	P	E	C	N	C	E	P	S	F	E	C	I	T

FIG. 22.

tion, and we need scarcely pause to give more than one example of them.[1] A better

[1] In this illustration, Fig. 22, taken from a monument in an old Spanish church, the inscription "Silo princeps fecit" can be read in over two hundred different ways, starting from the central S.

way is to wrap the letters up amongst divers non-significants, and resting on some such simple key as that the letters of the message shall be those that follow anything that begins or ends with S. All suspicious-

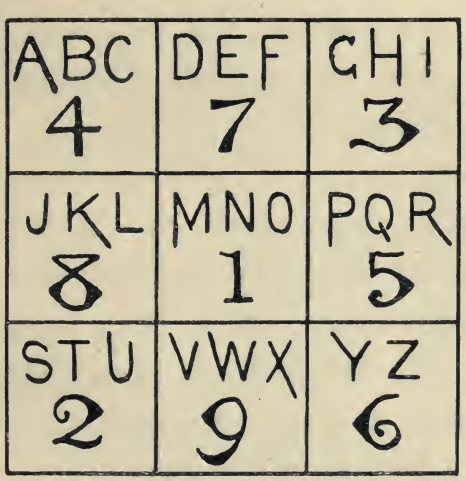


FIG. 23.

looking words should be well broken up. In the following illustration we have taken the intimation, "I will be up in London to-morrow"; and to make it clearer to our readers, we have put the message itself in

a different type—though that is, of course, in practice, the very last thing we should do—si *i* tels *wi* fet so *ll* sigh *be* o sigh *u* far sign *p* has *in* smu *lo* peps *ndo* ri s *n* see *tomo* ss *rr* ped sip *ow* ex.

The arrangement seen in Fig. 23 has sometimes been employed, and as it is one fairly good system the more to add to our store, we give details of it. At the same time, it is by no means so good as some of the others we have dwelt on. A square is drawn, and each face of it is divided into three equal parts. From these lines are so drawn that the big square is subdivided into nine small ones. In the first of these we place A B C, in the second D E F, in the third G H I, and so on in regular sequence, until all our squares are lettered. We then place, also in each square, any one number from one to nine, disposing them in an entirely irregular and casual way. In our present example it will be seen that these

numbers run as follows: 4.7.3.8.1.5.2.9.6. In this key a plain 4 stands for A, a once-dotted 4 for B, and a twice-dotted 4 for C, and so on all through. South Kensington

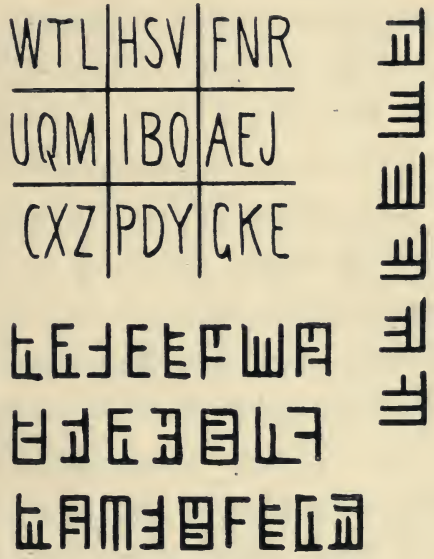


Fig. 24.

Museum would by this system appear as 2ï2ä23ö8ü7ï23ï32ï1ï01ä22ü21. In sending the key it would only be necessary to send 473 815296, as the receiver would then place the alphabet in the nine squares he would thus

number. If any treachery or underhand work were suspected, one would merely substitute 965213874, or any other fresh combination.

If two persons provide themselves with a copy each of the same edition of a good dictionary, they may be able to communicate with each other in cryptogrammic fashion, though the method is only available for fairly common words, and is of no use for proper names. The method is to write down not the word itself, but whatever word one finds a certain number of places back or forward. Thus, desiring to send off the warning, "Get away soon as you can," we use, instead of these words, those that we find in our dictionary three places behind them. So that our message reads, "Gesticulator awakening sonneteer artless yolk camphor."

The system shown in Fig. 23 is ingenious, and so is that shown in Fig. 13; but we have in thinking them over devised our-

selves a combination of the two, to which we will give the name of the Newark cryptogram, that we think is an improvement on both. For the dots of Figs. 13 and 23 we have substituted lines, as being somewhat clearer and more definite. It seems to us that it is rather a weak point in Fig. 23 that the second letter has one dot and the third two. In Fig. 24, the Newark, we have got rid of the X-like cross of Fig. 13, and have grouped our letters into threes, as in Fig. 23, the odd space over being given to a second E. Having got, as in Fig. 13, various arrangements of right angles, the one, two, or three lines may be disposed in them in any direction we please. The six characters in the vertical column are all, for instance, variations of the letter L, though they all agree in the essentials in having the right angle, and within it three lines. By this method, therefore, with a little ingenuity, we need scarcely repeat any form, and we may

get the twenty-six letters of our alphabet represented by over two hundred different symbols. W being the first letter, is represented by one line, T by two lines, and L, the third letter, by three lines; all being represented within a right angle of the same direction. F is the first letter, and therefore one-lined; N the second, and therefore two-lined; R the third letter, and therefore three-lined, in a right angle of the reverse direction.

In Fig. 25 we have a representation of the "clock-hands" cipher. It is less effective as a cryptogram than some of the methods that have preceded it, since all its values are constant—the same forms always representing the same letters, except in the case of the threefold E—and therefore rendering it more easy of analysis and ultimate detection. One great advantage of it is that the forms are so simple in character and so distinctive: it is, therefore, a very easy cipher to write or

read. The dots are absolutely meaningless, and are merely put at random as blinds. The intimation given beneath the alphabet in Fig. 25 is as follows: "Clock-hand cipher is simple in character."

Fig. 25.

The "two word" cipher is a very good one, the same letter being represented by different characters. To work this out, we take any two words of reasonable length and place them, one along the upper edge of a series of ruled squares and the other down

one side. In these squares we place the letters of the alphabet in regular sequence until all the squares are filled. The words (see Fig. 26) that we have selected are "ordinarily thoughtful"; this, therefore, will mean ten squares wide and ten deep, one hundred squares altogether: so that we get the alphabet repeated in full three times, and only four letters short of a fourth. We see now, by referring to E, that it may be either NT, OU, RH, or DU, while double S would be LH, NG, OF, or RL at pleasure. Of course, by taking more squares still—that is to say, longer key-words — still more combinations could be made, but the present number is really ample. There is no necessity that the two key-words should be of equal number of letters. "Ordinary thought" would have given us fifty-six squares, and that would have meant that the alphabet would have come twice over, and a few letters thrice. It is by no means necessary that the key

letters should be words at all; one might simply adopt any chance arrangement of letters in their place. The words are only useful as

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

FIG. 26.

being easily remembered should the key be mislaid and a new one have to be made. It makes transmission of the key easy also. If

we send to our correspondent the words "ordinarily thoughtful" on a post-card, no suspicion is aroused, and he at once proceeds to make his key, so many squares wide and so many deep, and then fills them in with the letters of the alphabet. Each real letter of the message is represented by two letters in the cryptogram; so that the receiver, on getting the message, takes a pencil and proceeds to cut up the communication at each pair of letters with a little upright line, and then, by the aid of his key, translate it into ordinary wording. The specimen message we append is, "Hope to be with you by Tuesday"—ITNHRGDU YHOG RTOU LGNUAGIT RFRTDFOT IHRF YHRGRHLHITRORF. The same message might be given in quite different characters; thus the "hope" might equally well have been IUOGILNT. Whether there be such a thing as an absolutely indecipherable cipher one cannot say, but this "two word" combination must come

sufficiently near that ideal for all practical purposes.

The subject is by no means exhausted, but enough has been brought forward, we trust, to justify in the first place our plea for the historic interest of cryptography, while the examples we have given are a testimony to the abundant ingenuity that the art has called forth. While the art of secret writing may be turned to the basest uses, to many it should be a source of innocent recreation and an ingenious form of puzzledom; while its value in time of peril is such that a knowledge of it may save hundreds of lives, or avert catastrophe from the nation itself.

INDEX

"So essential did I consider an Index to be to every book, that I proposed to bring a Bill into Parliament to deprive any author who published a book without an Index of the privilege of copyright, and, moreover, to subject him to a pecuniary penalty."—*Campbell's "Lives of the Chief Justices of England."*

Butler & Tanner, The Selwood Printing Works, Frome, and London.