


www.forgottenbooks.com

Copyright © 2016 FB &c Ltd.
All rights reserved. No part of this publication may be reproduced, distributed, or transmitted in any form or by any means, including photocopying, recording, or other electronic or mechanical methods, without the prior written permission of the publisher, except in the case of brief quotations embodied in critical reviews and certain other noncommercial uses permitted by copyright law.

# CRYPTOGRAPHY

BY

ANDRÉ LANGIE

TRANSLATED FROM THE FRENCH BY

J. C. H. MACBETH

AUTHOR OF "THE MARCONI CODE," "MARCONI DICTIONARY," ETC.

HOWELL C. BROWN W6BPU-WLVS
120 North El Molino Avenue
PASADENA, CALIFORNIA
Return Postage Guaranteed

CONSTABLE & COMPANY LIMITED
LONDON BOMBAY SYDNEY
1922

PRINTED IN GREAT BRITAIN

# PREFACE

I HAVE no intention of writing a complete manual of cryptography. Finality, even very relative, is not attainable in the domain of this art. Besides, good manuals are in existence on this subject, and the titles of some of them will be found at the end of this volume.

A cryptographer of considerable experience, however, can always add a few details even to the most complete works of this kind.

My object in writing this book is simply to explain what cryptography is, and to recall what it has been from antiquity to the present day; in short, to relate my experiences as a decipherer.

The first part of the volume contains a description of the principal systems of cryptography, together with a note on the rôle played by cryptography in history.

In the second part I relate how I succeeded in deciphering a dozen cryptograms of various kinds. In some chapters of this section I give the texts just as they came into my hands; but in the majority of cases, though preserving the system of cryptography actually employed, I have, on grounds of expediency, substituted an approximate reading for the actual text, and have modified the plan, and even radical features of the narrative, in such a way as to render abortive any attempt at identification and localisation.

878967

In the third part I give some advice in a general way on lines which have proved profitable to me, and, further, a certain number of tables and formulæ; but while I recognise these to be very useful, too much reliance should not be placed on them, under penalty of striking the wrong track, as I shall have occasion to repeat farther on.

In point of fact, as I have found by experience, in cryptography the exceptions are infinitely more frequent than the rule.

---

# TRANSLATOR'S PREFACE

I have to acknowledge with grateful thanks the valuable assistance I have received in preparing this work from the late Mr. W. Jarvis, Lieut.-Commander W. W. Smith of Washington, U.S.A., Mr. Albert M. Smoot of the Ledoux Laboratories, New York, and Miss A. Wishart of the Radio Corporation of America. It was not an easy task substituting English text for the examples of ciphers in French, and if there are any errors which have inadvertently escaped detection I humbly beg forgiveness.

J. C. H. MACBETH.

# CONTENTS


PAGE

## PART I

DESCRIPTION OF THE PRINCIPAL SYSTEMS OF CRYPTOGRAPHY, WITH HISTORICAL NOTICE - - - - 1

## PART II

EXAMPLES OF DECIPHERING - - - - - - 47

## PART III

LISTS AND TABLES - - - - - - - - 122

BIBLIOGRAPHY - - - - - - - - - 158

## PART IV

THE PLAYFAIR CIPHER SYSTEM, ETC. - - - 159

# ACKNOWLEDGMENT

OUR thanks are due to the following gentlemen in connection with translating the book from the original French, working out and substituting English "Examples" for the French ones, adding additional matter, and seeing the work through the Press:

Mr. J. C. H. Macbeth.
The late Mr. W. J. Jarvis.
Mr. H. G. Telling.
Commander Smith, U.S.N.
Paymaster-Commander J. E. A. Brown, C.B.E., R.N.

THE MARCONI INTERNATIONAL CODE CO., LTD.,
MARCONI HOUSE, STRAND,
LONDON, W.C. 2.

*25th July*, 1922.

# CRYPTOGRAPHY

## PART I

## DESCRIPTION OF THE PRINCIPAL SYSTEMS OF CRYPTOGRAPHY, WITH HISTORICAL NOTICE[1]

### I.

EVERYONE has, at some time or other, used cryptography,[2] or secret ciphers.

Who has not had occasion to make some note, or to correspond with somebody, by dotting letters in a newspaper or book? Even children amuse themselves in this way on their school desks. But a pen or pencil is not necessarily required to make use of a secret language.

More than one of us, in our young days, have been embarrassed by a question from the schoolmaster. We have been required to give a proper name in answer, but it is precisely this proper name which has slipped our memory. So we have glanced at a comrade with whom we had previously come to an understanding. And the latter passes a finger over his *h*air, his *e*ar, his *l*ips, his *e*ar, and his *n*ose, whereby we understand "Helen." We have thus corresponded by means of mimetic cryptography.

What is cryptography, after all? Cryptography is the art of recording one's thoughts in such a way as to

[1] This Part I. appeared in the *Bibliothèque universelle et revue suisse* in August, September, and October, 1917.

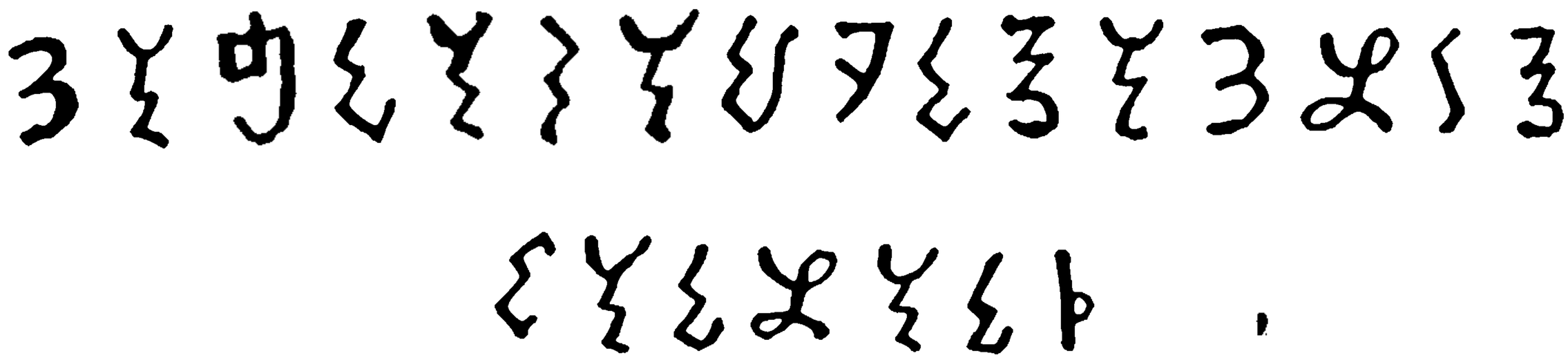
[2] From the Greek words κρυπτός, secret; and γράφειν, to write.

make them unreadable to others. Particularly, moreover, it enables two persons to correspond under cover of complete secrecy—at least in theory. A man will perhaps invent, on his own account, a system of writing by means of which he can write and preserve secrets which he prefers not to divulge, while ensuring the possibility of reading them again at any time.

The great thinker, Alexandre Vinet, composed a system of cryptography which was as simple as he was noble-minded. He used it to note in his diary his qualms and trials. The phrases he wrote in this way can be read almost at a glance.

The celebrated Swiss physiognomist, Jean-Gaspard Lavater, in his *Diary of a Self-Observer*, constructed several systems of secret writing to preserve his private reminiscences. These passages, which are omitted from the new French translation, are far more difficult to read than those of Vinet. Eight years after his death his countrymen had not succeeded in deciphering them all.

Some years ago I was asked by a friend, a professor at a university in German Switzerland, to decipher a piece of yellow paper, covered with strange characters, found among the records of a Swiss politician, a contemporary of Napoleon I., and which was supposed to have some historical importance. Here is a specimen, a part of the first line and one word of the sixth:



My friend had consulted his colleagues: one had declared it was not Sanscrit, another that it was not Ethiopic, and still others that it was neither Slavonic nor Runic. These professors spoke truly, for it was French!

This system was one of the easiest to decipher. There were some 800 signs in the text. One of the signs, the second in the above example, and the most frequent, occurred something over ninety times, while another, the fourth, occurred seventy times.

Now it is well known that in English, French, German, and most languages of Western Europe, the most frequently occurring letter is *e*; the letter which follows is, in French, *n* or *s*, according to the writer; in German, *n*; in English, *t*; in Italian, *i*; and in Spanish, *a*. In Russian the most frequently occurring letter is *o*, but *i* if the language is written in Roman characters. In Polish the most frequent consonant is *z*; not uncommonly three may be found in the same word. In Arabic and Turkish the letter ؛, *elif*, corresponding to the French stopped or silent *h*, occurs oftenest. In Chinese—at least, in the newspapers—the characters found in order of frequency are 之 (*chi*, of, genitive), 不 (*puh*, not, negative), and 工 (*kong*, work). To ascertain which letters occur oftenest in any language, one must "calculate frequencies."

The next thing to do is to study which letters most commonly adjoin. They are *es* in French and *en* in German. The most frequent groups of three are *ent* in French, *the* in English, *ein* in German, *che* in Italian, etc. Bulky works have been written on this subject containing long lists, more or less complete, of the various articulations and disarticulations of words. Of course, this requires an enormous amount of labour, involving a

statistical study of texts containing many thousands of letters.

To revert to our example, I encountered a difficulty at the first onset. The sign which came second in order of frequency, and which I supposed[1] should represent either *n* or *s*, caused me some embarrassment.

At last I abandoned the books I had been using, and began a new calculation of the frequency of letters in certain authors and French newspapers. In the letters of Voltaire I noted that the letter *u* occupied the second place in point of numbers, this being obviously due to the fact that the words *nous* and *vous* ("we" and "you") are common in the epistolary and conversational style.

In the sixth line of the document, a group of signs offered the peculiarity of conjoining twice in succession the two most frequent characters, the supposed *e* and the supposed *u*, separated by another sign and followed by one occurring rather rarely. Accordingly a new trial was made, which this time proved satisfactory. These signs might imply the tail of the word *valeureux* or the words *peureux* or *heureux*. This last proved to be correct.

Among the first signs of our example, the supposed *e* occurs preceded by the supposed *u*. In French, *u* followed by *e* occurs principally in the syllable *que*. It could not be the word *lequel* here, the sixth sign not being similar to the first. The group must read: *Ce que*. A little farther on we meet again with the sign representing *c*, followed by the *r* of the word *heureux* and preceded by *e*, a group of letters which might, for instance, form the words *écran*, *décret*, or, better still, *écrire*.

[1] The decipherment is based not only on statistics, but also on hypotheses. In fact, the famous expression, "Suppose that . . .," is the motto of the cryptographer

The result of the deciphering showed that there was no question of a conspiracy in this mystical writing, but of the enthusiastic sentiments inspired in the author by some charming person met at a fashionable party. It was, perhaps, the rough draft of a letter. The first phrase, translated, was as follows:

"What I am writing you here is merely to relieve my heart, since I am writing to the dearest object in my life to divert the frightful restlessness of my days. . . ."

And so on for twenty-five lines.

Cryptography has provided an entertaining field for novelists. They produce heroes who mark in secret writing the route to be followed in order to recover a fabulous treasure or to track the author of a crime, or perhaps learned men who reveal some stupefying discovery.

We have all read the story of the *Gold Beetle*, by the American novelist, Edgar Allan Poe. It will be remembered that, in order to recover the wealth buried by Kidd, the pirate, it was necessary to let the gold beetle fall from the left orbit of a skull attached to the highest branch of a big tree, and to extend by fifty steps a line leading from the foot of the tree and passing through the point where the beetle fell. A hole was dug at the spot reached, and, of course, an incalculable treasure unearthed.

Who has not read, also, Jules Verne's *Jangada?* And who has failed to be interested in the researches made by the Judge Jarriquez into a Portuguese document in secret writing in order to save the life of an innocent victim condemned to death?

In *A Voyage into the Interior of the Earth*, also by Jules Verne, we see a Danish scholar intent on piercing

the mystery of a cryptographic parchment which is to reveal the route to be followed in order to penetrate into the depths of our terrestrial globe. But old Professor Lidenbrock seeks too far, and it is his nephew Axel, a careless young man, who attains the object simply enough by reading the finals of the lines backwards.

It may be pointed out that the system deciphered by Edgar Allan Poe is comparatively simple. He himself acknowledges this, and claims to have deciphered keys[1] "ten thousand times" more arduous. The system conceived by Jules Verne in his *A Voyage into the Interior of the Earth* is also very easy. As to that in *Jangada*, the problem is solved, thanks to an incredible combination of favourable circumstances.

In one of the latest novels of the Arsène Lupin series, *The Hollow Needle*, Maurice Leblanc has the idea of uniformly substituting the consonants of a document by dots. Nothing can be said of this system, except that it is ultra-fantastical.

A final example, and this time historical: the poet Philippe Desportes wrote in cipher the life of Henri III., King of France. If this work had come down to us and been deciphered, probably not many edifying subjects would have been found therein. But it was burnt during the troubles of the Holy League.[2]

Some months ago I received a letter from a foreigner, who informed me that he was very interested in cryptography, and that he wanted to work on some official texts. He begged me to lend him some diplomatic documents, of which he would take copies for his use

[1] The 'key'" in cryptography is the formula which enables a text in cipher to be read.

[2] Henri Martin, *Histoire de France*, vol. ix., p. 472, note.

and return me the originals. "You do not know me," he wrote, "but you can rely on me entirely: I am *neutral*."

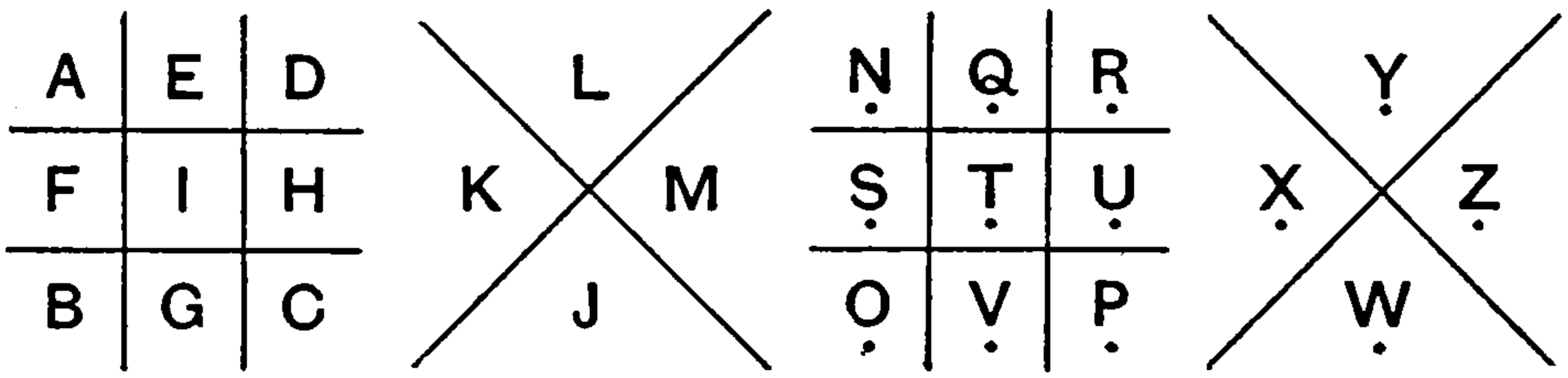
Despite this excellent recommendation, I had nothing to communicate. However, touched by his candour, I gave him some advice. Living in a large town, he had at hand a mine of small cryptograms: he had only to look in the windows of the curio dealers and antiquaries, take note of a number of prices marked in secret characters, and try to decipher them. It is a cryptographic exercise as good as any other. There are certain methods which enable one to guess which letter means 5, which 0, which 9, etc.[1] I refrained from pointing them out to him, since the value of these exercises lies precisely in finding out these methods for oneself. I wonder whether he followed my advice, which I consider was good.

We were just now recalling some specimens of secret writing where the key was in the hands of only one person. Let us now consider another order of cryptography, which enables two persons to correspond under shelter of secrecy. We will leave aside the various sympathetic inks, the employment of which affords no security, whether used on paper, or, as has often been seen in the course of the present war, on the skin—that of the arms or back—since a simple chemical reaction exposes them immediately. Conventional or shuffled alphabets alone are of any use.

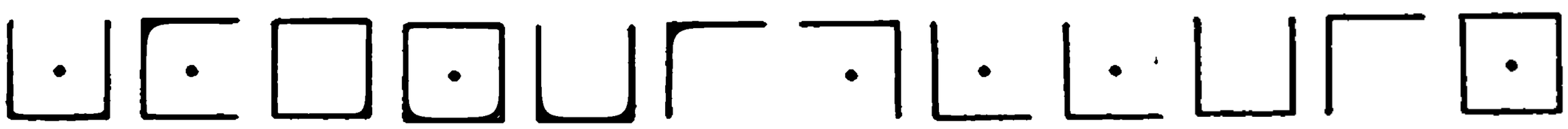
An example of a cryptography widely in vogue in the

[1] NOTE BY TRANSLATOR.—This is for decimal currency. In ciphers representing £ s. d., the same methods would first disclose 6, 1, and 0.

Middle Ages is furnished by the so-called alphabet of the Freemasons, of which the following is a specimen:




The following words will be read without difficulty:

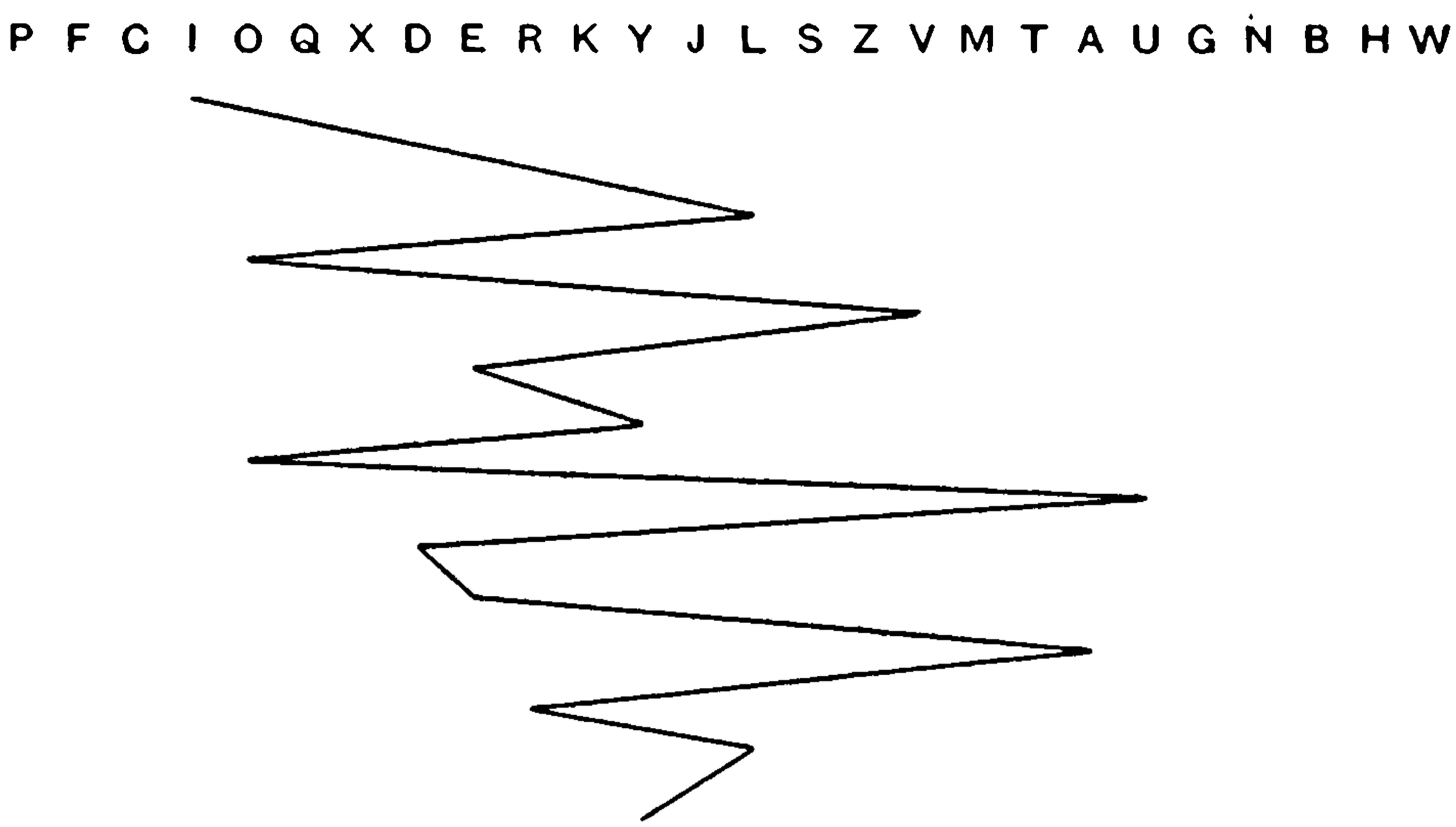


By writing the alphabet in a different order, the values of these angles and squares may be altered at will.

In December, 1916, I was given a bundle of papers in Spanish cryptography to decipher. It was a private correspondence written in the above system, a little complicated: there was not only one dot, but two or three in most of the letters.

Among many other ingenious systems may be mentioned that known as the "zigzag," which is constructed thus: Take a sheet of paper ruled in squares, and write along the top of the vertical columns the whole alphabet in any order you like. Having done this, superpose on the page a sheet of tracing paper, on which mark a dot in the vertical column headed by the letter required, taking care not to mark more than one dot at a time in each horizontal line. The dots once marked, you join them by zigzag lines, and send your correspondent the drawing thus obtained.

An inquisitive intermediary would see nothing in it, especially if the document were brief, whereas the recipient will place the message received on to a graph similar to that of the sender, and will have no difficulty in deciphering:



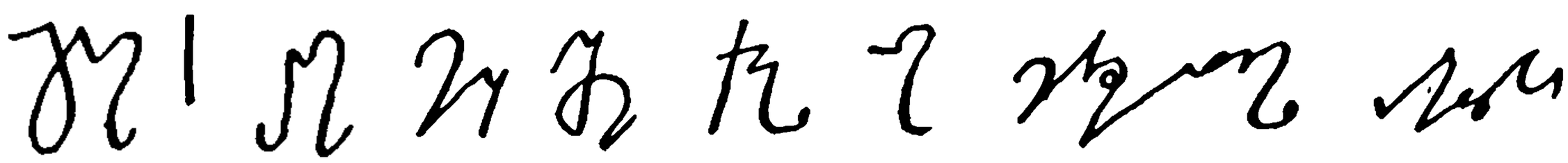

"I love you dearly."

He (or she) will reply in the same way, or perhaps by means of a thread. This is laid along the cipher alphabet, beginning on the left, and wherever the thread passes a letter required, it is marked in ink. Arrived at the right extreme of the alphabet, the thread is moved a section, and a new start is made from the left, and so on indefinitely until all the letters required have been marked. Thus, to write the words "I reciprocate" would require something over seven sections of the thread, each corresponding to the length of the alphabet.[1] This method

[1] It is needless to say that if the zigzag contains fifty angles and the thread bears fifty marks, a decipherer could discover the key of both.

of corresponding is very ancient. It is some 2,300 years since Æneas, the tactician, recommended a similar system in his *Poliorcetes*.[1]

Shorthand is not the same thing as cryptography, of course; it is not a secret writing, seeing that hundreds of thousands of persons can make use of it. Nevertheless, an artful mind can combine shorthand and cryptography in such a way as to form a fairly complicated secret writing. In 1913 I was handed several dozen pieces of paper which had been seized at a penal establishment in French Switzerland. They were covered with shorthand-like characters which had resisted the efforts of several professional shorthand writers. Here is a fragment:



It was the correspondence of two bandits, authors of robberies on a high scale, who were interned at the two extremes of the prison. They had transmitted their missives by means of a very well organised postal service. Their letter-box was purely and simply the backs of the volumes lent them by the prison library. They had agreed in advance as to what books they would borrow, and each found the letter of the other by opening the book wide, which allowed the little piece of paper concealed in the hollow space in the back of the binding to fall out.

They had other hiding-places all ready in case of alarm. Their alphabet consisted of more than 200 different signs.[2] I will dwell a moment on the contents of these

[1] Chapter xxxi.

[2] The method of deciphering applied here was to calculate the frequency of the various lines and curves.

messages in order to show the usefulness of a safe form of cryptography.

These two bandits, M. and S., had drawn up well-schemed plans of escape, and were on the eve of carrying them out when the unforeseen contingency of the deciphering occurred. They had organised their future movements, and projected the burglary of a jeweller's shop in an important Swiss town in order to get on their feet before proceeding to effect a gigantic coup at a jeweller's in the Rue de la Paix, Paris, or in Regent Street, London.

"Take the small cases," wrote M. to S., "but never jewels displayed on velvet trays, for jewellers have a trained eye, and can at a glance detect whether any piece is missing from a tray. The large dealers always have an assistant concealed in a corner, whose duty it is to keep his eyes fixed on a mirror in the ceiling, enabling him to watch most of the shop without the knowledge of the customer. When you go into the shop, find out, without attracting attention, where this mirror is situated, and operate outside its radius of reflection."

Some further advice followed:

"I should work in first-class railway-carriages: operate on solitary individuals, but never with a dagger, you understand; nor with revolver or chloroform. Hypnotism at all times and everywhere. So lose no time in taking lessons in hypnotism as soon as you have left this enchanting resort."

M., who had a taste for mental pursuits and was well read, mingled the practical advice which we have just read with philosophical considerations on perfect friendship, on Schopenhauer and Nietzsche, on the destiny of the soul, etc. Occasionally there is a postscript: "Ask our worthy chaplain to borrow my fountain-pen for you.

I will conceal a watch-spring in it, toothed like a saw, and you can begin on filing the bars of your cell, for we shall have to be out by the end of the month." He further writes: "Not one out of a hundred shorthand experts in Berlin—not one, I repeat—would be capable of reading my system *Sto*. So it is still more likely to remain a sealed book in French Switzerland."

The example given above in facsimile means: "Be on the alert! The pincers will be put behind the window-sill this afternoon." Its actual reading is: "Achtung! Zange wird nachmittags am Fenstersims hinterlegen." For this correspondence took place in German. I have chosen this phrase from a sample which begins with a succession of oaths of no particular interest for us.

## II.

As we have seen, cryptography is of service to private individuals—that is, to certain private individuals—but its main usefulness lies in furnishing a means of correspondence between heads of States, Ministers, and Generals. In wartime, especially, by its aid plans of action and secret information can be communicated, relief asked for, etc. Cryptography, when employed for diplomatic or military purposes, is termed "cipher," whether it be in the form of ciphers or figures, letters, or any other signs. Obviously, when war conditions prevail, only Government departments and military authorities are in a position to utilise cryptography,[1] which is of incalculable value to them.

[1] The author should have said "legitimately." It is a matter of common knowledge that numberless attempts were made by spies to convey information to the enemy by means of more or less ingenious ciphers. In most cases these attempts were foiled by the ingenuity of the expert staff of cryptographers employed in the various Cipher Departments.—TRANSLATOR.

## III.

The origin of secret writing is lost in the mists of antiquity. To go back only to 500 years before the Christian era, we find this record: "When Xerxes planned to invade Greece, a Greek named Demaratus, a refugee at the Court of the King at Susa, warned his countrymen of Lacedæmon by means of a message traced on wooden tablets covered with wax. At first nothing could be seen on them, and it was Gorgo, the wife of Leonidas the King, who discovered the stratagem."[1] The Carthaginians made use of a similar process, which seems to indicate the employment of sympathetic ink.[2] Herodotus[3] has recorded for us a not very practical system which was once employed in the East. "Histiæus, tyrant of Susa," he tells us, "wishing to communicate to Aristagoras, his lieutenant at Miletus, the order to revolt, could find only one way, all the roads being guarded. He had the head of his most trustworthy servant shaved, made some incisions in the scalp, and waited till the hair grew again." (The era of the telegraph had not yet arrived!) "As soon as this occurred, he sent the man to Miletus without giving him any further instruction than, on his arrival, to invite Aristagoras to shave his head and scrutinise it. Now, the incisions formed the word 'Revolt' (Ἀπόστασις)."

This rather slow means of correspondence was not in current use. At the same period the Spartans had a far better system of cryptography, the *scytales*, of which

[1] Herodotus, VII. 239.
[2] Aulu-Gelle, *Nuits attiques*, XVII. 9.
[3] V. 35.

Plutarch,[1] among others, has left us a description. The scytale was a cylindrical rod round which the sender of the secret message rolled a long band of papyrus in a spiral, after the fashion of the emblems which cover reed-pipes. On the wrapper thus formed he traced the words lengthwise along the rod, taking care to write only one letter at a time on each fold of the ribbon of papyrus. Once unrolled, this showed nothing but a meaningless succession of separate letters. The recipient rolled the band round a rod of the same length and diameter as that of the sender. The slightest difference in the diameter of the two rods made the reading of the message practically impossible.

To give an idea of the difficulty involved in deciphering these scytales without having the proper rod, or with a cylinder of a size dissimilar to that of the sender, it may be stated that twenty letters can be combined in 2,500 billions of different ways. A decodist who applied himself to discovering the meaning of a document thus transposed, and was so expeditious as not to devote more than one second to the scrutiny of each combination, would reach the trial of the final arrangement of these characters at the end of 75,000,000,000 years. If chance favoured him, he might hit upon the solution at the thousand and first or ten thousand and first trial, or it might happen that he would have to persevere to nearly the end, or, worse still, he might encounter the solution without knowing it and stopping there.

Nowadays, however, there is a process which enables us to decipher these ribbons of papyrus comparatively easily, even without being in possession of the desired

[1] *Life of Lysander*, ch. xix.

cylinder. Let us suppose that one of these messages has fallen into our hands, and that its twenty-five centuries of age have left it preserved in its original state of freshness. We begin by making an exact copy, which we shall manipulate in our own way, bearing in mind always to leave the originals intact. From one of the ends of this copy let us cut off, say, three fragments, each containing ten or a dozen letters, or more or less if we like. We place these segments one beside the other in the order in which we have cut them. This done, we slide the second along the first, either up or down, and the third along the second, endeavouring to form possible syllables or fragments thereof. (Assume, for convenience, the document to be in English.) Let us suppose that after various adjustments our attention is fixed on the following combination:

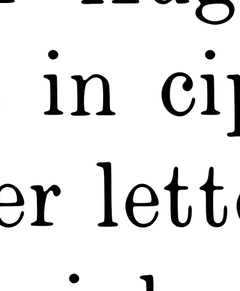
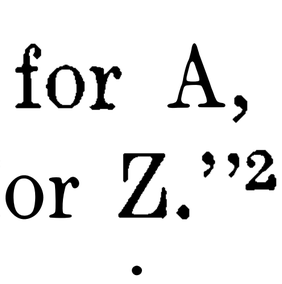
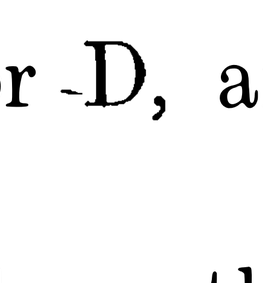
| | | |
|---|---|---|
| D | | |
| E | | |
| E | B | |
| A | R | |
| W | I | L |
| T | T | H |
| | I | N |
| S | | P |
| | | P |
| | | L |

We observe that of the two groups of three letters, W I L is capable of forming a part of the word *will* or *wild*. To test this, we refer to the original scroll to count the intervals between the three letters in the group, and find that I is the eleventh letter after W, and L the eleventh after I. It now becomes obvious that if the eleventh letter after L is another L or a D, we are on the right track. The trial proves this to be the case by yielding L. We now make a new copy of the papyrus and cut it into segments of eleven letters, which we place one by one to the right, the result being that the document becomes an open page to us, thus:

| | | | |
|---|---|---|---|
| D | | | |
| E | | | |
| E. | B | | e. o n. y o u r. g u |
| A | R | | d. t h e. e n e m y. |
| W | I | L | l. a r r i v e. a |
| T. | T | H | e. f r o n t i e |
| r. | I | N. | a. w e e k. a n d. |
| i | S. | P | l a n n i n g. t |
| | | P | |
| | | L | |

Drawing nearer the Christian era, we are told by Suetonius, the biographer of Julius Cæsar, that the latter "employed for secret matters a sort of cipher which consisted in writing, instead of the required letter, the third letter from it, as D for A, and so on."[1]

"The Emperor Augustus," says the same historian, "when he writes in cipher, puts B for A, C for D, and so on for the other letters, and AA for Z."[2]

Julius Cæsar's cipher is still in use in our day—that is to say, it remains in principle, but with complications which make it much harder to decipher. Alfred L, King of England, and Charlemagne also used cryptography for corresponding with their officers. I do not think I am violating a diplomatic secret, a thousand years having elapsed, in revealing that in Charlemagne's secret writing  meant *i*;  *d*;  *l*,

[1] *Cæsar*, ch. lvi.

[2] *Augustus*, ch. lxxxviii.

etc.[1] The Governments of Venice, Florence, and other Italian republics made use of secret writing from the thirteenth century.

Since the Middle Ages numerous investigators have pondered over an ideal system of cryptography. Among them we may mention Francis Bacon, the philosopher, and Blaise de Vigenère, the French diplomatist, whose ingenious table is still useful to-day, either for coding or decoding. Cardinal Richelieu, the great statesman, frequently resorted to cryptography. Louis XIV. used so complicated a cipher for corresponding with his Ministers when they were absent from Versailles, or when he himself was with the army, that it was not until 175 years after his death that the key was discovered.

Let us here pause in this historical survey to examine more closely the part played by ciphers. Nowadays all the Great Powers have a Cipher Department. There is one in London, and others at Paris, Rome, Petrograd, Berlin, Vienna, and elsewhere. When the head of a State and his Minister of Foreign Affairs leave the country, they are always accompanied by a staff of experts from the Cipher Department. M. Poincaré, during his last journey to Russia, a few days before the German aggression, had with him the Director of the French Cipher Department, with whose collaboration he was able to keep in touch with Paris without running the risk of indiscreet confidences.

Germany has a department, the *Chiffrierburö*, staffed by professional experts, whose mission is to find new ciphers, both complicated and safe, and to decipher the secret documents of the enemy. The newspapers in-

[1] G. Selenus, *Cryptomenice*, p. 282 (Alcuin).

formed us that in February, 1916, the Department at Vienna employed twenty-six cryptographers.

"Cryptography," said one of the most genial of Swiss Army commanders to me the other day, "is a German science. You must be a German, wear gold spectacles and a bushy beard, before one can properly study cryptography."

Not so long ago, however, when neither Berlin nor Vienna were capable of deciphering difficult cryptograms, they were glad, on occasion, and in secret, to have recourse to one of those little States which they so utterly despise.[1]

Each step in the progress of cryptography is accompanied by a corresponding step in the art of deciphering.

History has preserved the names of some celebrated decodists. Thus, the geometrician François Viète succeeded in deciphering for Henry IV. a very complicated system, formed of some five hundred signs, which was used by the heads of the Holy League and the Spaniards.[2] The latter angrily denounced Viète to the Holy See as a wizard and a necromancer. According to them, he could only have entered into possession of the secret by calling up the spirits of those who had known the cipher during their earthly career. But the Pope was a man of humour: he submitted the plaint to examination by a commission of Cardinals, "with urgent recommendation." The Cardinals understood the hint, and the examination is still unfinished.

[1] See the *Zürcher Post*, February 28, 1916, midday edition, and the *Bund*, February 29, 1916, Sup. No. 100. The military Court at Zurich, after seeming to hesitate subjectively over this point in a paragraph of its judgment, admitted it objectively in another paragraph.

[2] De Thou, *Histoire universelle*, Book 129, year 1603.

During the reign of Louis XIII. another decodist, Antoine Rossignol, made himself known, to the discomfiture of the Huguenots.

"It was in the year 1626," says Charles Perrault,[1] "at the siege of Réalmont, a city of Languedoc, then in possession of the Huguenots, that he first gave proof of his talent. The city was besieged by the army of the King, commanded by the Prince de Condé, and it opposed such a resistance that the Prince was on the point of raising the siege, when a letter from the besieged was intercepted, written in cipher, of which the most skilful in the art of deciphering could make nothing. It was given to M. Rossignol, who deciphered it forthwith, and said that the besieged were sending to the Huguenots of Montauban to say that they were short of powder, and that if they were not supplied with some immediately they would surrender to the enemy. The Prince de Condé sent the besieged their letter deciphered, with the result that they surrendered the same day. Upon this being reported to Cardinal Richelieu, he invited M. Rossignol to the Court, and the latter gave such astonishing proofs of his skill that the great Cardinal, despite that extraordinary disposition which prevented him from admiring many things, nevertheless could not forbear expressing his surprise. He (Rossignol) served very usefully during the siege of La Rochelle, discovering the enemy's secrets by means of intercepted letters, all of which he deciphered with scarcely any trouble."

He continued his activities under Louis XIV., who held him in such high esteem that once, on the way back from Fontainebleau, he called on him at his country

[1] *Les Hommes illustres qui ont paru pendant ce* (17*th*) *siècle.* Vol. i. *Antoine Rossignol, Maistre des Comptes.*

house at Juvisy to which he had retired. The poet Bois-Robert addressed many of his epistles in verse to Rossignol, in one of which, in accordance with the wishes of Cardinal Richelieu, he extols Rossignol's skill, regarding him as a redoubtable prodigy. The following is a rough translation of the passage:

"There is nought else beneath the skies
That may be hidden from thine eyes.
O what a mighty art is thine!
For by it provinces are won,
And secret plans of kings undone.
This is a right commodious art.
I prithee unto me impart
Thy methods, and thus justify
The years that be and those gone by.
The vanquished, fleeing from the fray,
Take oath a devil's in thy pay;
Hell's unseen imps their packets steal,
Their secrets to thine eyes reveal."

There is a certain amount of truth underlying this extravagant eulogy, not that an Antoine Rossignol would wish it. Colonel Schaeck, of the Swiss General Staff, has stated that "a good decipherer must have both natural and acquired qualifications, the former necessarily playing a predominant part. The natural qualifications are insight, the spirit of observation, patience, and perseverance. If a person be happily gifted in any degree for this kind of work, and finds an opportunity of developing his natural talents, he may attain by study and practice a surprising degree of skill. For this he will have to devote himself to a profound study of the various systems of cryptography, have a thorough knowledge of mathematics, and especially the calculation of probabilities, and be acquainted with languages and their literatures."

Two remarks may be added to this statement: First, in default of mathematics, we may be satisfied with arithmetic; secondly, one thing is indispensable, which Colonel Shaeck possessed, although he modestly refrained from mentioning it—common sense. I have heard of a case where fifteen months of assiduous research failed to produce any result, while, a little later, by the exercise of a little common sense, the goal was reached in two days.

In 1645 John Wallis, the English mathematician, acting under the order of Cromwell, deciphered the secret papers of King Charles I., which were seized after the Battle of Naseby, and which proved that the King, in negotiating with his adversaries, was playing a double game.[1]

On July 2, 1673, Louvois, the then French Minister of War, paid 600 livres, equivalent to £120 sterling, to one Vimbois for discovering the cipher of certain conspirators; four days later he prescribed a similar fee to the Sieur de la Tixère for a discovery of the same kind.[2] If these lines méet the eyes of any cryptographers, they will regretfully admit that the remuneration for their arduous labours has dwindled terribly since that period.[3]

In 1752 a German professor named Hermann, who had defied the mathematicians and learned societies of Europe to decipher a system of his invention, saw his secret unveiled by a Swiss named Nicolas Béguelin or De Béguelin, son of the Mayor of Courtelary, a village

[1] *Encyclopædia Britannica*, art. Cryptography.

[2] Valerio, *De la cryptographie*, vol. ii., p. 11.

[3] The amour-propre of the cryptographer does not always meet with the respect due to it. For instance, a cryptogram which I was charged officially to decipher in May, 1917, resolved itself into "  . . . for the fool who reads these lines."

situated in that part of the bishopric of Basle which was then under the Bernese Protectorate. He had required only eight days to discover the key. The story of this incident is preserved in the *History of the Royal Academy of Science and Literature of Berlin*.[1]

It was by methods used in cryptography that Münter, a Dane, and Grotefend, a German, succeeded in 1802 in deciphering a part of the alphabet of the Persian cuneiform inscriptions. One group of angles or arrow-heads struck them by its frequent repetition. Münter pronounced it to be equivalent to the word "king" (*Kh-shayathiya* in the harmonious language of the time), and this supposition was eventually confirmed.

Mention may be made also of Bazeries, a French officer, who not long ago succeeded in deciphering Louis XIV.'s system of cryptography, comprising some 600 numbers, some of which represented letters and some syllables. Thus, for example, the word "mine" could be written in these four ways—*i.e.*,

| | | | |
|---|---|---|---|
| I. | 46. | 144. | |
| II. | 230. | 59. | 125. |
| III. | 514. | 184. | 374. |
| IV. | 535. | 229. | 146. |

and by still other figure combinations.

* * * * *

As we have seen, cryptography has at all times been extensively used by conspirators, revolutionaries, and secret societies. On this point I will confine myself to the two following quotations:

"In May, 1603, a number of foreigners used to meet in a house near Fontainebleau, which they had bought

[1] Year 1758 (1765), pp. 369-389, with two plates.

for the purpose of meeting secretly. Their plottings, however, were frustrated, as their house was raided, and among other suspicious objects were found a quantity of letters in cipher which revealed the conspiracy."[1]

"Among the papers of the Chouannerie," says M. G. Lenotre,[2] "are to be seen a number of sheets written in bizarre characters which formed the cipher used by Georges Cadoudal and his associates at the time of the Directory and the Consulate. The key of these is known."

The archives of the Foreign Offices in various countries still contain cryptographic documents the keys of which are lost and the deciphering of which the cryptographers, after interminable efforts, have had to abandon—according to plan! A curious circumstance is that texts written in cipher are encountered even among the hieroglyphs. A certain inscription of Esneh contains a profusion of crocodiles, in groups of as many as eighteen at a time, the meaning of which is not apparent. The most hardened Egyptologists have not yet succeeded in forcing the teeth of these redoubtable saurians apart and making them disgorge their secret. Certain mysterious languages—perhaps Etruscan, for instance—might yield to cryptographic methods of decipherment.

* * * *

If the "black cabinets," or postal espionage offices, which were extensively used in France during the reigns of Louis XIV., Louis XV., Louis XVI., and Louis XVIII., unsealed letters to feed the police reports and to furnish gossip to the Court camarillas, the black cabinets of the German Empire in the eighteenth century were centres

[1] Dulaure, *Singularités historiques*, p. 303.

[2] See article on "Ciphers," in the *Temps*, September 29, 1917.

of cryptography. Count Brühl, Prime Minister of Augustus III., Elector of Saxony, organised a completely equipped establishment at Dresden. All the messages received or sent by the King of Prussia's Ambassador in that city were opened, copied, and deciphered during a period of sixteen years, from 1736 to 1752. As soon as the postal courier from Berlin arrived on Saxon territory, at Grossenhayn, his bag was picked during the changing of horses, the official letters abstracted and sent by a swift horse-rider to Dresden, where the black cabinet unsealed, copied, and resealed them, and returned them to the post, which delivered them at the same time as the rest of the mail, which had arrived in the interval. This black cabinet, known as the "Secret Dispatch," was directed by the Aulic Councillor Von Siepmann, assisted by numerous experts.

Another dignitary, Baron von Scheel, officer of the corps of cadets, excelled in forging handwriting, which made it possible to tear open envelopes too troublesome to unseal. The Court locksmith was under orders to go to the Legation and, with the connivance of the Prussian Secretary, force the lock of the chest in which the Prussian Minister kept the keys of the ciphers.[1]

Thanks to their laudable activity, Saxony was aware of the plans of Frederick II., and, when needful, communicated them to Austria and Russia. Count Brühl, however, gave the game away at an official dinner, when he indiscreetly mentioned something he had learnt through his perverted laboratory. Frederick II. changed his systems of cryptography, and thenceforth entrusted his correspondence solely to functionaries who were abso-

[1] *Schlözers Staatsanzeigen*, Part 62, p. 129 *et seq.*

lutely beyond suspicion.[1] But he did not complain, for he himself had for some time carried on the same kind of espionage, which gave him a tangible advantage over his opponents during the Seven Years' War.

Austria, moreover, did not lag behind, and—a masterstroke—her black cabinet was operated in a wing of the Imperial Palace of the Stallburg, at Vienna. The staff, who were Neapolitans and well versed in work of this kind, directed their energies to the correspondence of all the Ambassadors. On one occasion the deciphered copy was placed in the official cover addressed from Madrid to the Spanish Ambassador, instead of the original letter extracted therefrom. The Spanish diplomat lodged a complaint with the Austrian Prime Minister, Prince Kaunitz. The matter was serious, and might have involved grave consequences, so the Prince severely reprimanded the negligent official.

The work done in the black cabinets cannot be accurately termed "cryptography," as they merely deciphered cryptographic documents by means of the key, which they were quite incapable of discovering for themselves.

* * * * *

The *literature* on cryptography is very voluminous; it would be scarcely possible to mention in these pages the titles of all the works which have been published on this subject. I need say no more than that, of all those I have read, the most substantial is the work of a Frenchman. I might mention, also, the name of Von Kasiski, a German Major. Books, it is true, provide a great deal of interesting material, but they do not help to decipher

[1] The secretary changed his name and sought other fields for his talents.

documents which are in any degree complicated, any more than the best of grammars can make a good writer.

## IV.

Let us now examine some of the principal systems of cryptography or ciphers.

Broadly speaking, all the systems may be divided into two categories: Substitutional, where the real letters of a text are replaced by other letters, or by Arabic numerals, or by any other signs; and Transpositional, which retain the real letters, but shuffle them completely, so as to produce chaos.

1. In the *Substitutional* class—that is to say, where the letters are replaced by other letters, or by figures or signs—are comprised the systems of which examples have already been given: the first example, then those of the Freemasons, of the zizgag and the thread, and of the two thieves.

Here are some others: The Hebrew cabalists had several cryptographic ciphers, which they used principally to discover the hidden meaning of certain passages in the Bible. Thus the *Athbash*, the Hebrew spelling of which forms the key—A.Th.B.Sh—consisted in writing the last letter of the alphabet ת (*thaw*) instead of the first letter א (*aleph*), and the last but one ש (*shin*) instead of the second ב (*beth*), and so on. The application of the Athbash resulted, among other instances, in identifying under the place-name Sheshak[1] that of Babel, or Babylon.

Another system, *Albam*, consisted in replacing the first letter of the first half of the Hebrew alphabet א (*aleph*)

[1] Jer. xxv. 26.

by the first letter of the second half of that alphabet ל (*lamed*), and the second letter of the first half ב (*beth*) by the second letter of the second half מ (*mem*), etc.

In a third system, the *Atbakh*, the interchange of the letters was based on their numerical value. But I shall not dilate further on this, as that clever Hebraist, J. Buxtorf, has explained the whole thing far more clearly in Latin than I can in a modern language. Those desiring further details are referred to his book.[1]

Bacon thought he had found something wonderful in the following invention: He replaced each letter of the plain text by a group of five letters, writing:

AAAAA AAAAB AAABA

for A B C. The method of deciphering a document written in this way is obvious enough: the frequency of the groups must be calculated instead of that of the letters. In the example given below, representing the last letters of a message, and, according to the most plausible supposition, the termination of a feminine Christian name,

ABAAA BBBAB ABAAA

we are induced by the frequency of the groups to read ENE, and, accordingly, to presume such a name as Irene, Magdalene, or Helene. And, once we have arrived at the probable value of two letters in a ciphered text, success is only a question of time.

We have already seen how the systems of Julius Cæsar and Augustus were written. They followed a parallel progression: D for A, E for B, F for C, etc. But suppose we break this symmetry, and say, for instance, that

[1] *De Abbreviaturis Hebraicis*, Basle, 1613, pp. 24, 27, and 37.

R = A, O = B, V = C, P = D, H = E, etc. The difficulty then becomes apparent.

By making use of the *cipher square*, or Vigenère's table, it is possible to write in cipher by means of several secret alphabets, as many as four, five, six, or even ten or more at a time, in periodical succession. Here are the first few lines of Vigenère's table[1]:—

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

etc.

Suppose we wish to conceal the word "hieroglyphics" in cipher by using three alphabets, in the first of which B takes the place of A, C of B, etc.; in the second E = A; and in the third C = A. We accordingly adopt as the key-word to our cipher the combination BEC, being the letters standing for A respectively in the three alphabets. We now write the word "hieroglyphics," and under each letter add a letter of the word BEC in consecutive order, thus:

h i e r o g l y p h i c s
B E C B E C B E C B E C B

The next thing is to look in the above table for the letter H in the horizontal line of capitals, and for B in the column of capitals on the left; at the point where the two lines commanded by these letters intersect we find the letter *i*, which we write as the first letter of our

[1] The complete table will be found on page 155.

ciphered word. The same operation for the letters I and E yields *m*, which we take as our second letter, and so on. The finished result appears as follows:

h i e r o g l y p h i c s
B E C B E C B E C B E C B
i m g s s i m c r i m e t

Thus the word "hieroglyphics," written by the aid of the key-word BEC, is transformed into "imgssimcrimet." It will be noted that of the three *i*'s in the cryptogram only two stand for the same letter in the plain text; the same is true of the three *m*'s, while the two *s*'s also represent different letters.

Let us examine another cryptogram of the same order:

t a p v c c i g r q d u p r b h i t v c c a c e o e a o s c
a l i e c c.

Given the knowledge that this text has been ciphered by means of Vigenère's table and that the key-word is PIANO, we operate by reversing the process described above—that is, we write the key-word PIANO repeatedly under the letters of the cipher; then, looking for the first letter of the key-word P in the vertical column to the left of the table, we find in the line corresponding thereto the first letter of the cipher *t*, and at the head of the column in which this occurs we note the capital letter E, which will be the first letter of the deciphered text. Proceeding in the same way with the second letter of the key-word and cipher, I and *a* respectively, we obtain S, and so on until we have before us the whole text deciphered as follows: "Espionage compensation scraps of old iron."

As we have seen, deciphering by means of the key-word is quite easy when we know that word. When we

do not know it, however, there are certain methods, a little too long to explain here, which permit of its discovery almost mechanically. All that can be said is that in the above cryptogram, as well as in any other secret document, the first thing to do is to find the vulnerable point in the armour and attack it with the weapons at your command.

Now, in the text we have just deciphered, the weak spot is the double letter *cc*, repeated three times, and it is this which will help us pierce the mystery. After careful investigation, we find that they correspond in each case with the letters *on* of the plain text: Espi*on*age, compensati*on*, ir*on*, all three of which, in the ciphering, fall by accident under the letters OP of the key-word PIANO.

Let us now examine a somewhat different example. We are handed a document to decipher which reads as follows:

M A S E G X
I S O O M O X
A M O X E X
G K Y Y M N K
Y K O S E K

The valuable information is afforded us that this paper was confiscated from a traveller at Brigue, on the Italo-Swiss frontier, and we therefore "presume" that the text is in Italian. Noting that the first, third, and fifth lines each contain six letters, while the second and fourth have seven, we assume that the cryptogram is more likely to be a list of words, or rather names, than a phrase.

The letter occurring most frequently is O, which, according to the rule of frequency, should represent *e*,

but it is in vain that we try to decipher the second line, in which it appears three times. If we adopt the hypothesis that we have before us a list of proper names, we are compelled at the same time to recognise how little help may be expected from the manuals, otherwise the grammars, of cryptography. For we encounter interminable lists of family names in which the letter *e* is not the most frequent: Bacon, Byron, Foch, Churchill, Wilson, Dumont, Gounod, Marconi, Calvin, Loyola, Cagliostro, Victor Hugo, etc.

The axiom postulated by the books that the letter *e* is the pivot in deciphering will not carry us very far, so that another method must be adopted for deciphering proper names—not only those we have just enumerated, but names in general. The *frequency of their terminations* in each language must be taken as the basis. In French, for instance, 8 per cent. of proper names end in *er* or *ier*—*e.g.*, Mercier, Fournier, Garnier, Beranger, Boulanger; 7 per cent. in *on*—*e.g.*, *ond*, *ong*, *ont*: Masson, Champion, Dupont, Leblond, Long; 6 per cent. in *au*—*e.g.*, *eau*, *aud*, *aut*, *aux*: Boileau, Rousseau, Moreau, Clemenceau, Nadaud, Caillaux.[1] In Russian, *ov* and *ev* terminate 35 per cent. of names; *sky*, 25 per cent.; *in*, 9 per cent.; *itch*, 6 per cent., etc.

Those who wish to take up cryptography and to indulge in these interesting calculations without undue mental fatigue should confine their energies to Turkish family names—a by no means complicated task, for there are none! In the Ottoman dominions all that is necessary, even for official records, is to say that one is called John the son of James, or Ali the son of Mustapha. I once

[1] It must be understood that these proportions are only approximate.

asked a friendly Greek, who has long officiated as a magistrate in those parts, how they managed to avoid errors in a large city housing, say, 500 Alis sons of Mustaphas. My interlocutor seemed surprised at my question, and answered: "Oh, there is no trouble at all in identifying anybody."

A little digression. In that happy country, not only do fathers not transmit their family names to their children, but, on the contrary, in certain cases, it is rather the children who transmit their names to the fathers. For instance, a certain Osman has a son named Taleb, who becomes famous. The father then changes his name from Osman to Abu Taleb, "the father of Taleb." An historical example is that of Abd el Caaba, who, having given his daughter in marriage to Mahomet, was so proud of the event that he changed his name to Abu Bekr, "the father of the Virgin." Later he became Caliph and first successor to the Prophet.

Of German names, 25 per cent. end in *er*, and 6 per cent. in the syllable *mann*: Troppmann, Bethmann, Zimmermann, etc. Italian names end in *i* (40 per cent.), *o* (30 per cent.), *a* (20 per cent.), etc.

This brings us back to our example. We will suppose that the termination X, which is the most frequent, represents *i*. At the end of the third name we find two of these supposed *i*'s separated by a letter not yet identified. Now, as our study of proper names has gone considerably beyond the rudiments set out above, we know that *ini* is the most likely ending: Bellini, Rossini, Mazzini, Di Rudini, etc. We therefore assume that E = *n*.

A similar problem now confronts us at the end of the first word: n ? i. Careful reflection leads us to suppose that this word is a common noun in the plural, ending

in *nti* (example: *canti, conti, santi*), and that it might be a heading or the title of the list, perhaps *agenti*. Acting on this assumption, we make the required substitutions—ready, of course, to try other suppositions if this fails us—and our cryptogram assumes the following form:

A G E N T I
? E ? ? A ? I
G A ? I N I
T ? ? ? A ? ?
? ? ? E N ?

A moment's reflection induces us to substitute the letter *r* for O, which occurs three times in the second line, once in the third, and once in the fifth. From ? e r r a r i we automatically reach F e r r a r i. As our calculation of frequencies in Italian name terminations gives the second place to *o*, we substitute that letter for the K's in the last two lines. The letter Y causes some hesitation, but eventually we decide to replace it by *m*, and finally we have the following version:

A G E N T I
F E R R A R I
G A R I N I
T O M M A S O
M O R E N O

This method may seem empirical, even infantile, but it often produces satisfactory results.

The difficulty becomes really serious in the system of ciphering by means of Arabic numerals, in which a letter, a syllable, or a word is represented by two or three figures. For example:

28. 71. 54. 75. 09. 62. 20. 65. 13. 79. 52. 32. 75. 88. 79. 43. 22.

stand for "Travaillez, prenez . . ." ("Work, take . . ."). The numbers 54 and 09 each mean *a*; 13, 88,

and 43, *e*; number 52 means nothing; the first 75=*v*, the second 75=*r*. The methods of deciphering here are so delicate, fragile, and awkward to explain that I prefer to leave them to the innate sagacity of the reader.

* * *

An undecipherable system is that which consists in designating a letter by means of the number of the page in a book, the number of the line, of the order of the word in that line, and, finally, the position in that word occupied by the letter in question, thus: 127.6.4.2. The correspondent will decipher this if he has a copy of the same book in the same edition as the sender.

Unfortunately, this system takes a long time to cipher, and very long to decipher, without taking into account the inevitable errors. Moreover, you may not find the letter required. If you are using a French book, for instance, you may have to dispense with a *k*. True, you might use a *c* instead, but this would sometimes lead to confusion. Suppose you want to write: "Kiel is besieged." "*Ciel* (heaven) is besieged" is scarcely the same thing. Neither would your correspondent ever guess that in the phrase, "His Majesty ill; *cocher* (coachman) summoned to general headquarters," the word "cocher" was intended for the famous surgeon Kocher.

In Russian books the letter *f* is also infrequent, while in Italian publications *w* and *y* are rarely seen.

* * *

Correspondence has sometimes been carried on in the following manner: Most dictionaries are printed with two columns on a page. Instead, therefore, of writing

the required word, you adopt the word appearing on the same line in the parallel column, thus:

| | | |
|---|---|---|
| WADE | instead of | VISION |
| THERMOMETER | ,, | TERRIFY |
| BELLICOSE | ,, | BEARER |
| ESTUARY | ,, | EQUAL |
| TORRENT | ,, | TO |
| OMIT | ,, | OCCASION |

The word "terrify" appears here, but not "terrified," which would not be found in a small dictionary. And, in fact, the disadvantage of using ordinary dictionaries in this way is that the various grammatical distinctions cannot all be shown. Thus, with the aid of any dictionary you can say "Sen*d* letter," but not "Sen*t* letter," which two phrases are diametrically opposed in meaning.

Special dictionaries have been compiled, each page containing fifty words in current use. Thus, for instance:

(page) 17

23 GRADUAL
24 GRANT
25 GRAVE
26 GREEK
27 GREEN

If it is required to send the word "Greek," you write the number which precedes that word and the number of the page, 17.24, or the whole in one number, 1724.

Much more voluminous dictionaries have been utilised or compiled, in which all the words are accompanied in the margin by numbers ranging, say, from 1 to 100,000. Let us endeavour to decipher the following crypto-

gram, coded from a dictionary of 25,000 numbered words:

| | | |
|---|---|---|
| 24133 | 24029 | 15128 |
| 21682 | 01643 | 21531 |
| 05070 | 24127 | 09043 |
| 21531 | 02432 | |
| 01174 | 15311 | |

The first thing to do—and it is not easy—is to determine the exact meaning of two of the numbers, the same way as when preparing a survey map of a country it is first necessary to calculate with the utmost accuracy the height and distance of two given points, to form a base on which the triangulation of the whole region may be effected, and the altitude of all heights therein calculated, so in cryptography a secure base must be sought decoding a ciphered document.

Let us assume that we have discovered the meaning of the last two numbers in the above:

21531=THE; 09043=GENERAL.

It will be noted that 21531 occurs twice, which would favour the assumption that it represents a common word. Success in deciphering this form of cryptogram, however, depends mainly on a careful observation of the relative values of the numbers and their comparison with the approximate positions of the words in a dictionary. In the above cipher, for instance, the three highest numbers are all in the twenty-fourth thousand, and, as their values are very close, we cannot go far wrong in assuming them to stand for words beginning with W. This would place the twenty-first thousand somewhere about T, so that the probable initials of the first two words of the message are W and T. Leaving this on one side for the moment,

however, we will study the end, where the last two words are assumed to have been definitely established as THE GENERAL. Immediately preceding these, we note two numbers in the fifteenth thousand, which occur numerically about half-way between those representing GENERAL (09043) and THE (21531). We accordingly look in a dictionary, and find that the corresponding position is among the O's. Of words beginning with O likely to precede THE GENERAL, we observe OF, ON, OPPOSE, and OR, and provisionally select the first, OF, corresponding to 15128. We now have 15311, another presumed O-word, occurring later than OF in the dictionary. There are OPTION and ORDER, of which the second seems the more likely. This doubtless follows the word BY, which meaning we accordingly attach to 02432, the whole furnishing us with a useful tail-end: BY ORDER OF THE GENERAL.

Great patience will be required to ferret out the whole of the message, as there will be considerable fluctuation in the position of the words, varying according to the dictionary used to solve the cryptogram. We must make the most of the "landmarks" already more or less identified. The fourth word, 21531, is known to be THE, and the word following is probably, though not necessarily, a noun. We note that the number representing it, 01174, is the lowest of all, occurring doubtless among the A's. The message being of a military nature, we immediately think of ARMY and ARTILLERY, and look for a further clue. The next number, as well as the eighth, is presumed to be a W-word, as we have seen. The eighth number immediately precedes the phrase "By order of the General," and is therefore most likely a verb expressing something in connection with the

supposed army or artillery. Consulting the dictionary under W, we are attracted by the word WITHDRAW or WITHDRAWN. If the latter is correct, it should follow some part of the verb "to be," and, in fact, the seventh number, 01643, occupying numerically a position something over a third of the distance between ARMY (or ARTILLERY) and BY, would seem to represent the word BE itself. The sixth number, 24029, is a W-word, and both from the context and its numerical position a little earlier than WITHDRAWN (24127) in the dictionary, it excludes any other reading but WILL.

We have now to tackle the first three words of the cryptogram. The first number, 24133, closely follows that representing WITHDRAWN (24127) in numerical order, and the dictionary offers us as "probables" WITHIN or WITHOUT. After further study on the lines described, we produce WITHIN THREE DAYS as the first three words of the cipher. All that remains is to decide whether the fifth number, 01174, means "artillery" or "army." The words occur so closely in the dictionary that this is no easy task, but after careful calculation of the distances separating "be" and "by" from the beginning of the dictionary, we plump for "artillery," and our complete message reads: WITHIN THREE DAYS THE ARTILLERY WILL BE WITHDRAWN BY ORDER OF THE GENERAL.

It should be added that in practice such documents are not often found with the numbers written in this straightforward way. Usually the figures are transposed and all sorts of complications interspersed.

A common method is to rearrange the order of the figures in each group upon a prearranged plan. Thus, 24133, 21682, etc., are transformed into 13432, 62182,

etc. The great difficulty here is to discover the normal order of the figures in each number, and to restore them to their primitive form, before proceeding to the actual deciphering. It is a case of baling the ocean l

The principal inconvenience of those numbered dictionaries, known in diplomacy as "codes," is that when they are lost or stolen, in most cases others have to be compiled, and works of this kind cannot be made in a day. Even under the most favourable circumstances, when a fresh code is held in reserve for contingencies. considerable delay must ensue before instructions for their use can reach those concerned, and the enemy reaps the benefit. The following is one instance, among others, of this disadvantage: During the Russo-Turkish War in 1877, the Ottoman Field-Marshal, Osman Pasha, entrusted one of his Generals, Selim Pasha, with a confidential mission. It so happened that Selim was the officer responsible for ciphering, and, being prudent, he kept the code on his person. Unfortunately, he departed so promptly on his mission that he forgot to leave the volume with his chief. The latter, during the whole time of his Adjutant's absence, saw a pile of ciphered telegrams from Constantinople accumulate on his table, without being able either to read or reply to them.

## V.

2. The second category of cipher systems is the *Transpositional*, in which the actual letters are not changed, but are mixed together or shuffled, and in effect really amount to anagrams. Some anagrams are very short: *veil* for *live*, *are* for *ear*, *more* for *Rome*, *wander* for *Andrew*, *Angelus* for *Galenus*, *Vaussore*[1] for *Rousseau*, etc. In

[1] The pseudonym adopted by Rousseau when giving his famous concert at Lausanne.

cryptography, however, we encounter anagrams of 100, 200, 300, 500, and 1,000 letters. I have seen one comprising nearly 6,000 letters. It may be added that the longest are not the hardest to decipher; quite the contrary. Among these systems, which are very numerous, are included the "scytales" of the Lacedæmonians, which we have already considered.

A system easy enough to decipher is one which the cryptologist Vesin de Romanini called an "aerial telegraph cipher." The first letter of the text is written in the middle of the first line, the second letter at some distance to the right in the same line, the third letter similarly to the left, the fourth in the second line to the left, the fifth in the same line to the right, the sixth in the middle, and so on, inverting the order of the letters with each new line. Arrived at the foot of the page, a new start is made at the top, the letters being written in the same order as before, and immediately to the right—or left—of those already put down. A cryptographer will have no difficulty in reading a text ciphered in this way:

| | | |
|---|---|---|
| ER | TO | HP |
| SO | RE | TT |
| NT | GT | OC |
| UE | OH | GW |
| TA | TK | HE |

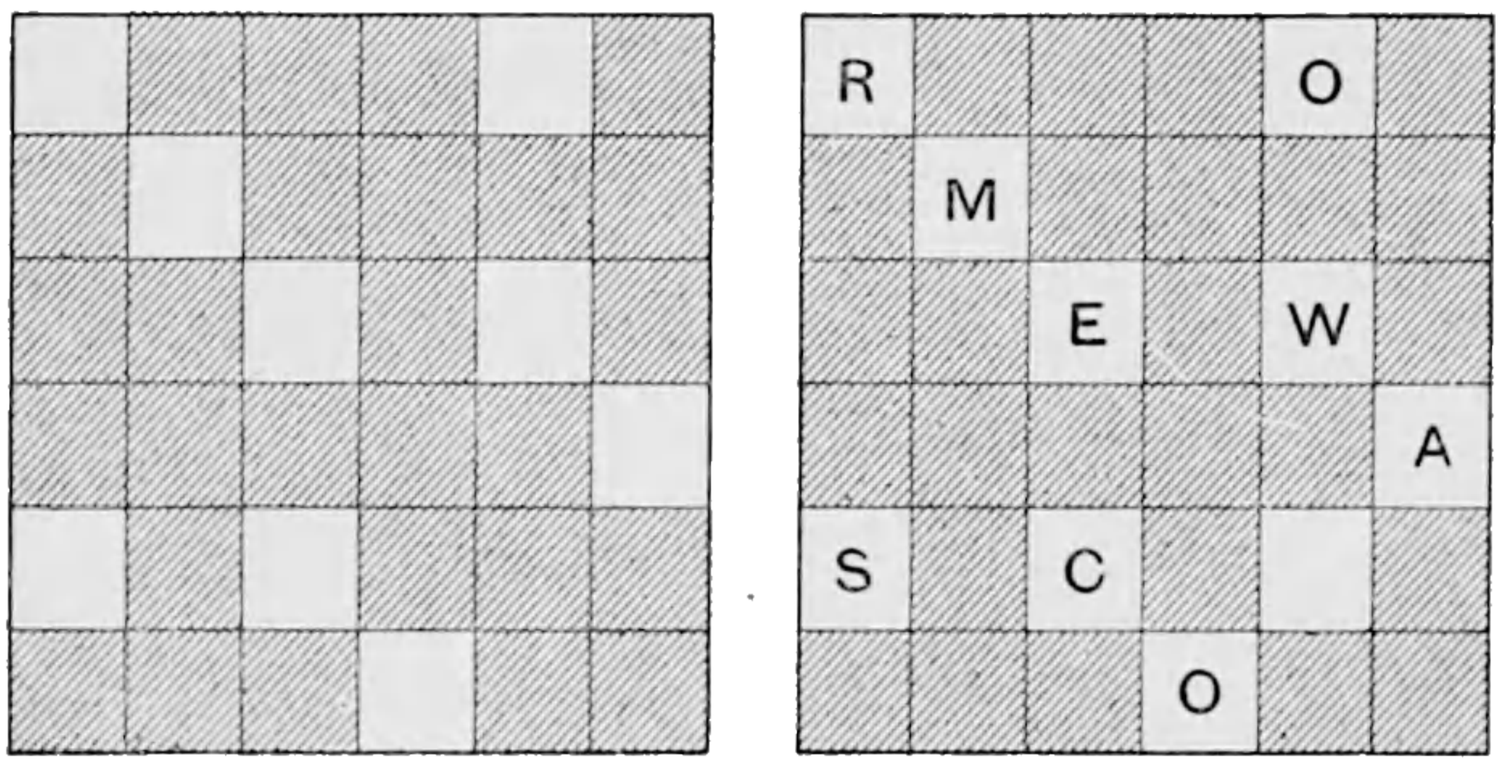
which means: THE STRONG OUGHT TO PROTECT THE WEAK. It was a similar cipher which Jules Verne used for his cryptogram in *A Voyage into the Interior of the Earth.*

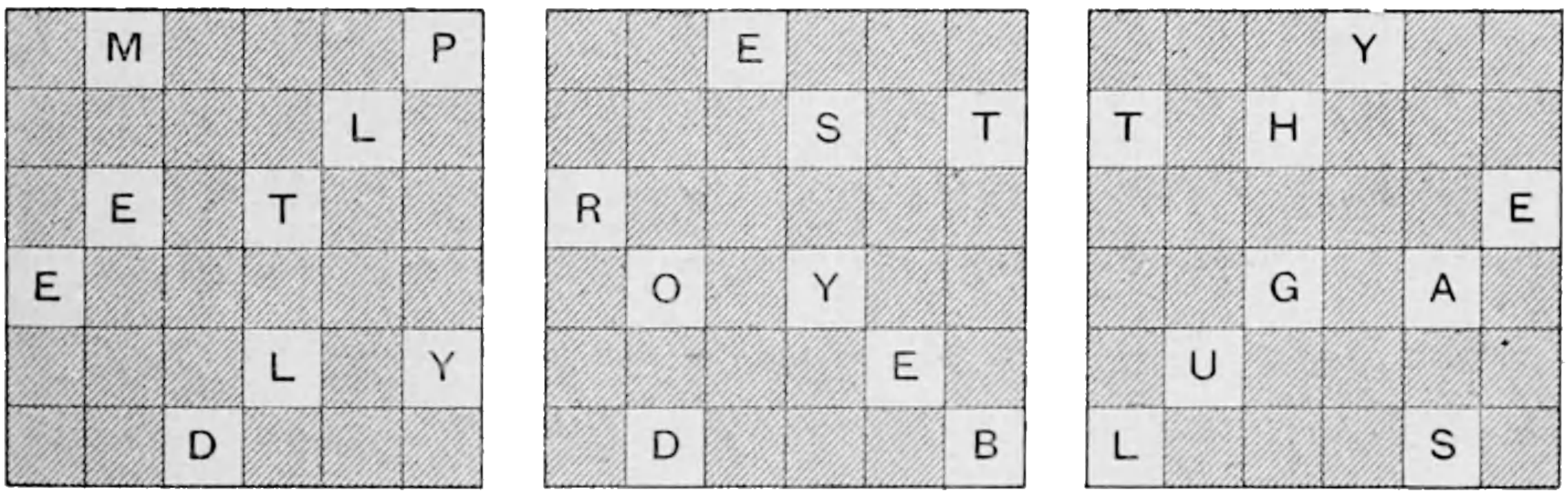
Let us now pass to the "*grille*," or "lattice," a well-known form of cipher. The grille is a square piece of stiff paper or cardboard in which a certain number of

holes are cut. The square thus perforated is superimposed on a sheet of white paper, and a letter is written in each hole. This done, the grille is turned 90 degrees to the right, so that what was the top left-hand corner becomes the top right-hand corner. The further letters of the message are now written in the holes, and the operation is continued until all four corners of the grille have occupied the same position. It need scarcely be said that, when cutting the holes in the grille, care must be taken to arrange them so that overlapping of the letters during the four turns will be avoided.

The following example can be read quite easily by means of the appropriate grille:

R M E Y O P
T M H S L T
R E E T W E
E O G Y A A
S U C L E Y
L D D O S D




Deciphered, this reads: ROME WAS COMPLETELY DESTROYED BY THE GAULS.

Grilles are usually larger than the above diagram, which, however, will suffice as an illustration. As may be seen, texts written in this code are very easy to read

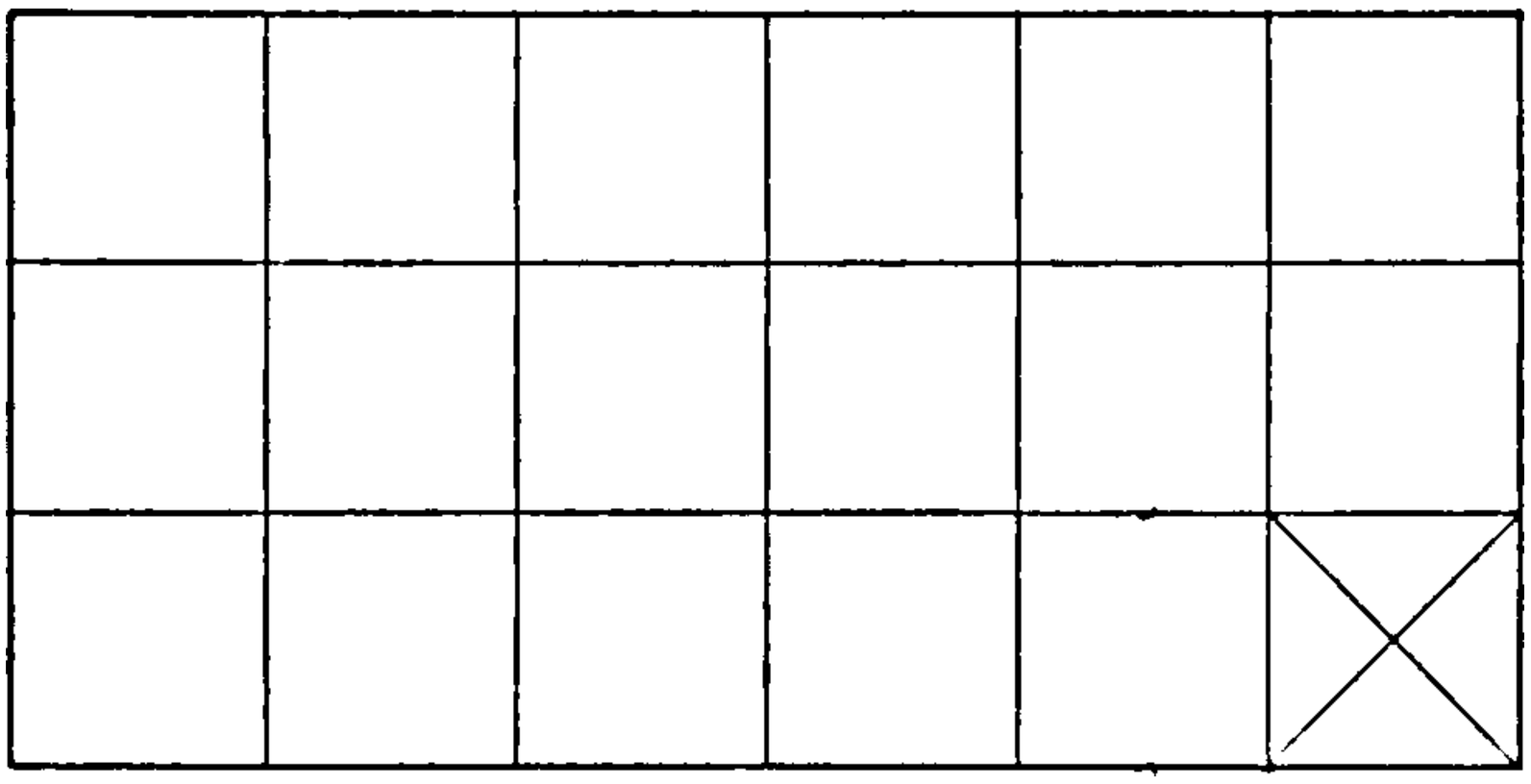
when one has the proper grille. Nevertheless, even without the grille the difficulty of deciphering is not very great, and in the second part of this volume I shall explain the mechanism of the process by which it can be done. To complicate this cipher, a high Austrian officer had the idea of mingling a number of blank or meaningless letters with the others; but this did not increase the difficulty of translating, as is proved by the fact that such a system is scarcely ever used.

The method of employing dividers is much to be preferred. It consists of cutting vertical slices in a text and mixing these columns of letters. Here is a very short example—just three names:

M A D R I D
V I E N N A
P A R I S

which we divide into vertical slices, proceeding then to write first the letters of the second column, next those of the last, fourth, first, fifth, and third—or in some other order as agreed on. In this case the key will be 2, 6, 4, 1, 5, 3: A I A D A R N I M V P I N S D E R.

How is the recipient of this brief message to deal with it? He knows that the key agreed upon provides for six letters in a line. Since the text contains seventeen letters, he proceeds to draw the following graph:



crossing through the last square, after which he writes in the letters of the cryptograms in the order indicated by the key—the second column, the sixth, the fourth, etc.—when the three names will be restored. On no account must he forget to cancel the last square, for if he absent-mindedly wrote a letter therein during the operation of deciphering, the whole of the little text would be thrown out of order. The name PARIS, for instance, would be changed to IAMDR. This system can be complicated indefinitely.

Let us examine another example:—

V H I I N R
U R S I N H
P W P L T N
K T D S S F
Z O O E I C
L E M B O E

This contains thirty-six letters, and is therefore very short; nevertheless, the number of possible changes of position which one might effect in the letters, to ascertain their meaning, is so enormous as to be practically incalculable. For the sake of comparison, take wheat-flour. If we could isolate a particle, and under a microscope count how many such scarcely perceptible molecules could be contained in a cubic millimètre, we should find, let us say, 100,000. Now, to form a sphere as large as our terrestrial globe, it would require a number of these particles equal to that of the combinations which it is possible to make with the thirty-six letters of our cipher, which would have to be represented by a series of thirty-seven figures.

The key to this last text is the same as that of the preceding cryptogram. Accordingly, the plain text must

be written six letters to the line, and the first letters of our example will form the second vertical slice of the graph. The phrase we are about to discover had for its author a great Captain who lived a century ago, and accomplished victories in Europe by the side of which the present victories of our enemy are insignificant.[1] He succeeded in a much more magnificent enterprise: he won the admiration of the enemy peoples. Deciphering by the graph produces the following:

K V L P Z U
T H E W O R
D I M P O S
S I B L E I
S N O T I N
F R E N C H

The first line is composed of blank letters, intended simply to embarrass the decipherer. The text begins from the second line: "The word impossible is not in French."[2]

This system of "dividers"—which distantly recalls the Lacedæmonian scytales, and was dubbed by an early nineteenth-century writer "the undecipherable cipher *par excellence*"—is very difficult to decode when one has to deal with texts more complicated than the elementary specimens we have just presented.[3] It may be pointed

[1] NOTE BY TRANSLATOR.—When M. Langie wrote this, the Germans were inflated with their military successes.

[2] The actual words are: "Le mot impossible n'est pas français."

[3] One method of complication, calculated to exercise the patience of the decipherer, consists in suppressing, *without leaving any trace*, if I may say so, of a certain number of *e*'s in a text in such a way as to upset the calculation of frequencies. But this proceeding is dangerous, inasmuch as it does not offer absolute security, and one runs the risk of entangling both oneself and one's correspondent.

out that the second and longer example, being regular, is less difficult to decipher than the first, which, though shorter, is irregular.

There are systems in existence which are literally undecipherable, the ciphers being sometimes composed by means of ingenious machines resembling the cash registers of the shops. But—there is a "but"—it is probable, and often certain, that systems absolutely undecipherable to an inquisitive outsider will also be so to their recipients, however well provided the latter may be with the desired keys. The reason is that important news is nearly always urgent. As soon as it is a question of urgency, resort has to be had to telegraphy[1] or radiotelegraphy. Now, in a long alignment of letters which are meaningless to him, the most skilful of telegraphists will commit involuntary errors—due to inattention, fatigue, or reflex movements. And when a telegram runs into a number of lines and has to be retransmitted several times, the case is worse.

It is stated that not 10 per cent. of telegrams in cipher are free from errors on their arrival. In the first place, there is continual confusion between the letters *u* and *n*, *o* and *a*, *e* and *c*, *e* and *l*, *m* and *n*, even in plain texts. Then it is so easy, by a false movement, to change the one letter *s* (...) into the two letters *i* (..) and *e* (.), or the two letters *m* (— —) and *t* (—) into the single letter *o* (— — —). It is precisely these extra or missing letters that do all the mischief.

One error is sometimes sufficient to make the whole text meaningless, as we have seen in the example MADRID. Hence, if one must use systems very diffi-

[1] Incidentally it may be pointed out that the telegraphic alphabet is nothing else but a system of cryptography.

cult to decipher, it is none the less indispensable to choose keys in which one error will not cause a repercussion throughout a document. Furthermore, it is not always convenient to carry about a dictionary or a code.

## Conclusion.

When one has a taste for cryptography, and opportunities arise to devote oneself to it seriously, the study develops into a passion. At first the amateur is bewildered. He must make persistent efforts, and not be discouraged by reverses. At all costs he must continue, assiduously persevering with trials not made haphazard, but reasoned out and based on induction and hypotheses. The slower the result is obtained, the more tardily success crowns our efforts, the more profound will be the satisfaction we experience when we reach the goal, and, like Archimedes, exclaim "Eureka!"

# PART II

## EXAMPLES OF DECIPHERING

### A Consultation.

One day a gentleman sent up his card and was shown into my office.

"It is to an unfortunate accident that I owe the pleasure of making your acquaintance," he said, very affably. "What has driven me to seek enlightenment from you is this: I have been sent here on a mission; you will excuse me from going into details. Arriving this morning, I had scarcely entered my hotel when a postman brought in a letter addressed to me. Now, it was an understood thing that those who sent it must write in cipher all communications of any importance. It is a wise precaution, for you will see, if you examine the envelope, that it had been opened by steam, stuck down again, and immediately dried. By whom? None of the hotel people could or would throw any light on the subject.

"The cipher agreed upon between us is a *grille*. I did not bring the grille—it might have gone astray—but I had noted on an old letter a method for quickly reconstructing the necessary grille, to be destroyed as soon as it had served its purpose. This method consisted merely of a list of the numbers of the small squares to be cut in a square sheet of paper, which would enable me

to read the secret message transcribed on to another square placed under the perforated sheet. Every night I destroy papers which I no longer want, and I fear I may have inadvertently burnt the letter containing the key in question. I was able to get your address without difficulty, and am come to beg you to bring all your skill into play, so that I may know the contents of the message without delay."

While saying these words, he handed me the ciphered text, which ran as follows[1]:

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

a total of sixty-four letters, or the square of eight. Even without the knowledge that I had to find a grille, that would have been the first idea to occur to me.

I begged my visitor to call again at the end of an hour, and immediately set to work. First I copied the text on to a square divided into sixty-four sectional squares, like that appearing below. I numbered the four corners in Roman numerals, and further added Arabic figures to the sixty-four squares for the purpose of easy identification.

The principle of the grille system has already been explained on p. 41. I revert to it merely to point out that the grille, numbered at the four corners in Roman figures, should fit exactly over the text, the corner of the grille numbered 1 covering corner I. of the text, corner 2 of the grille corner II. of the text, and so on. If, in our example, the first hole in the grille exposes the letter A (square 1), when the position of the grille is changed so that corner 1 covers corner II. of the text, and corner 2

[1] NOTE BY TRANSLATOR.—The text of the cipher, as well as certain portions of the explanatory matter, have been modified to meet the requirements of the English translation.

covers corner III., etc., the same hole will expose letter Y (square 8). A further operation will reveal the letter T (square 64), and a final turn the letter M (square 57). A similar result will be produced by all the other holes in the grille, which, in each of its four positions, will enable a quarter of the actual text to be read.

I II

| | | | | | | | |
|---|---|---|---|---|---|---|---|
| 1 A | 2 I | 3 T | 4 E | 5 G | 6 F | 7 L | 8 Y |
| 9 T | 10 B | 11 O | 12 E | 13 E | 14 H | 15 R | 16 E |
| 17 A | 18 U | 19 W | 20 N | 21 A | 22 N | 23 O | 24 A |
| 25 R | 26 R | 27 D | 28 R | 29 T | 30 E | 31 E | 32 T |
| 33 H | 34 O | 35 S | 36 H | 37 F | 38 P | 39 E | 40 T |
| 41 A | 42 P | 43 O | 44 T | 45 O | 46 Y | 47 H | 48 L |
| 49 R | 50 E | 51 T | 52 I | 53 H | 54 E | 55 N | 56 E |
| 57 M | 58 G | 59 A | 60 O | 61 A | 62 R | 63 N | 64 T |

IV III

In this case, however, the grille was missing, and my visitor, in his embarrassment, had asked me to reconstruct it. How must I proceed ?

I take a piece of tracing paper, cut a little larger than the above square, and superimpose it thereon. On the tracing paper I reproduce the outline of the square as it

shows through, and outside the four corners I write the Arabic numerals 1, 2, 3, 4. I then examine the text and endeavour to form a useful syllable.

On the first line my attention is attracted by A T (squares 1 and 3)—a common enough word in English, and one which might easily form the beginning of a message. Accordingly, I mark the place of these two letters on my tracing paper; after which I turn the latter, not a quarter only, but a half round, so that it is now reversed, and corners 1 and 2 cover corners III. and IV. of the text. The marks made on the tracing paper now coincide with R T (squares 62 and 64). This is a very good word-ending, and it is evident that from the last two lines we could easily extract the word H E A R T—squares 53, 54 (or 56), 59 (or 61), 62, 64. Marking these and again reversing the tracing paper, we find in the corresponding squares—1, 3, 4 (or 6), 9 (or 11), 12—the combination A T E (or F) T (or O) E. This not being very satisfactory, I abandon the combination and try another.

Having seen that the tracing paper is in its original position, I turn my attention to the second line, and decide to mark T H E (squares 9, 14, 16). This is conceded by investigators to be the commonest trigram in English, and is almost certain to occur in a text of sixty-four letters. Reversing the tracing paper as before brings the marks to the corresponding squares 49, 51, 56 in the sixth line, indicating the letters R T E. This is quite a promising combination, and I look for the vowel which should precede it. The first that meets the eye is O (square 45), while three squares farther back (42) appears P. We now have the group P O R T E, which seems to call for the final R, and sure enough this letter

occurs in the last line at square 62, though, of course, N T (squares 63, 64) are possible.

I now reverse the paper to ascertain what letters correspond to the new marks, and bring to light T (square 3) and N O (20, 23). We now have the group T T H E N O, the first letter being doubtless a final, and the last two the beginning of a new word. The next proceeding is tentatively to begin the construction of the grille, which I do by drawing squares round the letters P O R T E R (42, 45, 49, 51, 56, 62).

Let us now take crayons in four colours—say blue, red, green, and yellow. With the blue crayon we make a small mark in the text itself against each of the above six letters. We now turn the tracing paper, but this time only a quarter, and our six marked squares now cover the letters I O U S A G (2, 11, 18, 35, 41, 58). To these we attach a brown mark. Incidentally, it may be noted that the results of the quarter turn, unlike those of the complete half, are not necessarily to be read consecutively.

A further turn brings us to the group T T H E N O (3, 9, 14, 16, 20, 23), which we mark in red; and a final turn produces L A E H E N (7, 24, 30, 47, 54, 63), which we indicate in green.

We have now neutralised 24 out of the 64 squares, thereby narrowing considerably our field of research. Coming back to our original group P O R T E R, we look for a likely word to precede it, and are favourably inclined towards T H E (32, 36, 39). There are two H's between the T and the E, and we adopt the second experimentally. Marking these and reversing the tracing paper, we find the three corresponding letters to be R T H (26, 29, 33). This enlarges our red group to T THE NORTH—a result which proves that we are on the right

track. Accordingly, we mark in the four colours the corresponding letters in the four positions, bringing the total of neutralised squares to 36.

Progress onwards is by leaps and bounds. We have simply to study one or other of the coloured groups, ignoring meanwhile the now numerous ear-marked squares. For instance, on scrutinising our two red words, THE NORTH, and the unmarked letters following them, we quickly discern a P and an O, and think of "Pole." These letters are duly found in squares 38, 43, 48, and 50, and, having marked these in red and the corresponding letters in the other positions in their appropriate colours, we find that only twelve squares remain to be accounted for.

The materials for the grille are now almost complete, and we are able to cut out 13 holes from the 16, which, in the four positions, will enable us to read the whole of the text. Our four coloured groups, each requiring three letters to be complete, now appear as follows:

Red: T T H E N O R T H P O L E
Green: E L B E W A E F T H E A N
Blue: R A N D T H E P O R T E R
Brown: I F O U A R S A Y I N G A

A glance at our text shows Y (square 8) to be the only unmarked letter between the F and O in the brown line, which discovery enables us to fill in all the other blanks automatically, and at the same time proves the brown line to be the beginning of the message. We can now complete the cutting of the grille.

At this juncture my visitor appears. "Have you discovered anything?" he asks eagerly.

"Here is your grille," I reply. "Let us read it together: IF YOU ARE STAYING AT THE NORTH POLE HOTEL BEWARE OF THE MANAGER AND THE PORTER."

But our friend suddenly looks grave.

"Good heavens!" he exclaims, "I have some important papers in my portmanteau." And with a bound he disappears downstairs.

It is to be hoped he arrived in time.

## Where is the Money?

The Chief of the French Secret Service Department had invited me to call upon him, and after giving me a cordial welcome, said:

"You are aware that, following on the robbery at the Continental Bank, the notorious individual whose identity has not been established, and who is known only under one of his aliases, Pastoure, has just been sentenced to five years' imprisonment. Had he taken scrip payable to order or bearer, we should have been at ease, but he has confined his attention to cash.

"Now, a fellow of his stamp would hide the stolen sums in such a way as to be able to find them intact on regaining his liberty, and he is too keen a psychologist to have confided his secret to an accomplice. He has worked single-handed, and we only managed to lay hold on him thanks to an accident, a hole having been torn in one of the fingers of the rubber gloves he wore in his operations. By this circumstance we secured an imprint of his thumb, and identified it with the anthropometric record already made on the occasions of his previous collisions with justice.

"Unfortunately, six days elapsed between the robbery

and the arrest. We have been able to trace his movements during the last two days, but are still in the dark as to how he employed his time during the first four. Being determined to leave no stone unturned to recover the money, I have continued a strict investigation. Yesterday I visited the central establishment housing our man, and learnt that Patoure had, almost immediately on his entry, asked permission to write his will, which he handed sealed to the prison registrar. I had the package produced, and, having obtained a warrant from the Court, took cognisance this morning of the *last wishes* of the prisoner, and in his presence.

"The text of the will was somewhat to the effect that its author bequeathed his watch, a ring, the contents of his purse, and his personal effects to his brother and sister, who would make themselves known when required if an advertisement were inserted in a big daily asking for the 'heirs of M. de Pastoure.'

"I was struck by the aspect of the fourth page of this document, which the prisoner had covered with figures. I asked him what this meant, and he replied that they were merely calculations of interest on the income from land held in common by his family in their village!

"Here is the paper itself. I do not know why the contents of the fourth page perplex me. You see that in the four columns into which the page is ruled off, Pastoure has written sums in addition, subtraction, multiplication, and division, with erasures everywhere. Please take the document, examine it at leisure, and let me know at your convenience what you think of it."

I put the will into my bag, and, having arrived home, studied it with eager curiosity.

I began by verifying the results of the arithmetical

operations occurring therein. At first glance the whole was a confused medley. The number 158, for instance, multiplied by 86, was shown as 4,311; and similarly other sums were quite wrong. After prolonged reflection, I took a notebook and recorded the various observations suggested by a preliminary examination. I counted all the figures on the page, and found there were 144. I then made a list of them, column by column, as follows:

201010453787243667351876936177952984
847201224675294851852723645223612111
588643110225011813414375659521401593
579131544939454410212524481006422l2

These 144 figures were distributed in the following order of frequency:

| Figure: | 1 | 2 | 4 | 5 | 3 | 7 | 0 | 6 | 8 | 9 |
|---|---|---|---|---|---|---|---|---|---|---|
| Times occurring: | 24 | 21 | 20 | 17 | 12 | 11 | 10 | 10 | 10 | 9 |

I became more and more convinced that there was a key to be discovered here. But the frequency of the ten figures led to nothing. In French, even in a long phrase, the whole of the 25 or 26 letters of the alphabet are rarely used. On the other hand, the shortest phrases require at least 16, 17, or 18 different letters. The famous line of Voltaire's, "Non, il n'est rien que Nanine n'honore," where the *n*'s and *e*'s form nearly half the total number of letters, absorbs 12 different letters. It is scarcely possible, except perhaps in Runic, to write phrases with a total of ten different characters. In French, when Arabic numerals are resorted to for secret writing, groups of two figures, at least, are generally employed.

Accordingly, I proceeded to divide the 144 figures into sections of two: 20, 10, 10, 45, and so on. There were 72 such groups, but on a calculation I found that there

were never more than two groups alike: two 10's, 45's, etc. Twenty-one groups were repeated, and occurred only once.

Matters were not making much headway. The letter occurring, in French, on an average once in six letters, or 17 per cent., I had no means of deciding which of the 21 repeated groups could represent that letter. I then divided the 144 figures into groups of three; there were 48. But my disappointment was, if possible, still greater, only one group being duplicated—201—all the rest occurring only once. I went on to form groups of four, then six, eight, and twelve figures, after which I stopped.

In each category I had, of course, arranged the groups in numerical order, from the lowest to the highest. On examining them in rotation, my attention was attracted more particularly by the three-figure groups, and for this reason: I was struck by the very small difference between certain groups, which followed at intervals of 1. Thus: 010, 011; 110, 111; 223, 224, 225; 453, 454; 642, 643, then with a lacuna 645; 851, 852. It then occurred to me to add together the three figures of the highest group: 984. $9+8+4=21$. The groups following this in value gave: 952, or $9+5+2=16$; 939, or $9+3+9=21$.

"Hallo!" I said to myself, "none of these groups seems to exceed 21 when I add the three figures composing it." And I thereupon reflected that in many French phrases the letter *z*, 25th of the alphabet, does not occur; nor *y*, the 24th; nor *x*, the 23rd; the last in common usage being *v*, the 22nd. Perhaps, after all, each of the three-figure groups represented the order of a letter in the alphabet.

Accordingly, I made the trial, and added the figures of each group. This resulted in the groups 010 and 100

producing a total sum of 1; 011 and 110, each 2; 111, and the two 201's, each 3. The group which inced the largest sum was not, as I had at first sup-ed, one of the highest, but 787=22. According to y new hypothesis, the plain text probably contained the letters *a* to *v*, if the language were French. I was disconcerted, however, to find that the most frequent total of the additions was not 5, corresponding to *e*, but 9, equalling *i*, according to my theory. "It might be Latin," I thought.

Another serious irregularity which came to light was that the most frequent totals after 9 were 15 (five times), corresponding to the letter *o*, and 21 (five times), to *u*. This is contrary to the rules of letter frequency, not only in French, where, after *e*, the most frequent letters are *n*, *a*, *i*, r, *s*, *t* (only the *i* of our three supposed letters has any place here), but also in Latin, where the letters should occur in the following order: *i*, *e*, *s*, *u*, *a*, *n*, *o*, *r*, etc. Still we have here the *i*, *u*, and *o*; and, in any case, it was desirable to put our supposition to the test.

The first three figures, 201=3, meant *c*; the next three, 010=*a*; then 453=12=1. The complete text proved to be: "*Calvisius, Opus Chronologicum. Bibliothèque Municipale.*"[1]

"So he has deposited the sequel to his secret in a volume," I thought. "And with a psychological foresight by no means stupid, he has not trusted to his memory, having had experience of the transformations which memory can effect in a name after a certain number

[1] NOTE BY TRANSLATOR.—There are two errors in the cryptogram, the final letter in *Calvisius* being represented by the group 936=18=*r*, and the third letter in *Municipale* by the group 454=13=*m*.

of years. Furthermore, he has chosen, as the receptacle of his confidences, a kind of work which is among the least consulted in a collection of books. Old books on law or theology are sometimes referred to, but ancient manuals of chronology are generally allowed to sleep in peace."

The same day I repaired to the Bibliothèque Municipale, and asked for the volume by Calvisius. It was a quarto tome bound in a thick leather cover. The cryptogram giving no indication of a page, I thought Pastoure must have made some secret entries on the first or last pages. There could be no question of sympathetic ink, since the necessary manipulations to make it visible were scarcely possible in a public reading-room. I expected to encounter some letters dotted in pencil, which if joined would form words and phrases; but my hope was vain, although I did not stop till I had scanned every page of the volume.

I was lost in conjecture, when the idea occurred to me to examine the inside of the back of the book, pressing the latter completely open. I perceived no note or anything else. Still reflecting, I looked at the inside cover. I noticed nothing at the beginning of the volume, but at the end, in the top corner, the paper was somewhat creased and seemed to have been moistened. Feeling the place with my fingers, I became aware of the existence, under the paper, of a hard object, small and slender. It was imperative that I should see what was hidden there, so I had the book put on one side, and went out to obtain a small sponge, a bottle of water, and a tube of gum.

Armed with these objects, I returned for my Calvisius, and, operating in the same way as Pastoure must have

done, but *vice versa*, I slipped the little sponge, soaked in water, into the suspicious place, and, while waiting for the moisture to take effect, I turned to p. 215 and plunged into the mysteries of the chronology of the Kings Ezechias and Nabonassar. When the desired result was obtained, I drew from its hiding-place a small safe key, which bore the name Bauche and a number. I re-gummed the paper, and, having returned the volume, went in quest of the Chief of the Secret Service.

"Have you any idea of the meaning of the figures?" he asked, shaking hands and indicating a seat.

"Why, yes," I replied. "They have enabled me to find this little metal object."

Picture the astonishment, then joy, of the Chief! He made me describe point by point the development of my discovery. Then he started on the chase, accompanied by his sleuth-hounds. Two days later, on opening my newspaper, I learnt that the thirteen hundred thousand francs which had been stolen had been recovered from the strong-room of a bank, where a compartment had been rented for fifteen years by a client about to start for Australia!

## Arabic Numerals.

I will now give another instance of success in the discovery or key to a cryptogram. It was in Arabic numerals. One day I received in the usual buff envelope the following text:[1]

67534 34959 61496 54860 46495 14564 46496 25350
65646 04950 45664 45966 49664 56649 60494 96646
59665 06249 50536 65060 57496 85849

[1] See footnote on p. 60.

I began by arranging the numbers in order of importance, from the lowest to the highest:

04950 06249 14564 25350 34959 45664 45966 46495
46496 49664 50536 54860 56649 57496 59665 60494
61496 65060 65646 67534 85849 96646

It will be noticed that two-thirds of these groups range from the 40 to the 60 thousands, and two—46495 and 46496—differ only by a unit. Have we here one of those systems of combined codes, involving much complication in their decipherment, but rarely used, by reason of their extreme complexity? On the other hand, these groups of five figures may be purely arbitrary.[1]

A striking peculiarity is the preponderance of 6's and 4's, which occur 30 and 24 times respectively, whereas 1, 2, and 7 each occur only twice, 8 three times, and 3 four times.

Perhaps it is possible to group the figures differently. Can we divide the text into groups of four figures? No, because there are 110 figures. Neither can we form groups of three. We can, however, form 55 groups of two figures:

67 53 43 49 59 61 49 65 48 60 46 49 51 45
64 46 49 62 53 50 65 64 60 49 50 45 66 44
59 66 49 66 45 66 49 60 49 49 66 46 59 66
50 62 49 50 53 66 50 60 57 49 68 58 49

Having made the division, we observe that the group 49 occurs twelve times, which is somewhat above the normal frequency of the letter *e* in a total of 55 groups. We will, therefore, assume provisionally that 49=*e*.

[1] NOTE BY TRANSLATOR.—At first sight this cryptogram would be hard to distinguish from the dictionary cipher described on p. 35.

We next note the frequency of the numbers 49 (supposed *e*) and 66 in the series 66, 49, 66, 45, 66, 49, 60, 49, 49, 66. As a general rule, only a consonant can follow the doubled *e* in English, and the most likely consonants are *n*, *t*, *d*, and *l*. The first three letters in the series might well be *d e d*, but the sequence would be: ? *d e* ? *e e d*, which gives an unusual number of *d*'s in a small group. Suppose we try the much more likely *n* as the equivalent of 66. We now have the series *n e n* ? *n e* ? *e e n*. The letter *t* seems to be the obvious consonant to fill the second lacuna, and by replacing the first by the vowel *i*, we get the complete word "nineteen," with *ne* as the tail-end of the preceding word. This promising result yields us the following four equivalents:

$$49=e;\ 45=i;\ 66=n;\ 60=t.$$

We proceed to make trials with these four letters, and observe that, preceding the word "nineteen," there occurs the group *t e* ? *i n* ? ? *n e* (60, 49, 50, 45, 66, 44, 59, 66, 49). The combination leads us to the idea that a date is in question, in which case there can be no hesitation in filling in the three blanks thus: "ted in June." Our theory is confirmed on examining the series following "nineteen"—viz., ? *u n d* ? *e d* (46, 59, 66, 50, 62, 49, 50), which is obviously "hundred."

Before going any farther, we summarise the results so far obtained, to wit:

$$d=50;\ e=49;\ h=46;\ i=45;\ j=44;\ n=66;\ r=62;\ t=60;$$

and are immediately struck by the fact that the numbers proceed in two regularly descending sequences, so that, without further trial, we are able to construct our alphabet:

| | | | |
|---|---|---|---|
| a=53 | h=46 | o=65 | v=58 |
| b=52 | i=45 | p=64 | w=57 |
| c=51 | j=44 | q=63 | x=56 |
| d=50 | k=43 | r=62 | y=55 |
| e=49 | l=68 | s=61 | z=54 |
| f=48 | m=67 | t=60 | |
| g=47 | n=66 | u=59 | |

The complete text of the cryptogram is then found to be: "Make use of the cipher adopted in June, nineteen hundred and twelve."

Once more I would ask my readers to refer to the Preface to this volume.

## In the Flour.

Towards eleven o'clock one night, as I was about to retire to bed, I heard a violent ring at the door, and a moment later my maid appeared and smilingly informed me that a policeman was asking for me. She knows I am always pleased to see a policeman, whose visit usually leads to certain little expeditions, which generally result in something unexpected with a spice of adventure.

I opened the door half-way and asked: "Who is there?" An unknown voice replied: "May I trouble you to come at once to you know where? You will then receive instructions." I hastened to the rendezvous—an office in which were congregated officials, detectives, and policemen. We exchanged greetings, and then, a large motor-car having drawn up at the entrance, some of the party—myself included—took our places in the vehicle, which moved off at great speed.

I thoroughly enjoyed the moonlight trip. We rushed through villages and a wood and climbed a hill, conversing in low tones all the time. Suddenly the car

stopped; we got out and proceeded on foot to a solitary house, where a bright light gleamed from a window on the ground floor. Somebody knocked at the door. While waiting for it to be opened, the leader of the expedition took me apart and informed me that a domiciliary search was about to be carried out in the rooms of a man who had been arrested that day, and who had strongly protested, saying he had been entrusted with a diplomatic mission. In the papers to be submitted to me for examination I was to search for proofs of that statement.

At last we were inside, and I was installed before the drawing-room table, on which documents in various languages were being piled. I buried myself in the tedious and wearying task of selection, putting on one side the screeds which seemed to deserve a more minute examination. I had no knowledge of the case or of the allegations against the arrested man.

But something was taking place at a table at the other end of the room, where a mysterious personage, who was addressed as "Mr. Deputy," was occupied in taking notes. It appeared that a considerably larger supply of provisions had been found in the rooms than was authorised by the Food Order; and a detective, who had a reputation for smartness, had brought in a tin box which had aroused his suspicions, though it apparently contained only flour. There was also a sack of flour in the larder, and this pound or so, kept separately in a writing desk, had puzzled him.

Contemplating the white powder with an air of absorption, the detective murmured: "Old flour sometimes contains worms; I wonder whether there are any here." And while "Mr. Deputy" and other functionaries looked

on with interest, he passed the flour through a sieve which he had just procured, letting the fine powder fall on to an open newspaper. Suddenly, a small cylindrical object appeared, a sort of case for steel pen nibs. With obvious delight the detective examined this object, cleaned and opened it, and, to our astonishment, produced therefrom two ribbons of pink paper, covered with characters in red ink, which he deferentially submitted to the "Deputy." The latter abandoned the air of indifference which he had hitherto displayed, and eagerly seized the two documents, which he began to study with deep interest.

Several of us formed a circle round him, and I was able to read over his shoulder one of the texts:

YOUWOULDHARDLYKNOWTHERE
WASAWARPROVISIONSAREPLEN
TIFULANDQUITECHEAP.

("You would hardly know there was a war. Provisions are plentiful and quite cheap.")

The other text began with the letters USLAAVI, followed by several more without any apparent significance, though the words IDOL and SHEBA stood out among the meaningless array.

Returning to my seat, I glanced from time to time at the "Deputy." He was comparing the English text with the strange medley on the second ribbon, and seemed to be making great efforts of memory. Finally, with the careworn air of one who has not solved a problem, he carefully pressed the two bands of paper into their case and put the latter into his pocket.

Two hours had elapsed since our arrival. The examination was finished and the seals affixed. The "Deputy" disappeared, and we rejoined our motor. Going off at

a good pace, under the light of the moon, I reached home about two in the morning.

The word *uslaavi* kept running through my head. Surely this was a Slavonic word meaning "glory." And could one connect it with the words "idol" and "Sheba"? It might be some ritual. On the other hand, the initial word of the mysterious writing might be a variant spelling of the Russian *uslovie*, meaning "terms." I imagined some semi-Oriental conspiracy, and was frankly seized with a tormenting desire to know the whole text of the document.

On the following morning I was immensely gratified on hearing a policeman announced. He came to invite me to call upon "Mr. Deputy" at an hotel near the station upon a matter of great urgency. I at once made my way thither, and was immediately introduced into the presence of that important man, who plunged without preamble into the business.

"You see," he said, "these are the two documents seized the other night. Each contains sixty-five letters. One is evidently the transcription of the other, to which it has been attached in error. I have compared the frequency of the letters in each, and here is the result:

| Letter: | A | B | C | D | E | F | G | H | I | J | K | L | M | N | O | P | Q | R | S | T | U | V | W | X | Y | Z | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| Plain text: | 7 | 0 | 1 | 3 | 6 | 1 | 0 | 3 | 4 | 0 | 1 | 4 | 0 | 4 | 5 | 3 | 1 | 5 | 3 | 3 | 4 | 1 | 4 | 0 | 2 | 0 | =65 |
| Cipher: | 7 | 1 | 3 | 5 | 7 | 0 | 1 | 3 | 4 | 0 | 2 | 3 | 0 | 3 | 7 | 1 | 0 | 2 | 7 | 3 | 3 | 1 | 0 | 0 | 1 | 1 | =65 |

We have to discover the key. I will not hide from you the fact that it will be difficult. But it must be done, for we have received similar writings from other sources, on the same kind of paper and in the same red ink. Try and get on the track of the method by which we can decipher them.

"For instance," he continued, "both texts have an

equal number of A's, H's, I's, and T's. There are n J's, M's, or X's in either. The cipher contains B, G, and Z which are absent from the plain text, and my theory i that these and other redundant letters, such as sever instead of six E's, are intended to play the part of letters which are present in the plain text but absent from the cipher."

I went home and shut myself in with what eagerness may be imagined. With the respect due to a relic, I drew the precious paper from my pocket case and began to study it. It read as follows:

U S L A A V I P I C A S D H O I O T O E I D O L Y
S H E B A H A D A D S T C E S R E N E S O N E Z
T U K U K D G O E L O A C S N R

A rapid glance led me to the conclusion that the three words which had seemed so portentous were merely accidental groups in the cryptogram, and I proceeded to experiment on the lines indicated by the "Deputy," comparing the text with the supposed transcription. I soon became convinced, however, of the absolute impossibility of arriving at any result in this way, and began trying other methods, putting aside the plain text.

There being sixty-five letters in the cryptogram, I temporarily decided against the theory of a grille, which usually requires a square number. The pairs OE, AD, ES, NE, and UK, which were repeated, gave me the idea of looking for a key-word (see p. 70), but the intervals between the repeated groups furnishing no satisfactory indication, I passed on to another hypothesis.

I noticed that the letter O occurred three times in a sequence of five letters, thus: O—O—O; and that the same

hing happened with A: A—A—A. This favoured the dea that the cipher had been composed with the aid of the system known as "dividers" (see p. 44)—that is, the required phrases had been written in very short lines and the letters separated into vertical sections, which, placed end to end, had formed the text now before my eyes. Accordingly, I began to cut the text into groups of letters, which I juxtaposed with the object of reconstructing the original text. As a nucleus I took the two groups just mentioned, and arranged them in vertical columns, thus:

| | |
|---|---|
| O | A |
| I | H |
| O | A |
| T | D |
| O | A |

Of these pairs only OA could form part of an English word, but the other two pairs could each be the final and initial letters of separate words. I first tried the word "board." There was only one B in the cryptogram, and the group containing it was YSHEB. Juxtaposed with the above, this produced the series: YOA, SIH, HOA, ETD, BOA. The first trigram being unsatisfactory, I abandoned the word "board," and tried "coa(st)," "roa(d)," etc., but obtained no good result, one or other of the trigrams produced always proving an impossible combination.

It then occurred to me that the five pairs already marked off need not necessarily be consecutive letters. The pair IH, for instance, was very unpromising, but the insertion of S or T, making ISH or ITH, would yield a far more hopeful basis. Accordingly, I decided

to interpose a third group *between* the first two, and hit upon STCES. This produced:

O S A
I T H
O C A
T E D
O S A

The second line could not be "w*ith*," for there was no W in the cryptogram, but it might be "*I th*ink." Adopting this idea, I succeeded quite easily in adding three more groups to my word-skeleton, to wit: VIPIC, ENESO, and UKUKD, and now had quite an imposing array:

O S A V E U
I T H I N K
O C A P E U
T E D I S K
O S A C O D

But I could get no farther; none of the remaining groups would fit in.

I had, of course, marked each group of letters in the cryptogram as I had used them, and now found that several letters were isolated, and that there were two groups with only four letters each, among some longer series, as yet untouched. I looked again at the partial reconstruction. Certainly the words "save," "think," and "cape" seemed too good to abandon. I wondered whether the last could be a part of the word "escape," and in order to test this, omitted my first column, OIOTO, substituting the two groups OEIDO and USLAA. These could only be adjusted by moving them down one line. The word "think" was now preceded by OU instead

of I, so I completed the word " you " by adding the group YSHEB, and now read the following:

```
          S A V E U
Y O U T H I N K
S E S C A P E U
H I L E D I S K
E D A S A C O D
B O A
```

The first line looked as though it might be " save us "; I had two spare S's, but neither of the groups containing them would suit the rest of the context. I then extended each of the last five columns by one letter downwards, following on from the ciphered text. This made the last line read: BOARDANG. Assuming that ANG was part of the name of a ship, the word " on " seemed the proper word to precede " board." To introduce this, I prefixed the two groups DHOIO and OACSN.

I was gratified to note that the second line now read " do you think "; but the third line was not so flawless, being HASESCAPEU. A glance at the last column showed me a means of correcting this: it was the group UKUKDG. By cutting off the first two letters and sliding the column up two lines, the K of " think " was preserved and the third line became " has escaped."

Success was now a foregone conclusion. It turned out that the original text had been written in lines of eleven letters, and had then been divided into vertical sections, of which the fifth had formed the first letters of the ciphered text, the eighth forming the second series, and so on. The first line, SAVEU, had to be abandoned, and the complete reconstructed text proved to be:

D O Y O U T H I N K Z
H A S E S C A P E D T
O C H I L E D I S G U
I S E D A S A C O O K
O N B O A R D A N E U
T R A L V E S S E L

("Do you think Z has escaped to Chile disguised as a cook on board a neutral vessel?")

The document in plain language which accompanied the above was merely intended to throw investigators off the scent. Having found the key, I lost all further interest in the cryptogram. I was not at all curious to learn for whom the message was intended, any more than the name of the person referred to as "Z." I concerned myself only with forwarding the whole—ciphered and plain texts, key and my rough working—to my immediate principal.[1]

## Ciphering by Means of a Key-Word.

Let us suppose that I am requested to decipher the following cryptogram:

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

There are 120 letters in the text. I note the following repetitions: *ip*, *dd*, *cc*, *fv*, *ds*, *sx*, *vp*, *vy*, *yp*, *afs*, *iys*, *cvp*. I calculate the intervals by making a pencil mark between the *i* and *p* in the repeated *ip*'s (there are three of them), and count the letters between the marks. I do the same

[1] The reader is again referred to the Preface and to the footnote on p. 48.

with the other identical groups, and draw up the following table:

| | | | | | |
|---|---|---|---|---|---|
| From | ip | to | ip | 63 letters, | or $3 \times 3 \times 7$ |
| ,, | ip | ,, | ip 33 | ,, | ,, $3 \times 11$ |
| ,, | dd | ,, | dd 33 | ,, | ,, $3 \times 11$ |
| ,, | dd | ,, | dd 62 | ,, | ,, $2 \times 31$ |
| ,, | cc | ,, | cc 90 | ,, | ,, $2 \times 3 \times 3 \times 5$ |
| ,, | fv | ,, | fv 48 | ,, | ,, $2 \times 2 \times 2 \times 2 \times 3$ |
| ,, | ds | ,, | ds 11 | ,, | ,, 11 |
| ,, | sx | ,, | sx 61 | ,, | ,, 61 |
| ,, | vp | ,, | vp 3 | ,, | ,, 3 |
| ,, | vp | ,, | vp 60 | ,, | ,, $2 \times 2 \times 3 \times 5$ |
| ,, | vy | ,, | vy 33 | ,, | ,, $3 \times 11$ |
| ,, | yb | ,, | yb 9 | ,, | ,, $3 \times 3$ |
| ,, | afs | ,, | afs 31 | ,, | ,, 31 |
| ,, | iys | ,, | iys 63 | ,, | ,, $3 \times 3 \times 7$ |
| ,, | cvp | ,, | cvp 60 | ,, | ,, $2 \times 2 \times 3 \times 5$ |

It will be noted that the factor 3 occurs in eleven out of the fifteen lines, so it is fairly safe to assume that a key-word has been used in coding the text, and that this word contains three letters. The question is: Can we discover this key-word and successfully decipher the text? We begin operations by copying the whole of our text into three columns—that is, in lines of three letters, numbering each line to facilitate reference:

| | | | |
|---|---|---|---|
| (1) i p b | (11) x p t | (21) v y b | (31) s x f |
| (2) v d d | (12) f h k | (22) i p q | (32) v y c |
| (3) z o b | (13) t d d | (23) o a a | (33) i p l |
| (4) g q w | (14) d s k | (24) s y b | (34) d d l |
| (5) w n z | (15) b p f | (25) a c r | (35) a h v |
| (6) s c c | (16) v p c | (26) p w h | (36) w c c |
| (7) z a f | (17) v p a | (27) s m l | (37) v p z |
| (8) s t x | (18) f s v | (28) s n c | (38) d q a |
| (9) v i y | (19) k z v | (29) t g k | (39) g t c. |
| (10) s d s | (20) e j t | (30) n i y | (40) w d j |

The first column begins with the letters *i v z*, and ends with *d g w*; the second column begins with *p d o*, and ends with *q t d*; and the third column begins with *b d b*, and ends with *a c j*.

The next thing is to calculate the frequencies in each column, which gives us the following table:

First column: *s*, *v*, 7 each; *d*, *i*, *w*, 3 each; *a*, *f*, *g*, *t*, *z*, 2 each; *b*, *e*, *k*, *n*, *o*, *p*, *x*, 1 each.
Second column: *p*, 8; *d*, 5; *c*, *y*, 3 each; *a*, *h*, *i*, *n*, *q*, *s*, *t*, 2 each; *g*, *j*, *m*, *o*, *w*, *x*, *z*, 1 each.
Third column: *c*, 6; *b*, 4; *a*, *f*, *k*, *l*, *v*, 3 each; *d*, *t*, *y*, *z*, 2 each; *h*, *j*, *q*, *r*, *s*, *w*, *x*, 1 each.

According to the law of frequencies, E is the commonest letter in English, followed by T or S; the commonest bigrams are TH and HE, and the most frequent trigram and three-letter word is THE. We may, therefore, assume that *p* in col. 2 stands for E. In col. 1 we hesitate between *s* and *v*, either of which may represent E. How can we arrive at a decision?

Looking down our table of numbered lines, we note that *p* (col. 2) is preceded by *v* three times (lines 16, 17, 37). If, therefore, *v* (col. 1) represents E, we get the combination (lines 16 and 17) EE?EE, which seems unlikely. Recalling that one of the commonest bigrams is HE, let us substitute H for E as the value of *v* in col. 1. In our list of repetitions we find the group *c v p*. If we adopt HE as the value of *v p*, we may easily infer that *c v p* equals THE, and this combination does, as a matter of fact, occur in lines 16-17 and 36-37, the *c* in col. 3 and *v p* in cols. 1 and 2 on the succeeding lines.

If we are satisfied that we have established one equivalent in each column, we can immediately ascertain the

key-word used from one or other of the ciphering tables at the end of this book, and armed with this word decipher the cryptogram automatically. The process will be explained in due course.

Meanwhile, it will be interesting to see whether it is possible to effect the decipherment without knowing the key-word, and without reference to the ciphering tables. We will suppose that, for some reason or other, we have not at our disposal such useful adjuncts for finding a key-word, and that we are without any clues outside the cryptogram itself to help us in the decipherment.[1]

So far, then, we have established the following:

*v* (col. 1)=H; *p* (col. 2)=E; *c* (col. 3)=T.

Our copy of the cryptogram, written in column form, with numbered lines, should have sufficient margin to attach the transcription of the letters as we ascertain them. We now attach the letter H to all the *v*'s in col. 1, E to the *p*'s in col. 2, and T to the *c*'s in col. 3. Lines 16-17 attract our attention at once with the group HETHE, which looks like a part of the word "whether." We therefore tentatively add W as the equivalent of *f* in col. 3, and R as that of *a* in the same column, duly marking accordingly all the similar letters in the column. The next thing we notice is the group WH?T in lines 31-32, and we decide to fill the blank with A, attaching this value to the three *y*'s occurring in the middle column.

For the moment we cannot go any farther in this direction, so we fall back on the law of frequencies, which, however, might easily prove a pitfall if we did not recog-

[1] NOTE BY TRANSLATOR.—This experiment is not in the French edition, but is added here to amplify the example.

nise the possibility of numerous exceptions. It will be remembered that the letters *s* and *v* each occur seven times in col. 1, so that we could not at first decide which was likely to stand for E. However, having eliminated *v* by attaching to it the value of H, and noted that the next letter after *s* and *v* in order of frequency in the column occurs only three times, we feel justified in assuming that *s*=E, and accordingly mark in seven E's in col. 1.

We now find that one of these E's occurs in line 10, and another in line 31, and that in each case it is preceded by the letters *i y* (in the second and third columns of the preceding line). As the most likely group of three letters ending with E, and repeated in the same text, is THE, we tentatively adopt T and H as the value of *i* (col. 2) and *y* (col. 3) respectively.

We are now able to resume the thread of our internal clues with the group (lines 7-10) WE??HTHE, which we construe as "weigh the," thus obtaining two new equivalents—*i.e.*, *t* (col. 2)=I; *x* (col. 3)=G.

It will, perhaps, be as well to tabulate the results so far obtained:

| *Col.* 1. | *Col.* 2. | *Col.* 3. |
|---|---|---|
| *s*=E | *i*=T | *a*=R |
| *v*=H | *p*=E | *c*=T |
| | *t*=I | *f*=W |
| | *y*=A | *x*=G |
| | | *y*=H |

A glance at the above will show us how we may find a possible short cut in our operations. It will be noted that in the middle column *i*=T and, *vice versa*, *t*=I. We can soon ascertain whether this principle applies throughout.

The result of a trial, as far as we can go, confirms this hypothesis, and we quickly arrive at some gratifying

results. Our attention is first directed to the group (lines 20-21) S?CHA?, which we identify as "such as." Isolated groups begin to join up, as, for instance, E?T?YWEIGHTHE?B?EC?, which can scarcely be anything else but "ently weigh the object," ENTLY being part of an adverb yet to be discovered. Always substituting the new equivalents as we establish them, we continue to build up words and phrases. From line 20 we can now read SUCH AS ?E ??Y REAS?NA??Y E??ECT F??? THE? WHAT, which is soon resolved into "such as we may reasonably expect from them what," etc. In fact, we automatically decipher the rest of the cryptogram as fast as we can note the equivalents, which leap to the eye with ever-increasing rapidity.

Although we have solved the cryptogram (and the reader should by now have the complete plain text before him if he has duly followed our reasoning with pencil and paper), we still do not know the key-word by which the cryptogram was ciphered and by which it could be deciphered without resorting to the long empirical process just described.

Let us go back to our starting-point—that is, to where we had established only one equivalent in each column—viz.:

Col. 1, $v$=H; col. 2, $p$=E; col. 3, $c$=T.

These three letters are presumed to have been ciphered from three separate cipher alphabets, each indicated by a letter. The three indicating letters taken together form the key-word, as agreed upon between the sender and recipient of the message. Our object is to ascertain this key-word.

Turning to Vigenère's ciphering table on p. 155, we first look along the top line of capitals for the letter H,

from which we proceed directly downwards in the column immediately below until we arrive at the letter *v*; and on the left of the line in which this occurs we find the capital letter O, which should be the first letter of the key-word.

We proceed in the same way with the letters E and *p*, producing L as the second letter of the key-word; and with T and *c*, which gives us J as the third letter. According to this, then, the key-word is OLJ.

Thus armed, and with Vigenère's table before us, we refer to the text of the cryptogram, and proceed as described on p. 28. We first write the key-word repeatedly under the text, thus:

i p b v d d z o b g q w, etc.
O L J O L J O L J O L J

Starting from the capital O in the column to the left of the table, we follow the horizontal line which it commands and stop at the letter *i*, the first letter in the ciphered text. From this *i* we ascend the column containing it until we reach the top line of capitals, where we find the letter U. This should be the first letter of the plain text. We continue in like manner with the second letter of the cryptogram and of the key-word, *p* and L, which produces E, and so on. We thus decipher as far as the following: u e s h s u l d s s f n.

But here we stop, for this array of letters makes no sense at all. We are evidently on the wrong track. What is the next thing to be done? Fortunately, Vigenère's table is not the only ciphering instrument known to cryptographers. Possibly the table used was that of Porta, which will be found on p. 153.

To use Porta's table, we take our first pair of equivalents—*i.e.*, *v*=H—and we look in the top line for which-

ever of the two letters belongs to the *first half* of the alphabet—in this case *h*; we then descend until we encounter in the same column the second letter of the pair, *v*. At the left of the double line containing the conjunction of the two letters will be found two capital letters, Y and Z. Either of these—it is immaterial which—will be the first letter of the key-word. We proceed similarly with the second pair, *e* and *p*, which yields as the second letter of the key-word E or F, while the third pair, *c* and *t*, gives us S or T as the last letter.

We will say, therefore, that the key-word is YES. As before, we write it repeatedly under the text of the cryptogram, and, following the instructions accompanying Porta's table, proceed as follows:

```
i p b v d d z o b g q w w n z s c c z a f, etc.
Y E S Y E S Y E S Y E S Y E S Y E S Y E S, etc.
w e s h o u l d s u f f i c i e n t l y w, etc.
```

In this way the complete text is deciphered easily: "We should sufficiently weigh the objects of our hope, whether they be such as we may reasonably expect from them what we propose in their fruition."

Our readers will doubtless recognise this as one of Addison's *obiter dicta*.

A good cryptographer would have detected at once that Porta's table was the more likely to have furnished the key-word, for the three initial pairs of equivalents which gave the clue to the cipher consisted of letters belonging to different halves of the alphabet, and Porta's table is so constructed that no letter can be represented by another in the same half of the alphabet, whereas in Vigenère's table there is no such restriction.

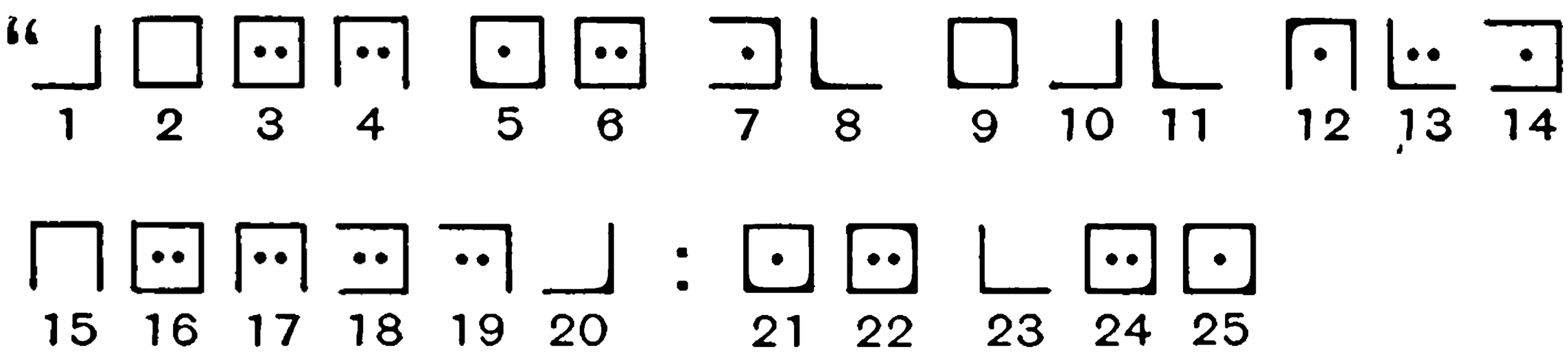
In order to decipher quickly by means of a table it is

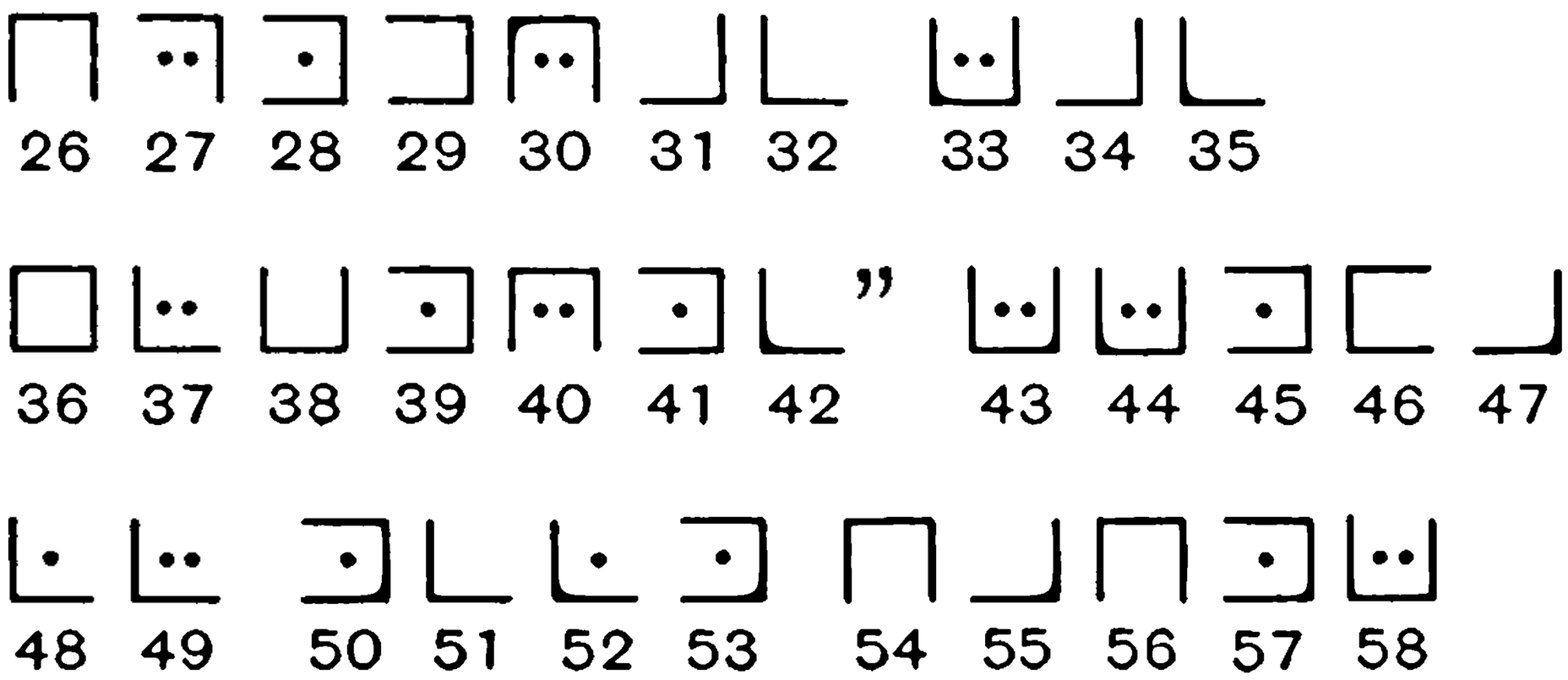
as well to write out the whole of the text of the cryptogram, accompanied by the key-word repeated throughout, then to proceed with the deciphering of all the letters under the first letter of the key-word—as, for instance, Y in YES—followed by those under the second letter, E, and finally those under the last, S. In the case of Vigenère's table a set square is a useful aid.

## A Billet-Doux.

A gentleman called upon me and complained that the behaviour of his son was not giving him entire satisfaction. It appeared that, while casually glancing through the textbooks used by the young man, who was studying for his B.A., he had found the missive which he now produced. Before mentioning the matter to his heir, he was anxious to know the meaning of the three lines in the document written in secret characters.

It was a sheet of blue paper, satined and perfumed, signed with the initial J, and contained the following (I have added numbers to the signs):



"Very good," I said to the anxious father; "will you kindly call to-morrow about two o'clock?"

Left to myself, I began to study the cryptogram.

The signs 1-42 are between quotation marks. The most frequently occurring sign is No. 7, which is repeated nine times in all—about the normal frequency of the letter E in a total of fifty-eight letters. One peculiarity struck me: the word starting from sign 43 begins with a doubled letter. This furnishes us with a useful piece of information—the text cannot be French, a language which does not contain words beginning with doubled letters.

Examples of such words occur in English—*eel*; in German, *Aal* (eel), *Aar* (eagle), *Aas* (carcase). Leaving aside Gaelic,[1] a language not very extensively used, the two principal languages which contain a considerable number of words of this sort are Russian and Spanish.

In Russian, a whole series of words begin with *vv*, the commonest being *vvedienie* (introduction). A certain number of other words begin with *ss*, among them *ssylka* (exile), and *ssora* (quarrel). Perhaps the word formed by the signs 43-47 is this very Russian word *ssora*. As if to confirm this, sign 45 is the most frequent in our text, and in Russia *o* is the commoneust letter. In this case, the word formed by signs 50-53 should be *odno* (one) or *okno* (window). But *n* is one of the most frequent letters in Russian, whereas sign 52, supposed to represent it, occurs only twice in the whole text. Furthermore, the word formed by signs 7 and 8, which, according to our supposition, should be *od* or *ok*, is meaningless in Russian. We must, therefore, abandon that language.

[1] NOTE BY TRANSLATOR.—Mention might be made of Dutch, with *oog* (eye), *een* (a, one), *uur* (hour), and other similar words.

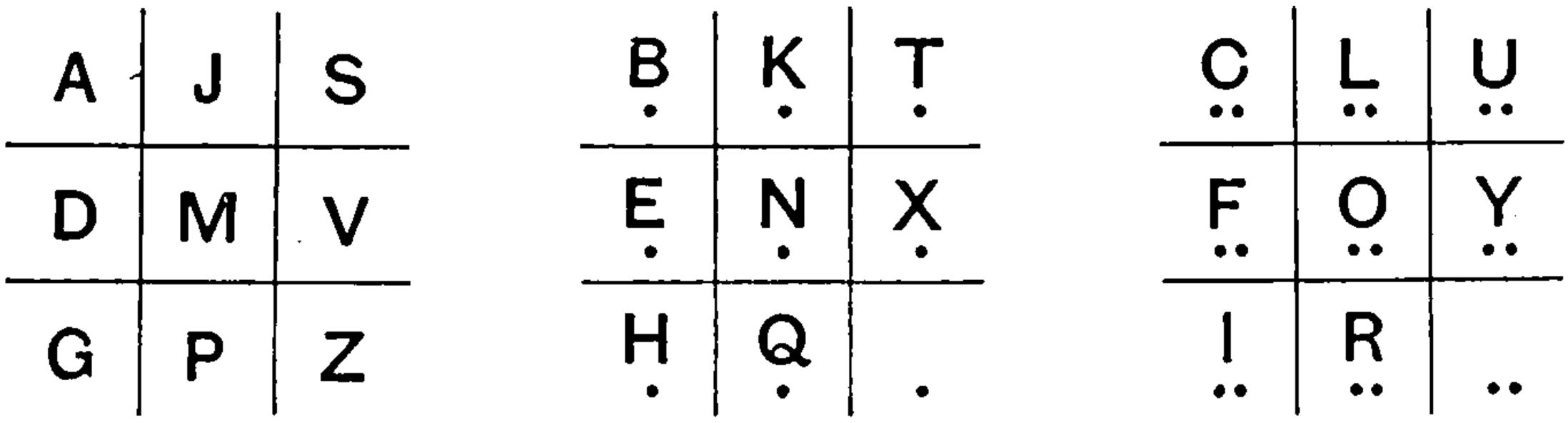
Let us now pass on to Spanish. Here the only letter which can be represented by the double initial 43 and 44 is *l*, and, in fact, *ll* forms the beginning of a large number of very common Spanish words. In this case, sign 45, the most frequent, would be *e*. These two letters, *l* and *e*, occur again at the end of the last word of our text, but in reversed order, *el*. This is in a word of five letters, of which the first is the same as the third, so that it can be no other than *papel* (paper).

Knowing now the letters *a* and *e*, we observe that signs 7 and 41, representing *e*, and 10, 31, and 34 (*a*) are all followed by the same final letter, which can only be *s*, in which case 33-35 is *las* (the) and 50-53 undoubtedly *este* (this). In our text we count nine *e*'s, seven *a*'s, and seven *s*'s. According to the rules of Spanish cryptography, *o* occurs as frequently in that language as *s*, if not more frequently. Now the sign occupying the fourth rank in order of frequency in our text is No. 3, which occurs five times. It is quite likely that this stands for *o*. We should then have for the word 23-25 SO?, doubtless *son* (are). With *n* tracked down, we identify 5-6 and 21-22 as *no* (not).

In Spanish, the commonest group of three letters by far is *que*; the word 12-14 ends with *e*, and, its first two letters being so far unknown to us, might well be *que* (that, than). This seems probable, for then 48-49 will be *tu* (thou, you). If 9-11 is *mas* (more), 36-42=MU?E?ES must be *mujeres* (women).

Summing up the letters so far obtained, we note that the alphabetically consecutive letters *m*, *n*, *o* each consist of a square, with this difference, that the square *m* is blank, *n* contains one dot, and *o* two dots. Comparing these with the other angles and open squares, with and

without dots, we are able to construct a symmetrical graph containing the complete alphabet, from which we can supply the letters still required to decipher the cryptogram:




The deciphered text proves to be as follows:

"Amor no es mas que porfia:
No son piedras las mujeres."
Lleva tu este papel.

("Love is nothing more than a squabble:
Women are not stones."
Keep this paper.)

When the fond parent returned, he was not particularly pleased to learn that he had had his son taught Spanish only to find him receiving such sentimental lessons as this on satin and scneted paper. I had a presentiment that his offspring was going to have a very uncomfortable interview. I retain one pleasant memory of my visitor: to his thanks he added a phrase which I hear none too often: "Don't forget to send me a note of your charges."

## A Little German.

In the German original of the *Diary of a Self-Observer*, by the celebrated physiognomist Jean-Gaspard Lavater, of Zurich, dated January 17. 1773, we find this sextet in cipher:

"Efs ekftfo Tubwc efs Fscf hkfcu,
Fs xbs hftffhofs woe hfmkfcu.
Fs ibssf efs Wotufscmkdilfku.
Ko tfkofs Obdiu tkdi pgu hfgsfwu !
Ft gsfwf tkdi, xfs ekftft mkftu,
Ebtt Fs, hmfkdi kin, wotufscmkdi ktu."

We begin by calculating the frequency of the letters in the text. The letter occurring oftenest is *f*, of which there are 33, whence we may deduce *f*=E. In actual practice, *e* in German has a frequency of 18 per cent., or an average of 1 in $5\frac{1}{2}$ letters. As this verse contains 156 letters, we ought to have here proportionately 18+10=28 E's. The proportion of E's, or letters supposed to be such, is therefore somewhat higher than the normal average.

According to an Austrian authority, Colonel Fleissner von Wostrowitz, the letters following E in order of frequency in German are: N I R S T. We will suppose, therefore, that *s*, the letter in our text occupying the second place in order of frequency (17 times), stands for N.

Next in order are *k* and *t*, each fifteen times. One of these should signify I, the other R. Then comes *u* (eleven times), probably equalling S. For the letter T we have the choice between *e*, *i*, and *o* (each eight times).

Let us confine ourselves at first to the two leading letters: *f*=E; *s*=N. We have the more reason to believe these equations correct from the circumstance that in German *n* is the most frequent terminal letter. Now, out of the thirty-three words comprised in the verse, ten do, in fact, end with our supposed N. Indeed, nine out of the ten end with EN, which is also in conformity with the rule.

Now that we have at our disposal two practically

certain letters, let us substitute the plain letters for the ciphered ones standing for them. We shall then have 33 E's+17 N's, making 50 known letters out of a total of 156. The undeciphered letters are replaced by dots:

"..en ..e.e. ..... .en En.e ..e..,
En."

Here we are brought to a stop; there is no such word as *en* in German, whether with or without a capital letter. We must have got on the wrong track through our too docile adherence to the rules given us. But not much harm is done, since we have only just started. Where is the fault?

For the moment we will retain our confidence in *e*, and assume that it is *n* which is out of place. A two-letter word in German beginning with *e* can only be *eh*, *ei*, *er*, or *es*, apart from such imported expressions as *en bloc*, *en gros*, and *en-tête*.

Can the word in question, then, be *Ei* (egg)? No, for it occurs three times in the sextet, and "egg" is not a term likely to be repeated so often in the poetic style. True, if this were the case, the fifth word in the first line might be *Eile* (haste), but the first word in the line, formed of the same letters, would then be *Lei*, a term non-existent. Can our word be *Eh* (before)? No, for although this would enable us to read the fifth word as *Ehre* (honour) and the first word as *Reh* (roebuck), we should have "roebuck" occurring twice in the same line, which is incredible; besides, the second *reh* is not written with a capital letter, and cannot, therefore, be a noun in German. Furthermore, the text would contain a disproportionate number of words ending with *eh*. Neither can the word be *Es*, for while the fifth word would then

be *Espe* (asp), the first word would be *Pes*, which is also non-existent in the German language.

Only *Er* is left, and we find this meets the case well. The fifth word in the first line now becomes *Er . e*, which can be no other than *Erde* (earth). The first word will be *Der* (the, who). Assuming, therefore, that *s*=R and *e*=D, the first line reads:

"Der d. e. e. ..... der Erde .. e..,"

Further trial favours the idea that the second word must be *diesen* (this), the value *t*=S being arrived at from the first word in the fifth line: *Ft*=probably ES. That *k*=I in the word *diesen* is confirmed by the second word in the fourth line, which, with the letters so far ascertained, gives us *tfkofs*=*seiner* (his), and by the preceding word, *Ko*=*In* (in).

From the letters already deciphered we make the following discovery: *f*=E—that is, the ciphered letter stands for the letter preceding it in the alphabet; *s*=R, *e*=D, the same remark applying in each case. Perhaps it will be the same for the whole of the alphabet. We accordingly make the trial, checking the result of the equations from time to time:

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

It will be noted that the letters *a*, *q*, *r*, *y*, and *z* of the secret alphabet, corresponding to the plain letters Z, P, Q, X, and Y, are absent from the sextet, which we now read as follows:

"Der diesen Staub der Erde giebt,
Er war geseegner und geliebt.
Er harre der Unsterblichkeit.
In seiner Nacht sich oft gefreut.
Es freue sich, wer dieses liest,
Dass Er, gleich ihm, unsterblich ist."

In English:

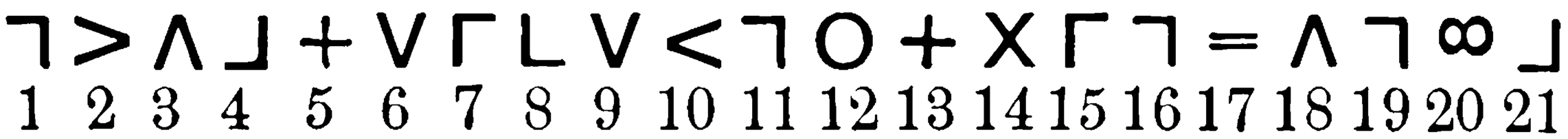
"He who gives this dust to earth,
Was blessed and beloved.
He waits for immortality.
In his night he has oft rejoiced.
Let him who reads these lines rejoice,
That he, like him, is immortal."

The same work contains a score of ciphered passages, some of which are less easy to read than the above example.

N.B.—It is worth noting as a rare phenomenon that this sextet contains only German terms. It is far more usual in German texts to find a proportion of pure French words varying from 5 to 8 per cent., or more.

## A Short Cut.

I have just received a picture postcard from a young friend who signs himself "M. J." It depicts a pretty rose-covered cottage near Penzance, in Cornwall. On the address side, in the part reserved for correspondence, appears the following. I number the signs for reference:



We begin by constructing a numerical table of all the signs in order of frequency:

| *Sign.* | *Times.* | *Sign.* | *Times.* | *Sign.* | *Times.* |
|---|---|---|---|---|---|
| + | 9 | 8 | 4 | ⌟ | 2 |
| ⅂ | 8 | < | 3 | X | 2 |
| V | 7 | □ | 3 | T | 1 |
| ⌜ | 4 | · \| | 2 | ⊥ | 1 |
| L | 4 | O | 2 | = | 1 |
| Λ | 4 | > | 2 | – | 1 |

We assume that +=E. According to the laws of letter frequency in English, ⅂, the second sign in the table, should be S, T, or A. Signs 30 and 31 would then represent either ES, ET, or EA, any one of which is possible. There being no other similar juxtapositions, we are unable for the moment to establish the point.

We observe that three of our supposed E's are followed by the sign V, which may, according to order of frequency, stand for R, D, N, A, S, etc. This sign occurs no fewer than seven times in the cryptogram, but as yet we are unable to establish from its connections more than that it must be a consonant, and that the sign L (Nos. 8 and 48) is probably a vowel.

Let us now try a trail that has proved very useful in deciphering other examples—the discovery of the trigram THE, which, of course, cannot be said with certainty to be present in the text, but is so frequent a group in English as to make its presence a very reasonable assumption. We have in the cryptogram nine triplets ending with E, of which 28.29.30 begin with E and 42.43.44 begin with a supposed vowel. This leaves us with seven groups, two of which start with the sign V, which we have

already noted as a consonant often following E, and three begin with the sign ∞. These three triplets are 20.21.22, 32.33.34, and 53.54.55. Assuming that one of the triplets is THE, we have for the value H to choose between the signs ⌋, ⊤, and □. The first, ⌋, occurs twice before E, while the last, □, occurs once before and once after E. The second sign, ⊤, appears only once in the cryptogram. We are therefore inclined to assume the sign ⌋ to represent H.

Just as we are about to examine the possibilities of the triplets 44.45.46 and 51.52.53, which open with E and end with T, it occurs to us to search for an external clue. Turning the card, we observe the name "Penzance," which suggests a short cut. Our young correspondent has possibly mentioned the name in his message. We note that the word contains two E's, separated by five other letters. Examining the cryptogram, we find that there really is such a group 21-28. The two N's are represented by the sign V at 23 and 26. The initial P, however, proves to be the sign ⌋, which we had assumed to be H. This letter must, therefore, be one of the two signs □ or ⊤—that is, if the trigram THE occurs in the text.

The results so far established are as follows:

⌝=A, |=C, +=E, V=N, ⌋=P, ∞=T, −=Z.

Having marked the equivalents in the cryptogram as far as we have gone, we note that the group following "Penzance"—*i.e.*, 29-35—is ?EAT?E?, which it does not require much imagination to transform into WEATHER. From A?EW (11-14)="a few" to ?A?N?F?CENT (36-46)="magnificent," we reach our goal in three or

four steps, thanks to our short cut, and finally read the following:

"Am spending a few days at Penzance. Weather magnificent. Kindest regards."

## A Dictionary Code.

The following cryptogram is handed to me:

5761 3922 7642 0001 9219 6448 6016 4570 4368 7159
8686 8576 1378 2799 6018 4212 3940 0644 7262 8686
7670 4049 3261 4176 6638 4833 4827 0001 3696 6062
8686 2137 4049 2485 7948 0300 9712 0300 4212 9576
2475 8576 8337 0702 9185

In practice, this kind of cipher, which is very commonly used, is subject to arbitrary complications, and it may well prove quite a long task to restore each number to its original integrity, the sender having probably shuffled the four figures throughout in accordance with a formula agreed upon with the recipient.

But as it is always best to proceed from the simple to the complex, we will act on the preliminary assumption that the above numbers have not been changed, and are to be read just as we see them. We begin by making a list of the forty-five numbers, of which the lowest is 0001 and the highest 9712, arranging them in numerical order:

| | | | | |
|---|---|---|---|---|
| 0001 | 2485 | 4212 | 6062 | 8576 |
| 0001 | 2799 | 4212 | 6448 | 8576 |
| 0300 | 3261 | 4368 | 6638 | 8686 |
| 0300 | 3696 | 4570 | 7159 | 8686 |
| 0644 | 3922 | 4827 | 7262 | 8686 |
| 0702 | 3940 | 4833 | 7642 | 9185 |
| 1378 | 4049 | 5761 | 7670 | 9219 |
| 2137 | 4049 | 6016 | 7948 | 9576 |
| 2475 | 4176 | 6018 | 8337 | 9712 |

We apparently have to deal with a dictionary code, numbered from 1 to 10,000. Faced with a system like this, so simple and regular, one has to be on the alert lest it should conceal a trap. On one occasion, in an example which seemed quite as clear, I produced the reading: "Either X or Y warmly recommended." But subsequently I ascertained that the numbers had been "cooked" in the cipher, and that the true reading of the phrase was: "Both X and Y absolutely unknown."

Assuming in the present case, however, that the numbers are unaltered, we make the following observations: The number 0001 occurs twice, as do 0300, 4049, 4212, and 8576, while 8686 appears three times. The following pairs occur with very short intervals:

2475 and 2485, 3922 and 3940, 4827 and 4833,
6016 and 6018, 7642 and 7670, 9185 and 9219.

All this should be borne in mind, as it will probably prove useful.

We will now suppose that the number 0001 represents the letter A. We next take a small English dictionary and begin on the real work, making use also of the table at the end of this volume giving the proportion of words in Webster's Dictionary, classified according to their initials.[1]

From this table we note that the middle of Webster's Dictionary occurs numerically about half-way through L. But as this bulky tome is rather difficult to handle, we will use in preference a small dictionary suitable for rapid reference, though there is the inevitable drawback that the proportions of the letters vary to some extent with every dictionary, particularly in the middle of the alphabet.

[1] See p. 138.

We have begun by supposing that 0001=A. The next thing is to look for certain words which one would expect to find in most texts, as, for instance, the prepositions "of" and "to," the conjunction "and," the article "the," etc. Now, we learn from the table that in Webster's Dictionary, theoretically divided into a hundred equal sections, words beginning with O are comprised between the 58 and 61 per cent. marks. If the dictionary were divided into 10,000 parts instead of a hundred, the O section would be found between 5,800 and 6,100. In the list of numbers in our ciphered text we observe three occurring in this section: 6016, 6018, and 6062. Can one of these be OF? From its position we tentatively give the first this reading, and, on looking up "of" in the dictionary, our attention is drawn to the words closely following it: "off," "offend," "offensive." Surely this last—a common military term—is the equivalent of our second presumed O number, 6018. At any rate, the close proximity of the two numbers is a promising indication that our surmise is correct.

It will be useful now to seek such words as "the" and "to." The dictionary table shows T's in Webster to fall between 8715 and 9298 (substituting the 10,000 division for the percentages). As already noted, the number 8576 appears twice in the text and 8686 three times. These numbers are outside the T limits, and fall in the S section. Nevertheless, allowance has to be made for variations in the proportion of letters according to the dictionary used, and our cryptogram was probably not coded from Webster. We may, accordingly, venture to suppose that either 8576 or 8686 represents THE.

Referring to the text of the cryptogram, we find that these two numbers occur consecutively—8686, 8576—

which favours the assumption that the first equals TO and the second THE.

Another number occurring twice is 0300. The dictionary shows A to extend to 6·43 per cent. of Webster, or 643 per 10,000, and as "and" is about half-way through the A section, this word may well be the reading of 0300.

There are two other pairs of duplicate numbers—4049 and 4212. These fall somewhere about H, but there are so many likely words with this initial, such as HAVE, HAS, HE, HIM, etc., that it is difficult to favour any isolated word without the assistance of the context.

It will be as well at this juncture to endeavour to construct a part of the text by using the words so far obtained as a skeleton. Can we fill in the lacunæ in the group TO THE . . . . . OFFENSIVE, for instance? The two missing words are represented by the numbers 1378 and 2799. This latter falls among the E's. We have, then, E . . . OFFENSIVE—doubtless "enemy offensive." It happens that the other number, 1378, which falls under C, is almost half-way between 0000 (A) and 2799 (ENEMY), and the only likely word in the dictionary occurring in this position is "coming." We may, therefore, not be far wrong in reading this group: TO THE COMING ENEMY OFFENSIVE.

Another group that attracts our attention is AND . . . . AND. This is followed by the number 4212, which occurs again after the word "offensive." Numerically, the number is nearly half-way to 8576, to which we have attached the reading THE. Allowing for a small margin, as we did in the case of the T's, No. 4212 should coincide with the beginning of I's rather than the H's. Tentatively adopting the pronoun "I" for this number, we

next note that the number occurring between the two AND's is 9712, the highest in the cryptogram. As this is near the end of the alphabet, the pronoun "you" seems to be indicated, and we have: AND YOU AND I.

The number following "I" in the above group is 9576, the second highest, and therefore probably a W word, perhaps WERE or WILL. It is followed by 2475, an undoubted D word, and the next is THE. What can this D word be? Alphabetically it occurs somewhere between "coming" (1378) and "enemy" (2799). The interval between these two is 1421, and the difference between 1378 and 2475 is 1097, or roughly three-fourths of the interval. This brings us among the DI's or DO's. There is another number in the text occupying about the same dictionary position—*i.e.*, 2485. We have, in fact, 2475 and 2485, one of which might be DO. Suppose we give this reading to the second *pro tem.*, and look for a word closely preceding it which will suit our context. The dictionary shows us "divulge" and "divide." The group we are studying may therefore be: AND YOU AND I WILL DIVIDE THE.

We must proceed patiently in this way, calculating intervals and working out the position of each letter. We shall, of course, make a false step occasionally, but every word established strengthens our foothold, and the context guides us more and more surely as we fill in the gaps.

In this way, the three numbers 8337, 0702, and 9185, which follow the group "and you and I will divide the," are quickly resolved into SUM BETWEEN US, the suggestion in the context, coupled with the approximate dictionary positions of the numbers, effectively narrowing our choice. After going on to establish some G and H

words, such as HIM, HAVE, and GOOD, only a very slight imagination is required to convert such a group as A GOOD O . . . TO into "a good opportunity to," and eventually we produce the complete reading of the cryptogram as follows:

"Mi . . . has secured a valuable piece of information in regard to the coming enemy offensive. I have been requested to send him five hundred pounds. It is a good opportunity to denounce him. Do so, and you and I will divide the sum between us."

Thus, all the words are deciphered with the exception of the first. The number of this, 5761, occupies a position relative to 4833 (IT) and 6016 (OF), its nearest neighbours numerically, which brings it among the ME's or MI's. It is apparently the name of an individual. We might, by a minute investigation, identify so much of the name as to reveal the nationality of its owner, but it does not matter much to us. The person who gave me the document to decipher will probably be in a position to throw light on the individual; I am not competent to do so.

In ciphers of this sort a ready reckoner is a useful adjunct to facilitate the calculation of letters, proportions, and intervals.

## The Sliding Rules.

A copy of the *Berliner Tageblatt* has been put into my hands with the object of verifying a suspicion that some hidden message has been concealed therein, the copy having been intercepted on its way to a quarter believed to be harbouring enemy agents.

Opening the journal, I observe an article with big headlines announcing an enemy victory. The article is heavily marked with red crayon. Concluding that this

is a mere blind, I scrutinize every page, column after column, until, on the last page, among the Stock Exchange quotations, my attention is attracted by a certain number of figures marked with dots in ink.

Taking a sheet of plain paper, I make a careful copy of all the figures marked in order as follows:

1 8 5 6 2 9 5 9 3 7 6 9 3 6 7 4 1 8 7 4 2 2 7 4 2 5 5 5
3 7 5 4 2 8 6 9 4 3 6 7 3 5 6 2 2 1 6 6 2 6 7 0 3 5 6 7
3 7 5 8 3 9 6 9 3 2 4 4 3 2 6 8 2 9 7 9 3 6 6 3 4 1 6 3
3 1 7 4 2 5 5 9 2 8 6 8 3 2 7 7 8 1 1 9 6 6 2 3 6 3 2 8
7 6 2 9 6 5 3 2 7 6 3 1 6 0 2 5 6 1 3 6 8 0 2 2 7 6 1 7
2 2 7 6 2 2 7 2 4 2 7 4 2 5 6 3 3 1 6 1 3 5 5 9 1 8 5 8
4 2 5 6 4 2 6 7 1 8 7 9 2 3 6 9 3 8 7 2 3 7 6 2 3 6 6 3
2 4 6 8 1 8 6 6 5 3 2 4 7 3 2 6 7 6 3 9 6 1 2 1 6 6

Altogether there are 222 figures. Have we here a dictionary code? No, because 222 cannot be divided by 5 or 4. It is, however, divisible by 6 or 3. With six figures a dictionary of a million words (including 000,000) can be constructed, but this would be too many. With three figures one might compose a dictionary of a thousand words (including 000), but this is obviously too few for practical purposes.

A dictionary code being apparently out of the question, we entertain the theory of a system of ciphering by groups of three figures, each group representing a letter. We accordingly make a trial, dividing the figures into groups of three, which we arrange in order from the lowest to the highest.

Of the seventy-four groups thus obtained, we note that six are duplicated—viz., 166, 267, 276, 425, 532, and 742.

If we admit that each of these seventy-four groups of three figures represents a letter, we shall require a pro-

portion of at least nine E's, and the total number of repeated groups does not reach that. Then how are we to get over the great difficulty of identifying the alphabetical value of the sixty-two groups not repeated?

Let us put aside for the moment our notes on the three-figure groups, after adding thereto the observation that the list shows a certain number of groups which differ from each other only by single units, to wit: 135-136, 255-256, 267-268, 296-297, 316-317, 366-367, 591-592-593, 622-623, 762-763, 868-869.

While being almost certain that this will not be of much use to us, we will hold it in reserve as a possible forlorn hope. It is just possible, too, that these three-figure groups may stand for syllables, but even so the repetitions should still be more frequent.

It then occurs to us to add the figures of each group to see whether the totals will correspond to the numerical rank of the letters in the alphabet. Putting the larger numbers to the test, we get the equivalents 938 (9+3+8) =20, corresponding to T; 879=24=X, etc.

So far, so good. On trying the small numbers, however, we meet with a check, there being no A, B, C, D, or even E; in fact, no number produces a lower total than 7 (160) or 8 (035). Now, a text of such a length without a single E will scarcely be found in any language of Western Europe.

It is evident that we must pursue our researches in a different direction. The number 222 is divisible by 2. We will, therefore, divide our cryptogram into sections of two figures, classifying them in numerical order. This enables us to produce the following table of frequencies:

| | | | |
|---|---|---|---|
| 17 once | 32 4 times | 55 once | 69 4 times |
| 18 5 times | 35 3 ,, | 56 twice | 70 once |
| 19 once | 36 4 ,, | 58 ,, | 72 twice |
| 21 twice | 37 4 ,, | 59 3 times | 73 once |
| 22 4 times | 38 once | 60 once | 74 5 times |
| 23 twice | 39 twice | 61 3 times | 76 5 ,, |
| 24 ,, | 41 once | 62 twice | 77 once |
| 25 4 times | 42 3 times | 63 5 times | 79 twice |
| 26 twice | 43 once | 65 once | 80 once. |
| 28 3 times | 44 ,, | 66 4 times | 81 ,, |
| 29 3 ,, | 53 ,, | 67 3 ,, | |
| 31 3 ,, | 54 ,, | 68 3 ,, | |

Out of the 111 groups of two figures obtained, we ought to find one repeated at least a dozen times to represent E. But no group occurs more than five times. There are four with this proportion—viz., 18, 63, 74, and 76. Can they all mean E? This would make a total of twenty E's, a proportion which, while not beyond the bounds of reason, is yet somewhat too high for the length of the text.

Have we to deal with a cipher of several alphabets, as the total of forty-six different numbers might lead us to suppose? But how many alphabets? We must endeavour to find out. While doing so we note that the consecutive groups 74.25 are repeated at two other places, that the consecutive groups 21.66, 36.63, 63.31, and 22.76 each occur twice, and that the groups 67.35 and 32.68 are repeated, but in inverse order.

If we calculate the intervals between the repeated pairs, as described on p. 70, we find thirty-two numbers between the first and second pairs, 74.25, and—a curious coincidence—a similar number between the second and third pairs, 74.25; thirty-six numbers between 63.31 and 63.31; 87 between 21.66 and 21.66; 58 between 36.63 and 36.63; and 3 between 22.76 and 22.76.[1]

[1] The interval is calculated, as already explained, from a stroke dividing the first pair to a corresponding stroke dividing the second pair.

Out of the above intervals, three are divisible by 4 and three by 3, which would suggest a possible key-word of three or four letters. On splitting up the cryptogram into segments of three (supposed) letters, and arranging them in columns, we find that col. 1 alone has no fewer than twenty-seven different numbers, which cannot, therefore, represent as many different letters. Furthermore, no number has a higher frequency than three in any of the columns, and, with the exception of 59, which is the only number occurring three times in col. 1, and might, therefore, stand for E, the frequencies of 3, 2, and 1 are too evenly dispersed to furnish any clue as to their significance.

The solid features to which we must revert are the repetitions of the groups 74.25, 21.66, 36.63, 63.31, and 22.76. These doubtless represent such frequently occurring bigrams as TH, ER (or E with another letter), IN, etc.

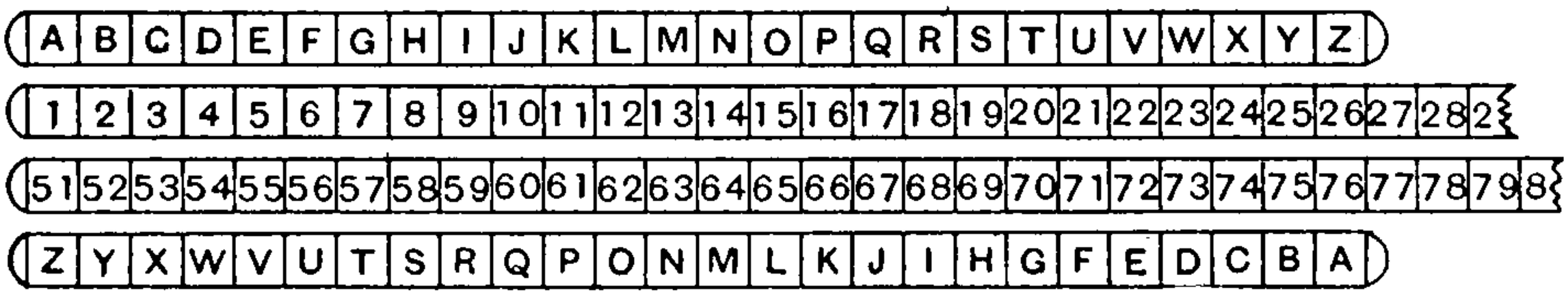
An examination of the table of frequencies set out above reveals a peculiarity which may help to put us on the right track. It will be observed that there is no number lower than 17 and none higher than 81. The cryptogram may, therefore, have been ciphered by means of the groove or slide system.

The numerical slide system is constructed as follows: Take a piece of cardboard, oblong in shape, and at each end cut a certain number of slits. Into these slits insert long strips of stiff paper or parchment, some of which are inscribed with the alphabet and others with a series of numbers. Calendars are sometimes made on the same principle. By sliding backwards or forwards a slip bearing the alphabet, the letters thereon are made to coincide with different figures on the numerical slips, and

by this means a great variety of secret alphabets represented by numbers can be formed.

Where the respective positions of the strips as adopted at the beginning remain unchanged to the end of the cryptogram, the system is that of numerical fixed slides. When the respective positions of the strips are changed once or several times during the process of ciphering, we are faced with the system of numerical movable slides.

Let us examine the simpler system, that of fixed slides; and, since strips of paper or parchment are very fragile and easily torn, we will replace the whole by small rules of plain wood, two long and two short. We graduate all the rules by means of equidistant strokes, and in the divisions thus made we inscribe, on one of the two longer strips, the numbers 1 to 50, and on the other 51 to 100. On one of the short rules we inscribe the alphabet in the usual order, and on the other the alphabet in reversed order: Z, Y, X, etc. The diagram will better illustrate the part which the four rules can play in ciphering.




As an example, to cipher the word "deed" from the upper alphabet, we can employ at will either of the two numbers falling under each letter, transcribing the word 04.56.06.55, for instance. Using the lower alphabet, we have the choice between the two lines of figures above it, and may produce 73.22.72.23. The two different letters in the word "deed" may, therefore, be represented by eight different numbers.

As regards the system of movable rules, we give farther on, in the chapter entitled "Spilt Ink," a proximate instance, coded by letters instead of numbers.

In what way must we adjust our wooden rules or slides in order to decipher the cryptogram which we are now studying? We have already noted that the double group 74.25 occurs three times in the cryptogram. Let us now endeavour to ascertain whether it corresponds to the frequently occurring bigram TH. For this purpose we adjust the upper alphabet in such a way that T is above 74 in the lower numerical strip. We then move the upper numerical strip until the 25 thereon falls below H in the upper alphabet.

Beginning from the first pair, 74.25, which occurs in the first line of the cryptogram, we decipher AT as the two letters following TH. The next number, 54, falls outside the range of the alphabet. Ignoring this for the moment, we proceed: KOZMRHDLIP. Plainly we are on the wrong track.

Suppose we try another of the repeated groups, 21.66. This pair occurs at the end of the cryptogram. Adjusting the rule so that T and H in the upper alphabet correspond to 21 and 66 in the upper and lower numerical rules, we proceed to work backward, but are brought to an abrupt pause by the number 39, which is far beyond the range. On jumping over this, we produce nothing more promising than WOYR?CTH.

There are other duplicated pairs open to investigation, but the fact that our first essay, though a failure, produced initially the combination THAT induces us to restore the rules to the position 74.25=TH. This time we take the second pair, which occurs in the fourth line

CALIFORNIA
Return Postage Guaranteed

of the cryptogram. We get as far as THEKNOW?BLFI, and are again baffled. Yet there are the initial letters that seem so promising.

Suppose we revert to the combination THAT (presumed) in the first line and try the letters preceding it. We get ETATSOTELBA. Reversing this, we recognise "Able to state." At last we are making definite progress. But we have now reached the beginning of the text; and when we attempt to go in the other direction, we get a mixture of comprehensible and incomprehensible groups, with occasional numbers which have no corresponding letter. Such numbers are 17, 44, 53, 54, and 81.

These perplexing numbers must be either punctuation marks, blank letters, or—as we are beginning to suspect—"changes of alphabet." In two cases, certainly, such numbers separate intelligible from non-intelligible groups. Perhaps Nos. 54 and 81, occurring, as they do, on the lower numerical rule, are intended to indicate that the groups following are to be read from the *lower* alphabetic rule, in which case 17 and 44 will refer to a change to the upper alphabet.

On putting this theory to the test, working from No. 54, we are agreeably surprised to encounter the group PLANISWORKING. By continuing to follow the indications given by the key numbers, we are very soon in possession of the plain text complete, as follows:

"Able to state that plan is working well. Only six in the know. Your people must have everything ready by May fourth. Signal three two.

What the further history of this interesting plot was I am unable to state. We may at least suppose that

the interception and disclosure of the message went far to bring it to an untimely end.

## A Contribution to History.

The post brings me a letter; I recognise in the address the handwriting of a well-known historian, with whom, however, I have not yet been in correspondence. On opening the envelope, I find therein nothing but a sheet of paper containing a cryptogram in the same writing. Who would have expected a communication in cipher from such a man? Decidedly, everybody is taking up cryptography nowadays. Let us see what he has to say:

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

The cryptogram contains, in all, 136 letters. A scrutiny of the text shows the following repetitions: OU (4 times), US (3), NS, NL, CM, AC, CP, EV, RI, GE, EG, GU, UU (4), SS, SD, UO, BA, IK (3), KA, AG, AF, IU, UI, II, GO.

We divide the two letters of the first OU with a stroke, do the same with the second, third, and fourth, and then count the letters between the strokes. Proceeding likewise with the other repeated pairs, we establish the following table (the figures represent the number of letters in the interval from one pair to its repetition):

| | | | |
|---|---|---|---|
| ou–ou | 24 or $2\times2\times2\times3$ | uu–uu | 1 or 1 |
| ,, | 26 ,, $2\times13$ | ,, | 72 ,, $2\times2\times2\times3\times3$ |
| ,, | 66 ,, $2\times3\times11$ | ss–ss | 26 ,, $2\times13$ |
| us–us | 24 ,, $2\times2\times2\times3$ | sd–sd | 26 ,, $2\times13$ |
| ,, | 63 ,, $3\times3\times7$ | uo–uo | 64 ,, $2\times2\times2\times2\times2\times2$ |
| ns–ns | 47 ,, 47 | ba–ba | 64 ,, $2\times2\times2\times2\times2\times2$ |
| nl–nl | 108 ,, $2\times2\times3\times3\times3$ | ik–ik | 42 ,, $2\times3\times7$ |
| cm–cm | 79 ,, 79 | ,, | 12 ,, $2\times2\times3$ |
| ac–ac | 37 ,, 37 | ka–ka | 54 ,, $2\times3\times3\times3$ |
| cp–cp | 37 ,, 37 | ag–ag | 49 ,, $7\times7$ |
| ev–ev | 55 ,, $5\times11$ | af–af | 15 ,, $3\times5$ |
| ri–ri | 48 ,, $2\times2\times2\times2\times3$ | iu–iu | 8 ,, $2\times2\times2$ |
| ge–ge | 48 ,, $2\times2\times2\times2\times3$ | ui–ui | 10 ,, $2\times5$ |
| eg–eg | 26 ,, $2\times13$ | ii–ii | 3 ,, 3 |
| gu–gu | 26 ,, $2\times13$ | go–go | 5 ,, 5 |
| uu–uu | 3 ,, 3 | | |

It will be noted that the factor 2 is common to 19 out of the above 31 intervals, and if there were no other important factor we should be tempted to assume a key-word of two letters; but the factor 3 is common to 14 of the intervals, which is nearly a half, and in any case there are bound to be a considerable proportion of 2's, because that factor must appear in every even number. The probability that a key-word of three letters has been used is strengthened by the fact that there are some repeated trigrams in the cryptogram, two of which, OUS and IKA, have intervals divisible by three.

Assuming, therefore, a key-word of three letters, we copy the whole of the text into three columns—that is, in sections of three letters, each forming a line, and number the lines for convenient reference. A sufficient margin should be left to attach the transcription, as described in the chapter on "Ciphering by Means of a Key-Word."

| | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|
| (1) | o | u | s | (17) | y | u | o | (33) | m | c | j |
| (2) | z | e | h | (18) | u | c | n | (34) | c | a | f |
| (3) | n | s | o | (19) | s | a | c | (35) | w | s | i |
| (4) | b | o | n | (20) | p | i | a | (36) | u | t | u |
| (5) | l | h | h | (21) | m | e | g | (37) | i | i | k |
| (6) | i | c | m | (22) | u | v | b | (38) | i | i | u |
| (7) | a | c | p | (23) | a | i | k | (39) | u | o | o |
| (8) | k | s | c | (24) | a | s | s | (40) | u | i | n |
| (9) | o | u | s | (25) | d | f | a | (41) | l | i | k |
| (10) | e | e | v | (26) | p | o | a | (42) | a | d | n |
| (11) | r | i | o | (27) | r | i | j | (43) | g | o | h |
| (12) | x | g | e | (28) | a | g | e | (44) | b | a | g |
| (13) | g | u | u | (29) | v | a | f | (45) | o | v | j |
| (14) | e | u | u | (30) | n | u | s | (46) | a | | |
| (15) | u | h | s | (31) | r | t | r | | | | |
| (16) | s | d | u | (32) | r | c | c | | | | |

Our text is thus arranged in three columns, the first beginning *o z n*, the second *u e s*, and the third *s h o*. Col. 1 is presumed to have been ciphered by the first letter of the key-word, which remains to be discovered, and cols. 2 and 3 by the second and third letters of the same key-word.

The best way to find the key-word is to ascertain, if possible, which letter represents E in each cclumn, or, failing that, to establish at least one letter in each column. Now, although E is the most frequently occurring letter in English, it is followed so closely by T and A that allowance has to be made for one or other of these predominating in a short text. In looking for E, it should be borne in mind that this letter very commonly follows H, also that TH is a very frequent bigram and that THE is the commonest trigram.

Now it happens that the first three letters, *o u s*, are repeated in line 9. The word "the" is not an unlikely beginning, and the fact that *s* is one of the two letters

having the highest frequency in col. 3 favours the supposition that it stands for E. In lines 1, 9, and 30 the letter follows *u*, whence we may draw the legitimate inference, subject to correction, that *us*=HE and *ous*=THE.

Armed with these three letters, we will now consult Vigenère's table on p. 155, and endeavour to reconstruct the key-word. From the capital letter T in the top line of the table we descend the column which it heads till we reach *o*, and to the left of the line in which it occurs we find the capital letter V, which should be the first letter of the key-word. As will be seen, the top horizontal of capitals represents the letters of the plain text, the small letters in the body of the table are the ciphered letters, and the column of capitals to the left are intended to form the key-word. This relationship must always be borne in mind when ciphering or deciphering from Vigenère's table.

Proceeding in the same way with H and *u*, the second letters in the supposed plain text and the ciphered word respectively, we obtain N as the second letter of the key-word, and, continuing, from E and *s* we obtain O. According to this, then, our key-word is VNO.

We must next write out a portion of the text of the cryptogram, and, underneath, the key-word repeated continuously. By means of the table we proceed to the decipherment, with the following result:

```
o u s z e h n s o b o n l h h i c m a c p k s c
V N O V N O V N O V N O V N O V N O V N O V N O
t h e e r t s f a g b z q u t
```

Plainly, it is useless to go any farther; we have struck a false trail, and must patiently go over our ground anew.

We cannot resort to Porta's table for enlightenment, it being so constructed that the plain letter cannot be in the same half of the alphabet as its ciphered equivalent, and this condition is not met in *ous*=THE. There is another duplicated trigram in the cryptogram which might represent THE—*i.e.*, *ika*. This occurs in lines 23-24 and 41-42, *i* being in the middle column, *k* in the third, and *a* in the first column on the following line. This group, *ika*=THE, does not prejudice, nor is it prejudiced by, *ous*=THE, the difference being due to the fact that the letters did not fall to be ciphered under the same alphabet. There could, of course, be still another form for THE if three alphabets were used.

On putting *ika*=THE to the test by means of Vigenère's table, we produce the key-word PDW, but this merely proves another failure. There can be no doubt that three alphabets were used, and, as we are unable to get any assistance from a key-word, the obvious conclusion is that we are faced with a cryptogram ciphered by means of three *irregular* alphabets. This makes our task rather more complicated, and we shall have to discover the meaning of the letters one by one.

We make a beginning by assuming that *ous* in line 1 in the columnar table represents THE, and, in addition to marking this word in the margin, we mark T opposite every *o* in col. 1, H opposite every *u* in col. 2, and E opposite every *s* in col. 3. We must always proceed in this way, going through the columns, and marking the appropriate transcription throughout, every time we establish the value of a letter. By this means we obtain our clues and build up the solid fabric of the plain text.

In the present instance this marking, besides bringing

out the word THE repeated in line 9, shows H to occur in two consecutive lines, 13-14, followed in each case by the ciphered letter *u*. This cannot be meant for E, since we have already given this value to *s*; neither can it be T, which would produce the combination HT?HT. The choice is limited to A and I, either of which is far more likely than O. If we assume A, we have in view (T)HA(T) HA(S) or (W)HA(T) HA(S), but these are both ruled out by the fact that the supposed T is represented by *g*, whereas T has already been adopted as the value of *o* in the same column.

On the other hand, if we assume the letter following H to be I, we have the possible group (W)HI(C)H I(S), and as neither of the parenthetical letters usurps the position of T, we will boldly adopt this reading, which gives us the equivalents: *g*=W, *e*=C, *u*=S (all col. 1), *u*=I (col. 3).

We have already noted another trigram in the cryptogram which appears likely to represent THE—*i.e.*, *ika*. It occurs isolated in lines 41-42, but enables us to produce THE(R)E in lines 23-24 and TH(A)T IS in lines 37-39.

The word "of" would naturally be expected in a text the length of our cryptogram, perhaps more than once, and probably preceding "the." The group THE in lines 41-42 is preceded by *nl*, and as this bigram occurs twice in the text, we may not be far out in ascribing to it the value OF. It occurs isolated in lines 4-5, but in lines 37-42 it gives us the very substantial result: THAT IS (EA)ST OF THE. The parenthetical letters cannot be WE, because E (col. 3) has been established as the equivalent of *s*, whereas the ciphered letter here is *o*.

Let us pause here a moment to summarise our discoveries:

| *Col.* 1. | *Col.* 2. | *Col.* 3. |
|---|---|---|
| o=T, 3 letters | ~~s~~i=H, 6 letters | s=E, 5 letters |
| l=F, 2 ,, | =R, 4 ,, | o=A, 4 ,, |
| i=A, 4 ,, | o=E, 4 ,, | n=O, 4 ,, |
| a=E, 5 ,, | =T, 8 ,, | u=I, 5 ,, |
| e=C, 2 ,, | | k=H, 3 ,, |
| g=W, 2 ,, | | |
| u=S, 6 ,, | | |

Total: 67 letters out of 136, which indicates good progress. It is as well to summarise results in this way from time to time, as it shows how far the realm of hypothesis is being narrowed down by the extension of that of certainty.

To show how the summary will elucidate such a group as that in lines 25-28 (the capitals represent the plain text so far as discovered, and the small letters are ciphers still under investigation), apEarTjEge, it will be observed that the repeated ciphered letter *a* occurs in col. 3. Therefore, it cannot represent any of the letters E, A, O, I, or H, any more than *p*, the second letter in the group, and occurring in col. 1, can be intended for T, F, A, E, C, W, or S. The commonest bigram ending E is HE, and the commonest trigram THE, so that, as T has not yet come to light in col. 3, nor H in col. 1, we attach these values to *a* and *p* in the group, which now appears as THE TrTjEge. The only letter that fits the *r* sandwiched between two T's, and not yet accounted for, is I. This enables us to submit the group to the following transformation: THE TIT(L)E (OF), the parenthetical letters requiring confirmation.

The solution is now in sight. The letters remaining unknown are merely isolated rocks in an ocean of understanding. Thus the group extending from line 9 to

line 17 now appears as: THE CevITAx OF WHICH IS hEsdIy. The second word can be no other than CAPITAL, while as to the last, the name of a capital having six letters, of which the second is E and the fifth I, there need not be much hesitation in pronouncing it BERLIN.

The cryptogram holds no further terrors for us. BERLIN makes us think of (P)R(U)S(S)IA (lines 35-37), and eventually we have this table of all three alphabets:

| | | | | | | | | | | | | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| Plain text: | A | B | C | D | E | F | G | H | I | K | L | M | N | O | P | R | S | T | U | V | W | Y |
| Cipher Col. 1: | i | d | e | – | a | l | n | p | r | v | x | z | y | m | w | s | u | o | k | b | g | c |
| ,, ,, 2: | e | h | – | – | o | – | – | u | a | – | d | – | c | g | – | s | t | i | v | – | – | f |
| ,, ,, 3: | o | p | – | m | s | e | c | k | u | r | j | b | f | n | v | h | g | a | i | – | – | – |

The plain text proves to be as follows:

"The Margrave of Brandenburg, the capital of which is Berlin, has no right to assume thereby the title of king. He is king only in Prussia—that is, east of the Lower Vistula."

NOTE BY AUTHOR.—This statement by my correspondent, who is not a man to assert anything lightly as a rule, aroused my curiosity. Upon investigation, I find he is right, as is borne out by the admission of German jurists who are regarded as authorities in "Prussian" public law: Hermann Schulze, Ludwig von Roenne, and Ludwig Bornhak, who, with considerable reticence, acknowledge that the Margrave of Brandenburg is only, and has never been other than, "king *in* Prussia." The immense kingdom of Prussia, as we know it to-day, is only a fiction; its existence has no serious historical or juridical basis.

## SPILT INK.

This morning's post brought me a letter from a well-known professional man who has been utilising his spare time in constructing a safe cipher. He sends me a specimen, and warns me that he has submitted it to several amateurs, who failed to decipher it, the last re-

turning it intact with the remark that it was so much "spilt ink." "Perhaps you will have better luck," adds my correspondent, no doubt smiling up his sleeve as he wrote.

Let us glance at this cryptogram. If I do not succeed in deciphering it, I will frankly admit it without any false shame:

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

Total: 93 letters. I prepare a list of frequencies, and find that the most numerous letters in the text are *h*, *s*, and *z*, which each figure eight times. Can any of these represent E? Normally, there should be about a dozen E's in a text of this length.

The next letters in order of frequency are *g* (seven times), *f*, *n* (six times), and *d*, *x* (five times). These figures are too close for a simple alphabet cipher. Besides, what double letter could the initial *ss* stand for? If we assume a name beginning LL, they would have to be followed by O or E, and as *e*, the cipher equivalent, appears only three times in the whole of the cryptogram, it is useless to go any farther in this direction.

It would appear that more than one alphabet has been used, and that we may have to seek a key-word. The procedure to ascertain this has already been described in the chapter on "Ciphering by Means of a Key-Word."

It will be noted that there are several duplicated pairs of letters in the text, *zd*. for instance, occurring three times. Accordingly, we insert a stroke between the two

letters in each pair and count the intervals, making the following tabulation:

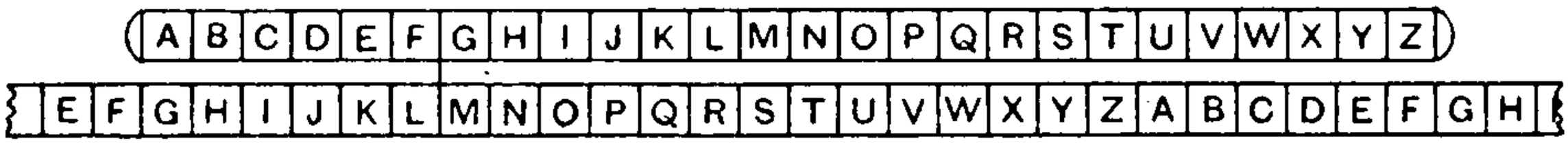
| | | | | |
|---|---|---|---|---|
| gz-gz | 3 | letters, | or | 3 |
| zd-zd | 8 | ,, | ,, | 2×2×2 |
| ,, | 39 | ,, | ,, | 3×13 |
| gg-gg | 20 | ,, | ,, | 2×2×5 |
| ys-ys | 5 | ,, | ,, | 5 |
| zn-zn | 37 | ,, | ,, | 37 |

Thus, there are two intervals having the factor 2, two with the factor 3, and two with 5. This absence of a predominant factor does not augur well for the key-word theory, and the experiment of dividing the text into three columns on the ground that, of the three equal factors, 3 is the most likely to indicate a key-word, if any, leads to no result.

The cryptogram contains several double letters—viz., *ss*, *gg* (twice), *nn*, *dd*, *hh*, and *yy*. A close scrutiny reveals the fact that the *gg* in one case is followed by *h* in alphabetic sequence, and in like manner *nn* is followed by *o*. This detail gives me a clue to the right track. The system of ciphering used appears to be that known as the "Saint Cyr Slides."

By means of the Saint Cyr slides we can obtain twenty-six different alphabets. Anyone can make these slides. All that is necessary is to obtain two rules or strips of plain wood, one long and one short. On the short rule mark equidistant divisions, and in them inscribe the twenty-six letters of the alphabet. Proceed in the same way with the long rule, but with the difference that two consecutive alphabets—*i.e.*, fifty-two letters, A-Z and A-Z—must be marked here, in order that, when the smaller rule is moved up or down in juxtaposition with the

longer, it will always be in contact with twenty-six letters on the latter, as shown:




When the short rule is moved so that its A is above Z on the long rule, the Z of the former will coincide with Y on the latter. The short rule represents the alphabet of the plain text, and the long rule the cipher alphabets.

In the above example A is represented by G, B by H, and so on. If we want to change the cipher, we have only to slide the small rule to the right or left, and a new ready-made secret alphabet is produced on the long rule underneath. In this way we have twenty-six different alphabets at our disposal.

It is even possible to make a change of alphabet with every letter ciphered, and that without risking a mental breakdown. Suppose, under this scheme, we wish to cipher the word "gun." The G on the short rule is seen to be over M on the lower rule, so we write M as our first letter. We now decide to use a new alphabet based on this M; for this purpose we merely slide the short rule to the right until its A is above M on the long rule. To cipher the second letter of our word, we look for U in the upper rule, and below, in the new alphabet, we find G. Having written this, we again change the alphabet by sliding the upper rule to the position where its A will be over G, and now find the ciphered equivalent of N, our last letter, to be T. Thus, the word "gun" becomes MGT by means of three different secret alphabets, one for each letter, obtained automatically in the way described.

Is this the method by which our cryptogram was

ciphered? If we knew the secret of the first letter, everything could be unfolded mechanically; but we do not, and this is the mystery of the "spilt ink."

However, there are ways and means. When the groups *ggh* and *nno* attracted my attention just now, I consulted a notebook in which I record rules which appear deducible from a long series of observations on ciphers, and found an entry entitled: "Cipher established by means of Saint Cyr slides, with automatic change of key at every letter." This is what I read:

A. When two like letters occur together, the second represents the plain letter A (*mm*=?A).

B. When two like letters are followed by the next letter in alphabetic sequence, the second and third letters in the trigram represent AB (*mmn*=?AB).

C. When an *a* occurs in the ciphered text, the letter which follows is identical with the corresponding plain-text letter (*ae*=?E).

I have noted some further rules on the subject, but these three will be ample for our purpose. Let us apply them to our cryptogram:

Rule A. In *ss* the second *s* equals A
„ *gg* „ „ *g* „ A
„ *nn* „ „ *n* „ A
„ *dd* „ „ *d* „ A
„ *hh* „ „ *h* „ A
„ *hh* „ „ *h* „ A
„ *yy* „ „ *y* „ A

Rule B. In *ggh* the last two letters equal AB
„ *nno* „ „ „ „ „ AB

Rule C. In *ay* the letter *y* equals Y

By these rules we would appear to have accounted for twelve letters (*gg* occurring twice). Using these as a

check, it now remains to decipher the remaining eighty-one letters.

We do not know the value of the first letter, S, but that does not matter; in the dozen letters presumed to have been established we have a plentiful choice of starting-points. With the Saint Cyr slides to our hand, we select for a beginning the first group containing two known letters—*i.e.*, *ggh*. From what has gone before, we infer that the ciphered letter *h* is the first letter of a new alphabet. The cipher being represented by the long rule and the plain text by the short one, we slide the latter until A thereon is above H in the lower rule. We now have to see which letter on the upper rule corresponds to the letter following *h* in the cryptogram, of which a section is reproduced for convenience:

g g h z n y s l p a y

The letter in question is *z*, which we find to correspond to S. Adding this to the two letters already known, we obtain three consecutive plain-text letters, ABS.

The letter *z* now becomes the ciphered equivalent of A in a new alphabet. Proceeding as before to adjust the rules, we identify *n* as the equivalent of O. Again changing the alphabet by giving the value of A to *n*, and continuing similarly with each letter, we decipher the above group as the word ABSOLUTELY.

The whole of the text is thus deciphered quite easily, with the exception of the first letter. The cryptogram begins with *ss*, and we know that the second *s* stands for A. Further, we know that this is by virtue of the fact that the value of the first *s* was altered to A, but we have no means of knowing what the original value of this initial *s* was. However, we have the context to guide us

where our formulæ are impotent, and effectively the series of letters from the second prove to be, AMCONVINCED, so that we may safely conclude that the mysterious first letter is I. The complete transcription is as follows:

"I am convinced that the present system is absolutely undecipherable. Accordingly, I am proud to have invented it."

With the view of softening the disappointment of my correspondent, to whom I have communicated the deciphered text, I am able to inform him in a covering note that this system offers safeguards by no means negligible, since, for example, the word "am" appears in two different disguises, *se* and *ht*; the "in" of the words "conv*in*ced," "accord*in*gly," and "*in*vented" is dissimulated under three separate forms: *kx*, *xk*, and *fs*; while "ent" in "pres*ent*" and "inv*ent*ed" is ciphered as *iwp* and *rex* respectively.

## An Undecipherable System.

In the spring of 1917 the post brought me a cryptogram to which was attached a visiting card with the words, in the handwriting of a friend: "You are fond of solving difficult problems. Here you are, then! I wish you joy." The cipher text, which contained fifty-two letters, was as follows:

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

I began by calculating the letter frequencies, and, to my stupefaction, found two *a*'s, two *b*'s, two *c*'s—in fact, two of each letter of the alphabet, neither more nor less. Only one group, *ds*, was repeated, and, that being the case, it was useless to seek a key-word.

There could be no question either of a grille or "dividers." In any case, these two letters of every kind were a strange coincidence, though instances almost as curious are encountered from time to time. I reflected on the possibility of a dictionary code. There are conventional codes composed of three-letter groups: *aab wkf*, etc.

By combining the letters of the alphabet in threes, a large number of groups can be obtained, sufficient to replace the words of a considerable-sized dictionary. Thus, the letter A, followed by one other letter, gives twenty-six different groups, and each of the other letters of the alphabet, followed by another letter, similarly yields twenty-six combinations. In this way, $26 \times 26 = 676$ different groups of two letters can be formed, and $676 \times 26 = 17{,}576$ groups of three letters.

I might have made some investigation in this direction but for two obstacles: (1) The fifty-two letters of the text were not divisible by three. One of them might be a blank letter, but which? (2) In whatever way the text was divided into three-letter groups, these were all different, and I needed at least one repeated group to serve as a base or starting-point.

I thought of a code composed of four-letter groups; 52 is divisible by 4, but the sectioning of the text into four-letter groups failed likewise to furnish any guide. Only two groups began with *b*—*bheg* and *bxja*. But all my efforts proved futile. I could not identify these groups approximately with such frequently occurring words as "and," "at," "be," "but," and others with initials in the early part of the alphabet.

Not being able to obtain the faintest clue as to the method of ciphering employed, I called on my friend,

informed him of my lack of success, and begged him to acquaint me with the key.

"Quite simple," he said. "This is how I wrote that cryptogram: I cut fifty-two slips of paper, on each of which I inscribed a letter of the alphabet. After using up twenty-six, I repeated the alphabet on the other twenty-six. I dropped the whole fifty-two slips into my hat, and, after shaking them up, took them out one by one haphazard, and noted them down just as they came to hand. The text thus formed I sent to you."

"Then it has no meaning!" I exclaimed.

"Of course," he replied, "and I must ask you to forgive my little trick; but you are so clever at cryptography that if I had submitted you a text with any meaning at all, you would probably have deciphered it far too quickly!"

## The Antique Dealer's.

A friend had asked me to meet him at the tramway terminus. I was there to time, with a minute to spare, and was first. While I walked to and fro, with an eye on the various approaches, the long hand of the clock tripped jauntily on its way, marking off the minutes in silence. At the end of a quarter of an hour I had decidedly lost all right to repeat the famous remark, "I almost had to wait," attributed gratuitously to Louis XIV., who appears to have said quite the opposite.[1]

How should I pass the time? There was no newsvendor. Besides, when one is in the habit of reading the news at certain regular hours, it is just the same as with meals—one has no appetite between.

[1] "Why scold him? Don't you think he is sorry enough to have kept me waiting?" (*Œuvres de J. Racine*, Hachette's edition, 1865, vol. v., p. 125).

But I descried an antique dealer's shop across the road, and as from that spot I should easily see my dilatory friend or be seen by him, I went over to examine the articles displayed. My eye quickly fell upon the prices inscribed on the labels, and, succumbing to the fascinations of my innocent hobby, I set myself the task of deciphering the values of the letters which took the place of Arabic numerals. Drawing out my notebook, I took note of a number of the articles exposed for sale in the four or five windows, as well as their mysterious prices —viz.:

| | | |
|---|---|---|
| 1. | Bronze statue (Psyche emerging from bath) | z.r.p |
| 2. | Incense burner - - - - | i.mp.p |
| 3. | Coloured engraving (national costumes) - | m.mp.p |
| 4. | Large double mirror, old frame, gilt much rubbed - - - - - | mi.mp.p |
| 5. | Inlaid card table - - | e.p.p |
| 6. | Iron dagger - - - - | mp.p |
| 7. | Small picture (glacier), white wood frame - | mr.p |
| 8. | Small engraving (Marie Antoinette), black frame - - - - - | mi.z |
| 9. | Small picture (The Flirt), worn gilt frame - | mi.z |
| 10. | Black and gold metal tray, flowers in centre | mf.z |
| 11. | Old barometer - - - - | m.r.p |
| 12. | Old picture (rustic scene) - | f.z |
| 13. | Four old engravings: the four - - | m.mf.z |
| 14. | Grandfather clock - - - - | mr.p.p |
| 15. | Card table, with inlaid draughtboard - | b.r.p |
| 16. | Glass cheese dish - - - - | f.z |
| 17. | Small Flemish painting. copy (? of a copy) | i.mp.p |
| 18. | Large trunk, much patched - - | z.r.p |
| 19. | Devotional picture, cloisonné worked on wood - - - - - | mf.z |
| 20. | Head of lion in bronze (door-knocker) - | mi.z |
| 21. | Concave shield, bas-reliefs, in gilt frame - | z.r.p |
| 22. | Large oval metal tray, Watteau subject in centre - - - - | mf.z |

23. Small mirror, large black wooden frame - b.p.p
24. Mirror, brown carved frame - - m.mr.p
25. Tin candlestick - - r.p
26. Oval silver tray, tarnished - m.mp.p
27. Bronze bowl on three feet - z.p
28. Large bronze hand lamp - - - i.mp.p
29. Small china vase, coloured and gilt - - m.mp.p
30. Engraving (the Signing of Magna Charta) - r.p
31. Engraving (Friends till Death) - mp.p
32. "Library of Famous Men," volume with 49 plates - - - - m.p.p
33. Silver bell - - - - m.i.z
34. Small silk mat, silver fringes - o.p
35. Silver strainer - - z.p
36. Old decanter; silver stand - - m.i.z
37. Locket, with cat's-eye and amethysts - mf.z
38. Chased silver egg-cup - - mf.z
39. Copper seal - - m.m.p
40. Old silver chafing dish - - o.mp.p
41. Old decanter - - mi.z
42. Liqueur stand, with two flagons - - b.b.p
43. Old beer mug, coloured stoneware - mp.p
44. Bronze medal set in ring of chased silver - o.p

The first thing I noticed was. the large number of *p*'s, reaching a third of all the letters I had noted. It occurs among the pence and shillings, but never among the pounds.

We all know the rôle played by zero in arithmetic when high numbers come into play. Zero, the value of which is defined as nil, then assumes an extreme importance, provided it appears on the right side—that is, to the right. This is the figure that best gives the notion of infinity, if repeated to a sufficient extent. If I were a mathematician and were commissioned by the Board of Research, I would willingly write a book on *The Value of Naught*.

From the above it follows that, our letter *p* never occurring to the left of any of the prices, but being often repeated to the right, we may boldly conclude *p*=O.

Next we observe that the only other letter in the pence column besides *p* is *z*, these two sharing the column in the proportion of two-thirds and one-third respectively. The conclusion is fairly obvious that *z* stands for 6.

Of the bigrams occurring in the shilling column, the first letter is always *m*, and since numbers in this column do not go beyond the teens, *m* can mean no other than 1.

Parenthetically it may be noted that there are only nine different letters in the price list, so that one figure out of the ten is unrepresented. This is most likely to be 9, a figure that is rarely seen in prices of antiques. Nine or 19 shillings or pounds is very unusual. Prices hovering in the region of the 9's are wandering asteroids which usually succumb to the minor attraction of the smaller planets 8 or 7, or the increasing attraction of the larger planet 10.

We have presumptively disposed of the four figures 0, 1, 6, and 9, and almost certainly know that the price of the coloured engraving (3), tarnished tray (26), and china vase (29) is £1 10s. each; of the "Library of Famous Men" (32), £1; of the copper seal (39), £1 1s.; of the dagger (6), engraving (31), and beer mug (43), 10s. each; and of the bronze bowl (27) and silver strainer (35), 6s. each.

The incense burner (2), small Flemish painting (17), and bronze hand lamp (28) are all the same price—that is, 10s., plus a number of pounds indicated by *i*. The double mirror (4) is the same price, augmented by £10—*i.e.*, mi.mp.p. Further, the engraving (8), picture (9), door-knocker (20), and decanter (41) are each priced at mi.z. These articles seem to me quite dear enough

at 12s. 6d., so that there is no need to ascribe a greater value than 2 to *i*.

This brings the price of the incense burner, etc., to £2 10s., and that of the double mirror to £12 10s. There are also two items—silver bell (33) and decanter with silver stand (36)—priced at £1 2s. 6d.

The letter *i* shares with *r* the third place in order of frequency among these prices. The bronze Psyche (1), trunk (18), and shield (21) are each priced at £6 plus *r* shillings; the picture of a glacier (7) is 10 plus *r* shillings; the barometer (11), £1 plus *r* shillings; grandfather clock (14), 10 plus *r* pounds; brown-framed mirror (24), 30 plus *r* shillings; and the candlestick (25) and engraving "Magna Charta" (30), each *r* shillings. So ubiquitous a letter can scarcely be intended for anything but 5. Certainly the two last-named objects would not fetch more than 5s. each, while such quotations for the other articles as 15s., £1 5s., £1 15s., £6 5s., and £10 5s. are commonly seen. We therefore attach the value of 5 to *r*.

Our attention is now attracted to the letter *b*. There is a mirror (23) at *b* pounds, a liqueur stand (42) at *b* guineas, and a card table (15) at *b* pounds 5 shillings. The first named is a very woebegone-looking object, and must be regarded as dear at £3. The card table is more presentable at £3 5s., but however good value this may be, the liqueur stand at *b* guineas is an obstacle to the placing of *b* at any higher value than 3. Accordingly we appraise *b* at 3.

Summarising, we have established six out of the nine digits. Those remaining to be discovered are 4, 7, and 8.

The letter *f* occurs among the shillings, and is always accompanied by *z* (=6) pence. This latter factor induces

us to ascribe the value of 7, rather than 4 or 8, to *f*. On this assumption, prices are as follows: Black and gold tray (10), devotional picture (19), Watteau tray (22), locket (37), and chased silver egg-cup (38), 17s. 6d. each; rustic scene (12), cheese dish (16), 7s. 6d. each; four engravings, the four (13), £1 17s. 6d.

The letter *o* occurs three times. The silk mat (34) is marked o.p. It was originally marked b.z., or 3s. 6d., which price has been crossed out. The value is scarcely likely to have jumped suddenly to 8s., so that the only alternative is 4s. Assuming, therefore, that *o* equals 4, the price of the bronze medal (44) is also 4s., and that of the chafing dish (40) £4 10s.

The prices of all the items have thus been established, with the exception of the inlaid card table (5). This is marked *e* pounds, which must mean either £8 or £9. The letter *e* occurs nowhere else, so we have no means of drawing any reliable inference. Compared with the other card table, which appeared fairly good value at £3 5s., the present article is relatively not cheap at £8.

While I was debating within myself whether to invite confirmation from the dealer, who had come to the door and was regarding me with an inquisitive air, a commotion took place behind me, and my friend, a good hour and a quarter late, greeted me in breathless tones:

"So sorry, old fellow; but, you know——"

"Yes, yes; I know," I interrupted. "If you had kept me waiting ten minutes, I should have been annoyed; but people who are more than an hour late are assumed to have been victims of an accident, and they are always excused in advance. But don't worry. I have not wasted my time."

# PART III

## LISTS AND TABLES

NOTE.—This third part consists of a series of calculations of letter frequencies and combinations in English and certain foreign languages.

Of the practical value of these lists, compiled as a result of numerous experiments, there can be no doubt, but the fact must not be lost sight of that they constitute *only one of the factors* which the decipherer must take into account if he would push his investigations to a successful issue. Cryptograms are often encountered in which the normal frequency of letters has been deliberately upset.

The *second factor* is untiring effort, supported by persevering study.

The *third factor* is *flair*, or insight. This need not be regarded as purely instinctive or in the nature of a lucky gift. A reasoned and discerning ingenuity plays a large part here, as well as the exercise of that gumption or common sense which enabled Christopher Columbus to stand an egg in a position contrary to the laws of physics.

### ENGLISH.—I.

*Order of Letter Frequency.*

According to Edgar Allan Poe: E A O I D H N R S T U Y, etc.

According to Vesin de Romanini: E T A O N I R S H D L C W U M, etc.

Normal frequency table (Hitt): E T O A N I R S H D L
U C M P F Y W G B V K J X Z Q.
Telegraphic frequency (Hitt): E O A N I R S T D L H U
C M P Y F G W B V K X J Q Z.

### *Order of Frequency of Final Letters.*

According to Valerio: E S D N T R Y O F A, etc. (See also English.—III.)

### *The Commonest Bigrams (Valerio).*

TH, HE, AN, ER, ON, RE, IN, ED, ND, AT, OF, OR, HA, EN, NT, EA, etc.

### *Frequency of Double Letters.*

EE, OO, FF, LL, SS, etc.
According to Valerio: SS, EE, TT, LL, MM, OO, FF, etc.

### *The Most Frequent Two-Letter Words (in Order).*

OF, TO, IN, IT, IS, BE, HE, BY, OR, AS, AT, AN, SO, etc.

## ENGLISH.—II.

### *The Commonest Trigrams (Valerio).*

THE, AND, THA, HAT, EDT (triED To, carriED The), ENT, FOR, ION, TIO, NDE, HAS, MEN, NCE, OFT, STH.

### *The Commonest Three-Letter Words.*

THE, AND, then FOR, ARE, BUT, ALL, NOT, etc.

### *The Commonest Four-Letter Words.*

THAT, WITH, FROM, HAVE, THIS, THEY, etc.

*Words of One Letter.*

A, I, O.

Proportion of E (Valerio): 13 per cent.

Proportion of vowels (Valerio): 40 per cent.

## ENGLISH.—III.

(Compiled by Translator.)[1]

*Order of Letter Frequency in Relation to Position of Letter in Word.*

Initial letters: T A O M H W C I P B E S, etc.

Second letters: H O E I A U N R T, etc.

Third letters: E S A R N I, etc.

Antepenultimate letters: I T E A H N O, etc.

Penultimate letters: E N A R H I L C O, etc.

Final letters: E T S D N R Y G, etc. (See also English.—I.)

*Consonant Bigrams at the Ends of Words (Order of Frequency).*

NG, ND, NT, DS, KS, ST, TS, TH, HT, RT, SS, CT, LL, LT, GH, SH, CH, DD, LD, LS, NS, RN, RS, WN, FF, LP, MS, RD, RL.

## ENGLISH.—IV.

*Final Bigrams.*

An English text of 1,000 letters contains, *on an average* (excluding two-letter words):

11 words ending HE.

10 words ending ED.

[1] This and the following sections up to page 138 have been compiled specially for the English Edition.

8 words each ending ER, NG.
7 words each ending OR, RE.
6 words each ending AT, ND.
5 words ending NT.
4 words ending LY.
3 words each ending AN, DS, EN, ES, LE, ON, RY, SE, TY.
2 words each ending AD, AS, CE, HT, ID, IS, KE, KS, ME, NE, OT, OW, RT, SS, ST, TS, TH, VE.
1 word each ending AL, AP, AR, AY, CH, CT, DE, EE, EM, ET, EW, EY, GE, GH, HY, IG, IL, IN, IR, LD, LL, LS, LT, NS, NY, OM, OU, RN, RS, SH, TE, UE, UL, UR, US, UT, WN, WO, YS.

### *Final Trigrams.*

An English text of 1,000 letters contains, *on an average* (excluding three-letter words):

5 words ending ING.
3 words each ending ENT, HAT.
2 words each ending AVE, ERE, GHT, ION, IED. NDS, PLE, RTY, VER.
1 word each ending ACT, AID, AND, ANT, ART, ATS, EEN, END, ERY, ESS, EST, HED, HEN, HER, HIS, ICE, IES, ISE, ISH, ITH, LLY, LOR, NCE, NED, NTS, OKS, ORE, RED, TED, TER, UND.

### *Initial Consonant Bigrams (Order of Frequency).*

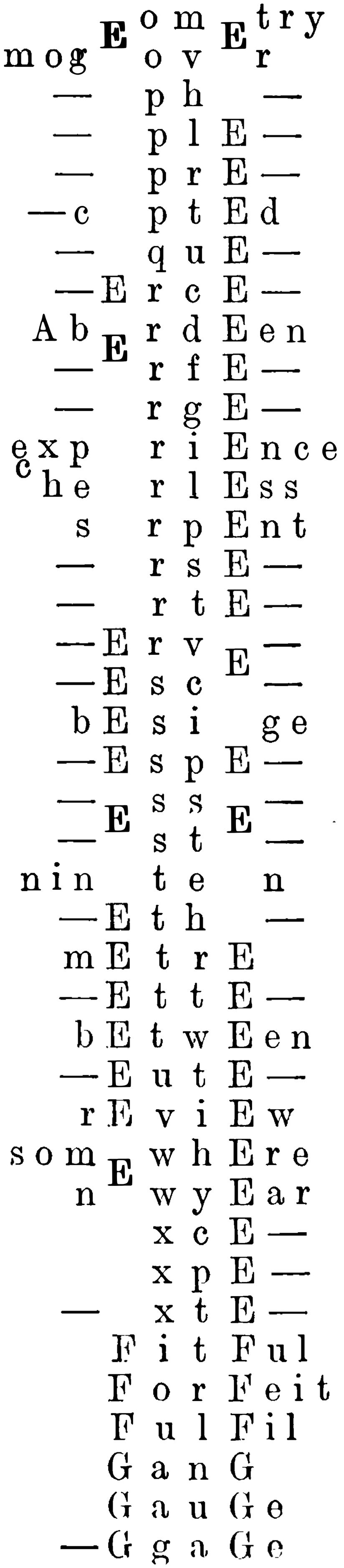
TH, PR, WH, CH, FR, SH, TR, CL, SP, CR, PH, PL, BR, GL, SC, SM, ST, WR.

## ENGLISH.—V.

*Like Letters at Equal Intervals (separated by two Letters).*

A b b A c y
A r A b i A
A b l A t i v e
A b o A r d
—A c i A—
p A c k A g e
s A c r A m e n t
e v A c u A t e
r A d i A—
h e A d l A n d
q u A d r A n g l e
g r A d u A l
A d v A—
h e A d w A y
A f f A i
A f r A i d
p A g e A n t
—A g g A—
m A g n A—
—A g r A—
A h e A d
a v A i l A b l e
c l A i m A n t
—A i n A—
c o m p l A i s A n t
b r e A k f A s t
—A l i A—
—A l l A—
s i g n A l m A n
p A l p A b l e
—A l t A—
v A l u A—
—A l v A—
A l w A y s
A m b A s s a d o r
A m i A b l e
—A m m A—
d A m n A b l e
A m p A i g n
t A m w A y
—A n d A—
—t e r A n e A n
m A n i A
—A n s A c t
A n t A g o n i s t
J A n u A r y
c A n v A s
c h A p l A i n
A p p A—
—A p t A—
A q u A—
—A r c A—
w h A r f' A g e'
—A r g A—
—A r i A—
r e m A r k A b l e
A r m A e n
c A r n A t i o n
—A r r A—
p A r t A k e
s t A r v A t i o n
—A s c A—
A s h A m e d
A s i A
—A s t A—
d e v A s A t e
c A s A l
'A t A s

—AttA—
—AudA—
restAurAnt
cAveAt
—AviA—
drAwbAck
tAxpAyer
lAymAn
BarB—
BomB
BriBe
suBurB
coBweB
CalCulate
—CarC—
CatCh
—CenCy
CheCk
CirC—
CloCk
sCorCh
SCotCh
—CraC—
seCreCy
CriCket
CroC—
CruC—
speCtaCle
—CtiC
stanDarD
DeaD
DeeD
DiaDem
DieD
hunDreD
reDunDant
dEadEn
EagEr
spEakEr
—EalE—
—EanE—
chEapEr
—EarE—
asE
atE—
avE—
—EbbE
—EcreE—
—Ect
—EctEd
rdeEm
EdgE
expEdiEnt
neEdlE
WEdnEsday
rEdrEss
dEepEn
EffEct
dEfiEd
—EflEct
nEglEct
sEgmEnt
—EgrE—
—cEivE
—EliE—
—EllE—
ElsE
—EltE—
—ElvE—
—EmbEr
—EmpE—
thEmsElves
—EncE
—EndE—
—ngE—
convEniEnt
—EnnE—
—EnsE—
—ntE—
nvElop


EomEtry
mogEovEr
—phE—
—plE—
—prE—
—cptEd
—quE—
—ErcE—
AbrdEen
—rfE—
—rgE—
expriEnce
chrlEss
sprEnt
—rsE—
—rtE—
—ErvE—
—EscE—
bEsige
—EspE—
—EssE—
—EstE—
ninteen
—EthE—
mEtrE
—EttE—
bEtwEen
—EutE—
rEviEw
somEwhEre
nEwyEar
xcE—
xpE—
—xtE—
FitFul
ForFeit
FulFil
GanG
GauGe
—GgaGe
—GinG—
neGligent
GonG
GorGe
—GreGate
langGuaGe
sHepHerd
wHicH
HigH
rHythm
—cIalIst
—IatIon
—IctI—
midnIght
besIegIng
IffIcult
IftIeth
—IgnI—
—IldI—
—IllI—
—ImmI—
—ImpI—
—IncI—
—IndI—
—InnIng
—InsI—
—IntI—
—InvI—
—IodI—
curIosIty
—IplI—
—IppIng
—scrIptI—
—IquI—
skIrmIsh
—IrrI—
—IscI—
satIsfIed
—IshIng
dIslIke

dIsmIss
—IssI—
—IstI—
BrItaIn
KhaKi
KicK
booKmaKer
singuLarLy
caLcuLate
ceLluLar
MadMan
MaiM
coMmeMorate
MneMonic
MumMy
iNcaNdescent
—NceN—
—NciN—
—NcoN—
—NdaN—
—NdeN—
—NdiNg
—NdoN
iNfa t
—NgeN—
eNgi e
—NioN
—NjuNction
—Nki g
—Nla d
—Nme t
caNnoN
aNoiNt
NooN
NouN
reNowN
—NseN—
—NtaN—
—NteN—
—NtiN—

coNveNe
—NviNce
OblOng
ObsOlete
MorOccO
atrOciOus
—OctO—
OdiOus
lOgwOod
pOisOn
fOliO
—OllOw
cOmfOrt
—OmmO—
cOmpO—
—OndO—
erroneOus
cOnfO—
—OniO—
cOnvO—
—OphO—
tOpmOst
—OppO—
fOrbOre
fOrgOt
—OriOus
fOrlOrn
enOrmOus
—OrpO—
—OrrO—
fOrsOok
—OscO—
explOsiOn
blOssOm
—pstO—
—tiOn
—ttO—
budOir
nxiOus
bxwOod

bOyhOod
PalPable
PamPer
PauPer
PeoPle
PerP—
PorPoise
PreP—
ProP—
PulP
PumP
PurP—
fRatRicid
extRaoRdinaœy
—RdeR
ReaR
caReeR
RepR—
waRfaR
peRfoRm
laRgeR
—RieR
pRimRose
—RioR
—RkeR
—RmeR
coRneR
RoaR
—RogR—
—RpaRt
—RpeR
puRpoRt
—RroR
hoRseRace
cuRsoRy
—RteR—
depaRtuRe
FebRuaRy
foRwaRd
aSbeStos
diScuSs
SeaSon
SenS—
asSetS
diSguSt
—SheS
enthuSiaS—
SmaSh
—SmiSs—
—SneSs
conSolS
treSpaSs
deSpiSe
diSpoSe
pSseSs
SsiSt
ch StiSe
SubS—
TacT
TanT
sTarT
TasTe
TauT
—TecT
— enT
èsT
exT
ouTfiT
ThaT
paThetic
wiThsTand
—TiaTe
—TieTh
TilT
TinT
—TisT
ouTleT
disTorT
ToutT
ouTputT

—T r a T e
—T r e T —
—T r i  i o n
b e T r o T h
  T r u  h
o u T s e
 a T t i  u d e
 s i T u a  i o n
  T u f T
g r a T u i T —
  s U b d U
  s U c c U m b
—U c  U —
 s U f  U e
—U l o  s
—U l t  —
 h U m b  g
—U m o U r
  U n h U r t
  U n l U c k y
  U n s U i t a b l e
 r U p t U r e
 t U r b U l e n t
 p U r s U e
 m U s c U l a r
M U s e U m
b r U s q U e
 g U t t U r a l
  V a l V e
  V e l V e t
—V o l V e
  W a y W a r d
  Z i g Z a g

## ENGLISH.—VI.

*Like Letters at Equal Intervals (separated by Three Letters).*

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

lAnguAge
gAngwAy
mechAnicAl
AnimA—
orgAnisAtion
AnnuAl
AnomAly
mAnslAughter
trAnspArent
substAntiAl
mAnufActure
dilApidAted
cApitA—
AppeA—
ApplAud
chArcoAl
chArgeAble
chAritAble
pArliAment
AromA
ArreArs
—ArriAge
—ArtiAl
reAsonAble
AsphAlt
AssuAge
AstrA—
lAterAl
—AticA
coAtofArms
—AturA—
AverAge
nAvigAte
AvocAtion
AvowAl
AwkwArd
aBsorB
volCaniC
ChanCe
CharCoal

teChniCl
ChurCh
—CienC—
—CifiC
neCklaCe
ClinCh
ClutCh
CoalCellar
ComiCal
ConsC—
CounCil
CrutCh
eleCtriC
CubiC
—CuraCy
DeciDe
DeluDe
DesiDeration
DiviDe
WeDnesDay
DreaD
DwinDle
—EablE
—EachE—
EaglE
mEagrE
lEagu
clEans
fEarl ss
—EarnE
rehEarsE
EastEr
—EathE—
—EbatE
dEcidE
spEcimEn
prEcisE
corrEctnEss
sEcurE
—EcutE

mEdiaEval
—EducE
schEdulE
dEfacE
—EforE
—lEgatE
bEhavE
dEifiEd
forEignEr
EitherE
—ElatE
dElinEate
dElivEr
envElopE
bElovEd
EludE
EmblEm
EminEnt
—EmisE—
rEmunErat—
parEnthEsis
sevEntiEth
gEntlE
cEntrE
EnumErat—
pEoplE
rEpliEd
—EposE
scEptrE
—EputE
—EragE
ErasE
—EratE
ovErduE
expErimEnt
dErivE
nevErthEless
intErviEw
wholEsalE
rEscuE

rEsidE
dEsirE
—EsomE
—EsquE
invEstmEnt
rEsumE
—EtchE—
rEticEnt
lifEtimE
bEtokEn
EvanEscent
—EvicE
EvidEnt
—EvisE
rEvivE
EvokE
benEvolEnt
dEvotE
bEwarE
ExchEquer
ExprEss
ExtrEme
FearFul
GoinG
GrudGe
HarsH
HatcH
arcHbisHop
HeatH
HeigHt
HitcH
tHougH
—IentI—
—IghtIng
compIlatIon
pIlgrIm
vIllaIn
ImplIcit
ImprI—
InquI—

InspIre
InstInct
IntuItion
dimInutIon
InvoIce
cIrcuIt
mIschIef
dIscrI—
bIscuIt
dIstrI—
capItalIst
—ItatIon
stocKbroKer
KnacK
KnocK
KnucKle
LabeL
LandL—
cLearLy
LegaL
siLentLy
compLeteLy
LibeL
symboLicaL
LikeLy
LiveLy
LocaL
LoveLy
LoyaL
LuckLess
absoLuteLy
MadaM
comMandMent
MaxiMum
aMazeMent
aMendMent
soMetiMes
MiniMum
MonuMent
MoveMent
—MpleMent
coMpliMent
syMptoM
aMuseMent
—rNameNt
coNcerN
eNchaNt
aNcieNt
—NdemN
coNdigN
—NdmeNt
—NemeNt
coNfroNt
ENglaNd
saNguiNe
cogNisaNce
pheNomeNon
NomiN—
kNowiNg
deliNquet
—Nshie
—NsigN
—Nsie N
—NstaNt
—NtaiN
iNterN
—NtioN
ObviOus
—cOctiOn
—rgatry
tilsme
whlesme
slilquy
smebdy
sOmehOw
cOmprOmise
cOnglOmeration
cOntrO—
anOnymOus
OptiOn

fOregO
hOrizOn
pOrtfOlio
OrthOdox
—OrtiOn
tOrtuOus
pOstpOne
—OtatO—
thrOughOut
neighbOurhOod
OutdO
OutgOing
ParaPet
PersP—
PhosPhate
PlumP
PostPone
PromPt
ProsPer
QuinQuennial
—RatoR—
tRaveRse
suRchaRge
aRdouR
RecoRd
ReveRse
buRglaR
bRibeRy
auRifeRous
wRiteR
coRkscRew
aRmouR
bRokeR
pRopeR
fuRtheR
ARthuR
paRtneR
moRtuaRy
diSburSe
diScloSe
—SeleSs
—SeneSs
diSguiSe
beSideS
buSineSs
suSpenSe
diSperSe
reSponS—
—SticS
ChriStmaS
StreSs
abStruSe
TainT
—TeenTh
TempT
—TeraT—
TheaTre
hefT
auhenTic
hiherTo
hirTy
ahleTic
ihouT
awmehysT
—iciTy
—ienT
—TigaTe
TighT
esTimaTe
—TincT
culTivaTe
—pTiviTy
—TmenT
uTmosT
ToasT
—TracT
—TraiT
conTrasT
TreaT
sTreeT

sTricT
pTrioT
—TrucT
TrusT
congraTulaTe
—rTunaTe
TwenTy
trusTworThy
qUadrU—
chaUffeUr
rUinoUs
frUitfUl
sUlphUr
scUlpture

sUmptUous
pUnct —
Undo bted
conUndr m
UniqUe
—UrioUs
UsefUl
—UthfUl
beaUtifUl
caUtioUs
—VatiVe
VotiVe
WestWard
WindWard

## ENGLISH.—VII.

*Three Like Letters with Intervals of One.*

pAlAtAble
MAlAyA
CAnAdA
cArAvAn
cAtArAct
extrAvAgAnt
—EcEdEnt
piEcEmEal
prEdEcEssor
rEfErEnce
—EgEnErate
vEhEmEnt
ElEmEnt
ElEvEn
cEmEtEry
whEnEvEr
whErEvEr

—EvErE
—IbIlIty
—hIbItIon
rIgIdIty
dImInIsh
InItIa—
—IsItI—
crItIcIsm
cIvIlIan
dIvIsIon
lOcOmOtive
chrOnOlOgy
mOnOpOly
mOnOtOn—
chlOrOfOrm
—sTiTuT—
UnUsUal

## *Bigrams Repeated.*

C O C O a
—d E R E R
I C I C l e
—I N I N g
b A G g A G e
b A R b A R o u s
B A r B A r o u s
C A l C A r e o u s
C A s C A d e
C A u C A s —
D A r D A n e l l e s
p E A c E A b l e
—E N d E N t
—E N t E N
r e v E R b E R a t e
—E R g E R
p E R v E R s e
—I N g I N g
—I N k I N g
M A d M A n
M U r M U r
—N G i N G
—N T e N T
O N i O N
P A l P A b l e
P O r P O i s e
R E d R E s s
R E p R E s e n t
S E n S E
a S S a S S i n
—S S e S S

T H i T H e r
m U R m U R
o U T p U T
h A B i t A B l e
C H u r C H
p i C K p o C K e t
D E c i D E
D E l u D E
I N c l I N e
I N f r I N g e
I N s t I N c t
p e r I T o n I T i s
O R a t O R
P H o s P H a t e
P O s t P O n e
Q U i n Q U e n n i a l
r e m i S S n e S S
d i S T r u S T
f o r T H w i T H
s E N t i m E N t
M A t h e M A t i c s
s e N T i m e N T
c o N T i n e N T
c O U r t e O U s
p l E N i p o t E N t i a r y
i n t E R p r e t E R
ç o N T r a v e N T i o n
c O U r a g e O U s
i n T E r p r e T E r
u N D e r s t a N D
etc., etc.

*Words of Ten Different Letters, which may be used in Substitution of the Figures* 0–9 or 1–0, *and thereby form Numeral Key-Words.*

AUTHORISED
BACKGROUND
BANKRUPTCY
BUCKINGHAM
CHIVALROUS
COMPATIBLE
COMPLAINTS
DESOLATING
DESTROYING
EXHAUSTION
FLOURISHED
FORMIDABLE
GELATINOUS
HYDRAULICS
HYPNOTISED
HYSTERICAL
ILFRACOMBE
IMPERSONAL
IMPORTANCE
JOURNALIST
LACHRYMOSE
MACKINTOSH
MENDACIOUS
METAPHYSIC
MINERALOGY
MISFORTUNE
MODERATING
PATRONISED
PATRONYMIC
PLAYWRIGHT
PRESUMABLY
PREVIOUSLY
PROCLAIMED
PROFLIGATE
PROMULGATE
PURCHASING
REGULATION
REPUBLICAN
SUBJECTION
SYMPATHISE
UNSOCIABLE
WORKINGDAY

Surnames such as *Tichbourne*, or short sentences such as *Fair Custom*, may also be used.

## ENGLISH.—VIII.

*Proportion of Words in Webster's Dictionary classified according to their Initials.*

| | *Per Cent.* | *Total.* | | *Per Cent.* | *Total.* |
|---|---|---|---|---|---|
| A .. | 6·43 | 6·43 | N .. | 1·61 | 58·71 |
| B .. | 5·35 | 11·78 | O .. | 2·38 | 61·09 |
| C .. | 9·82 | 21·60 | P .. | 8·51 | 69·60 |
| D .. | 5·95 | 27·55 | Q .. | 0·59 | 70·19 |
| E .. | 4·22 | 31·77 | R .. | 4·94 | 75·13 |
| F .. | 4·22 | 35·99 | S .. | 12·02 | 87·15 |
| G .. | 3·27 | 39·26 | T .. | 5·83 | 92·98 |
| H .. | 3·69 | 42·95 | U .. | 1·55 | 94·53 |
| I .. | 4·22 | 47·17 | V .. | 1·84 | 96·37 |
| J .. | 0·83 | 48·00 | W .. | 2·92 | 99·29 |
| K .. | 0·77 | 48·77 | X .. | 0·12 | 99·41 |
| L .. | 3·39 | 52·16 | Y .. | 0·30 | 99·71 |
| M .. | 4·94 | 57·10 | Z .. | 0·30 | 100·01 |

The extra 0·01 per cent. in the total is due to the approximate nature of the calculations. The above proportions vary from one dictionary to another.

## FRENCH.—I.

### *Order of Letter Frequency.*

According to Valerio: E N A I R S T U O L D C M P V F, etc.
According to Langie (in the works of Bossuet, Voltaire, Maupassant, and France): E S A T I N, etc.
According to Kasiski: E S R I A N T O U *L*, etc.

### *Order of Frequency of Final Letters* (*Valerio*).

E S T R A N L I U D, etc.

### *The Commonest Bigrams* (*Valerio*).

ES, EN, LE, DE, ON, OU, NT, RE, NE, ED, TE, EM,
SE, ER, AR, ME, AN, IT, ET, IE, TI, EL, NS, UR.

### *Frequency of Double Letters.*

According to Valerio: SS, LL, EE, NN, TT, FF, CC, RR, MM, PP.
According to Kasiski: SS, EE, NN, TT, FF, CC, RR.

### *Double Letters at the End of Words.*

ÉE.

## FRENCH.—II.

### *The Commonest Trigrams.*

According to Valerio: ENT, EDE, LES, LLE, QUE, AIT, EME, ION, EUR, ELL, SSE, EST, DAN, DEL, MEN, DES, TIO, ESE, ANS.
According to Kasiski: ENT, QUE, ION, QUI, TIO, ONT, AIT, ANT, OUR, ANS, LES, AIS, OUS.

### *The Commonest Two-Letter Words.*

AN, AU, CE, CI, DE, DU, EN, ET, IL, JE, LA, LE, MA, ME, NE, NI, NU, ON, OU, SA, SE, SI, TA, TE, TU, UN.

### *Words of One Letter.*

A, O, Y.

### *Four-Letter Groups repeated in Succession.*

NOUS NOUS, VOUS VOUS.

Proportion of E (Valerio): 17 per cent.
Proportion of vowels (Valerio): 44·5 per cent.

## FRENCH.—III.

### *Order of Letter Frequency in Relation to Position of Letter in Word.*

Initial letters (Valerio): D L E P A C S M R I F, etc.
Second letters (Langie): E O A U N R I T, etc.
Third letters (Langie): S E U N T I R, etc. (order indifferent).
Antepenultimate letters (Langie): E, followed by A, I O L (no order), etc.
Penultimate letters (Langie): E U N I L O R S, etc.
Final letters (Valerio): E S T R A N L I U D C X, etc.

### *Initial Consonant Bigrams (Valerio).*

BL, BR, PL, PR, FL, FR, VR, CL, CR, GL, GR, TR,
DR, CH, PH, TH, SC, SP, ST.

### *Final Consonant Bigrams (Valerio).*

NT, NS, RT, NC, CT, RC, SC, ND, RD, NG, RG,
MP, NQ, ST, GT (doigt, vingt), SS (express).

## FRENCH.—IV.

### *Final Bigrams (Langie).*

A French text of 1,000 letters contains, *on an average:*

25 words ending ES.
23 words ending NT.
10 words ending RE.
9 words each ending NE, ON.
7 words each ending UN, LA.
6 words each ending ME, SE, UR, UI, LE, NS, ER.
5 words each ending TE, UE, DE.
4 words each ending IE, EC, ET, EN, OU, UX.

### *Final Trigrams (Langie).*

A French text of 1,000 letters contains, *on an average:*

9 words each ending LES, ENT.
7 words ending ONT.
6 words ending RES.
5 words each ending GES, INE.
4 words ending TRE.

## FRENCH.—V.

*Five-Letter Group repeated in Succession.*

FAIRE FAIRE.

*Repeated Groups separated by a Single Letter.*

VIS À VIS, PEU À PEU, PETIT À PETIT, DOS À DOS.

*Consecutive Words ending with Like Letters.*

LES BELLES ACTIONS.

*Three-Letter Words ending with E.*

UNE, QUE, etc.

*Final S preceded by Three Like Letters.*

CRÉÉES.

Q is always followed by U in the body of a word.
X is preceded by U, except in the words six, dix, fixe, prolixe, mixture, etc., axe, sexe, boxe, etc.
H is preceded by
C, as in chemin, cheval, cher, etc.
P, as in photographie, etc.
T, as in théâtre, etc.

*Word of Twelve Different Letters, which may be used in Substitution of the Figures* 1–12, *and thereby form a Numerical Key-Word.*

IMPRÉVOYANTS.[1]

[1] In English "considerably" might be used.—TRANSLATOR.

## FRENCH.—VI.

*Like Letters at Equal Intervals (separated by Two Letters).*

A f f Aire
c A l c Aire
c A m p A g n e
f s r A n ç A i s
c A n d A l e
é r A n l A
— A p p A —
b A r b A r e
— A r r A —
p A r t A g e
— A s s A —
A t l A s
— A t t A —
B a r B a r e
B o m B e
C a l C a i r e
C i r C —
— C o n C —
— C r o C —
s p e C t a C l e
D a r D —
D i n D e
p E c h E r
s i E c l E
s E c r E t
r E c u E i l l i r
E f f E t
r E f l E c h i r
r E g i E
s E g m E n t
a l ! E g r E s s e
c h a n c E l i E r
— E l l E

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

—EuvE—
rEvuE
ExpE ition
ForFdit
GonG
HacHe
vIctIme
dIffIcile
sIgnIfier
aIguIlle
recueIllIr
mIllIon
ImmI—
aInsI
—crIptIon
mIssIon
apItaIne
milItaIre
—LluL—
iNfaNterie
uNioN
aNnoNcer
—NseN—
—NtaN—
—NtiN—
—NtoN—
pOisOn
fOliO
c mm tion
— nt —
p p se
— r d —
h r l ge
— r t —

explOsiOn
—OtiO—
tOujurs
cOurnne
PeuPle
PréP—
ProP—
extrRaoRdinaire
RepRsentant
empeReuR
—RieR
cRoiRe
—RruR—
moRsuRe
foRteResse
—RtiR
—SaiS—
SanS
SenS
SouS
aSsiSter
deSsuS
SuiS
—TanT—
—TenT—
TorT
—TouT
aTtiTude
beaUcoUp
rUptUre
poUrquoi
poUrsUite
brUsqUe
etc., etc.

## *Like Letters at Equal Intervals (separated by Three Letters).*

—nAissA—
cApitAine
ChanCelier
prEcisEr
sEcouEr
—EcutEr
—EillE—
ElogE
—EmblEr
—EndrE
—EntiEr
EntrEr
—EritE—
prEsquE
mEsurEr
EtagE
EtalEr
pEtitE
mEttrE
ExtrEme
InstInct

LégaL
LocaL
siMpleMent
eNchaNter
ciNquaNte
iNstaNt
iNstiNct
hOrizOn
propOrtiOn
PourPre
faRceuR
paRcouRir
pRendRe
laRgeuR
pRopoRtion
maRqueR
deSsaiSir
TraiT
éTroiT

etc., etc.

## *Bigrams Repeated.*

cAN c AN
bAR b ARe
BA r BAre
CA l CAire
CA n CAn
CA s CAde
—EN d ENt
—EN s ENt
EN t EN—
—ER c ER
—ER g ER
fER m ER
gouvER n ER
vER s ER
—EU r EU—
MU r MUre
—NS e NS
—NT a NT
—NT e NT—
—ON t ON—
tOU j OUrs
PRo PRe
SEn SE
poSSe SSion

T E n T E r
f U R e U R
m U R m U R e
C H e r C H e r
c h E R c h E R
c H E r c H E r

l o I N t a I N
Q U e l Q U e
— R E n d R E
T R a î T R e
q U E l q U E
etc., etc.

## FRENCH.—VII.

*Proportion of Words in Littré's Dictionary classified according to their Initials.*

| | | Per *Cent.* | *Total.* | | | Per *Cent.* | *Total.* |
|---|---|---|---|---|---|---|---|
| A | .. | 6·00 | 6·00 | N | .. | 1·90 | 61·55 |
| B | .. | 3·80 | 9·80 | O | .. | 2·60 | 64·15 |
| C | .. | 10·80 | 20·60 | P | .. | 10·60 | 74·75 |
| D | .. | 6·75 | 27·35 | Q | .. | 0·80 | 75·55 |
| E | | 7·00 | 34·35 | R | .. | 7·50 | 83·05 |
| F | .. | 4·85 | 39·20 | S | .. | 7·10 | 90·15 |
| G | .. | 3·30 | 42·50 | T | .. | 5·60 | 95·57 |
| H | .. | 2·50 | 45·00 | U | .. | 0·40 | 96·15 |
| I | .. | 3·50 | 48·50 | V | .. | 3·20 | 99·35 |
| J | | 1·30 | 49·80 | W | .. | 0·02 | 99·37 |
| K | .. | 0·05 | 49·85 | X | .. | 0·03 | 99·40 |
| L | | 3·00 | 52·85 | Y | .. | 0·01 | 99·41 |
| M | .. | 6·80 | 59·65 | Z | .. | 0·11 | 99·52 |

The shortage of 0·48 per cent. in the total is due to blanks and the approximate nature of the calculations. The above proportions vary from one dictionary to another.

## ITALIAN.—I.

*Order of Letter Frequency.*

According to Valerio: E I A O R L N T S C D P, etc.
According to Vesin de Romanini: E I A O, followed by L N R S, etc.

*Order of Frequency of Final Letters (Langie).*

I A E O N L R D U.

The same letter frequently ends two, three, four, or five consecutive words.

*The Commonest Bigrams (Valerio).*

ER, ES, ON, RE, EL, EN, DE, DI, TI, SI, LA, AL, AN, RA, NT, TA, CO, IN, LE, TO, IO, AR, NE, OR.

*Frequency of Double Letters (Valerio).*

LL, SS, TT, EE, PP, NN, BB, GG, CC.

All the consonants may be doubled except H, J, and Q.

*Words of One Letter.*

A, E, I, O.

## ITALIAN.—II.

*The Commonest Trigrams (Valerio).*

CHE, ERE, ZIO, DEL, ECO, QUE, ARI, ATO, EDI, IDE, ESI, IDI, ERO, PAR, NTE, STA.

The letters J and H are always followed by a vowel.

The letter H is used only in the groups CH and GH, and in four forms of the verb *avere* (to have): HO, HAI, HA, HANNO.

The letter Q is always followed by U.

Proportion of E (Valerio): 12·6 per cent.

Proportion of vowels (Valerio): 46 per cent.

## SPANISH.—I.

*Order of Letter Frequency (Valerio).*

E A O S I R N L D T C U P, etc.

*Order of Frequency of Final Letters (Valerio).*

A E S O N L R Y I D Z U, etc.

*The Commonest Bigrams (Valerio).*

ES, EN, EL, DE, LA, OS, AR, UE, RA, RE, ER, AS, ON,
QU, ST, AD, AL, OR, SE, TA, CO, CI, IO, NO.

*Frequency of Double Letters.*

CC, LL, RR, infrequently AA, EE, OO, NN.

According to Valerio: EE, LL, RR, SS, DD.[1]

*Words of One Letter.*

A, E, O, U, Y.

Single-letter words that may occur in succession are O A or Y A.

## SPANISH.—II.

*The Commonest Trigrams (Valerio).*

QUE, EST, ARA, ADO, AQU, DEL, CIO, NTE, OSA,
EDE, PER, IST, NEI, RES, SDE.

*Doubled Letter beginning a Word.*

*L*L.

The letters Z, J, H, and V are always followed by a vowel.

Q is always followed by U.

Proportion of E (Valerio): 14 per cent.

Proportion of vowels (Valerio): 48 per cent.

[1] Neither S nor D can be doubled in the same word, but they occur consecutively as the final of one word and the initial of the next.—TRANSLATOR.

## GERMAN.—I.

### *Order of Letter Frequency.*

According to Kasiski: E N I R S T U D A H, etc.
According to Valerio: E N R I T S D U A H, etc.
According to Vesin de Romanini: E, then N I R S U Ü, etc., the rarest being Q X Y J C.

### *Order of Frequency of Final Letters (Valerio).*

N E R T S D H U Z F, etc.

### *The Commonest Bigrams (Valerio).*

EN, ER, CH, ND, DE, IE, TE, RE, EI, UN, GE, DI, ES, BE, IN, IT, HE, etc.

### *The Commonest Final Bigrams.*

EN, ER, then the letters S, T, and E.

### *Frequency of Double Letters.*

EE, TT, LL, SS, DD.

### *Double Letters at the End of Words.*

NN, SS, less frequently LL, EE.

## GERMAN. II.

### *The Commonest Trigrams (Kasiski).*

EIN, ICH, DEN, DER, TEN, CHT, SCH, CHE, DIE, UNG, GEN, UND, NEN, DES, BEN, RCH.

*The Commonest Two-Letter Words.*

AB, AM, AN DA, DU, ER, ES, IM, IN, OB, SO, UM, WO, ZU, then JA, NU, etc.

The bigram UN frequently commences a word.
Q is always followed by U.
C is always followed by H or K, except in "foreign" words.
Proportion of E (Valerio): 18 per cent.
Proportion of vowels (Valerio): 35 per cent.; (Kaeding): 42·12 per cent.[1]

## GERMAN.—III.

*Proportion of Words in Sachs's Dictionary classified according to their Initials.*

| | | Per *Cent.* | *Total.* | | | Per *Cent.* | *Total.* |
|---|---|---|---|---|---|---|---|
| A | .. | 11·50 | 11·50 | N | .. | 1·92 | 63·39 |
| B | .. | 7·70 | 19·20 | O | .. | 0·88 | 64·27 |
| C | .. | 0·66 | 19·86 | P | .. | 3·08 | 67·35 |
| D | .. | 3·92 | 23·78 | Q | .. | 0·26 | 67·61 |
| E | .. | 5·15 | 28·93 | R | .. | 2·46 | 70·07 |
| F | .. | 4·67 | 33·60 | S | .. | 10·67 | 80·74 |
| G | .. | 6·44 | 40·04 | T | .. | 2·80 | 83·54 |
| H | .. | 6·55 | 46·59 | U | .. | 3·96 | 87·50 |
| I | .. | 0·96 | 47·55 | V | .. | 4·90 | 92·40 |
| J | .. | 0·77 | 48·32 | W | .. | 3·85 | 96·25 |
| K | .. | 6·40 | 54·72 | X | .. | 0·03 | 96·28 |
| L | .. | 3·45 | 58·17 | Y | .. | 0·03 | 96·31 |
| M | .. | 3·30 | 61·47 | Z | .. | 3·08 | 99·39 |

[1] The German authority, F. F. W. Kaeding, based his calculations on a total of 60,558,018 letters (!); he established the presence of 9,260,044 E's, 6,363,537 N's, etc. It may be noted that one volume of the large dictionary of Larousse contains about 20,000,000 characters.

The shortage of 0·61 per cent. in the total is due to blanks and the approximate nature of the calculations.

NOTE.—These proportions vary from one dictionary to another. In this case, the middle of the dictionary occurs at K; in Feller's pocket dictionary it occurs at M; in Niethe's numbered dictionary at *L*, etc.

## RUSSIAN.—I.

### *Order of Letter Frequency.*[1]

According to *L*angie: O A N I S E T V R L K M, etc.

The letter I predominates in French transcription.

Texts in Russian characters: O A I L E N, hard sign, D T M V R U K P, etc.

English transliterations: O Y A I E L N H D T S M U V R Z K P, etc.

French transliterations: O I A E L N T D C H M U V R K P, etc.

### *Final Letters.*[1]

According to *L*angie: Hard sign, then O, E, (I)A, I, (K)H (ignoring final hard sign), A, Ĭ, etc.

Russian texts: Hard sign, U, O I, soft sign, (Y)A, E, Y, A, M, V (ignoring final hard sign), etc.

English transliterations: A, U, E, O, I, soft sign, Y, M, V, etc.

### *The Commonest Bigrams (Langie).*

ST, NO, EN, GO, TO, KA, KO, NA, ER, RA, *L*I, SK, OS, M', RO, PO, ZA.

[1] Including results of supplementary investigations by translator.

*The Commonest Trigrams (Langie).*

AGO, STV, ENI, OST, YKH (bigram in Russian characters), TOR, STA, IKH (bigram), ENN, NOV, ORO, STO, EGO, LIS, NI(I)A, SKA, AL', OM', NNO, ERE, ĪSK, NY(K)H, etc.

NOTE.—The apostrophe represents the final hard sign.

*Double Letters (Langie).*

NN, (I)A(I)A, EE, (I)U(I)U, SS, OO, ZZ.

*Words of One Letter (Langie).*

I, (I)A, O, U, A.

NOTE BY TRANSLATOR.—To these may be added, if final hard sign is ignored, V', K', S'.

## RUSSIAN.—II.

*The Commonest Tetragrams (Langie).*

NY(K)H', PRAV, TSTV, VENN, UET:, VSTV.

NOTE.—The colon in the above represents the soft sign.

*The Commonest Pentagrams (Langie).*

SKAGO, STVIE, L:STV.

*The Commonest Hexagrams (Langie).*

STVENN, NNOSTI.

*Like Letters separated by One Letter (Langie).*

ILI, KAK, OBO, OVO, OGO, ODO, OKO, OLO, ONO, OSO, POP, TOT, TUT, etc.

Proportion of O (Langie): 10·7 per cent.
Proportion of vowels (Langie): 43·5 per cent.

## PORTA'S TABLE.

This table was composed by Giovanni Battista da Porta, a Neapolitan physician, author of a work on cryptography entitled *De furtivis litterarum notis, vulgo de ziferis*, Naples, 1563.

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

The capital letters on the left serve to form the key or word agreed upon, the letters of which, in succession, indicate the alphabets selected. Each pair of capitals jointly control the alphabet ranged in two lines to their right.

Let us suppose that the capital letter G is used to cipher the plain letter *i*. It will be noted that in the double line to the right of G the letter *s* occurs immediately

below *i*; accordingly *s* is taken as the cipher equivalent of *i*. Again, the plain letter *n*, ciphered by means of the same G, will be represented by d, which occurs *immediately above*. The rule, therefore, is to take the letter which occurs either below or above that of the plain text in the double line corresponding to the key-letter. For instance, to cipher the word "red" by means of the key-word CAR, we first look for r in the double line to the right of C, and find immediately above it the letter *f*. Proceeding in like manner with the second letter e (key-letter A), and the third letter *d* (key R), we obtain the result:

r e d
C A R
=f r v

For deciphering, we adopt exactly the same method, the cipher word "vtu," with the key-word NOT, for example, resulting in:

v t u
N O T
=b a d

## VIGENÈRE'S TABLE.

This table was established by Blaise de Vigenère, translator and French diplomat, author of a work entitled *Traité des chiffres ou* secrètes *manières* d'*écrire*, Paris, 1586.

The upper horizontal line of capitals represents the plain-text alphabet; the column of capitals to the left is used to form the key-word.

Supposing the first letter of the key-word is R, and the first letter of the plain text i, we descend from I in the top line of capitals until we reach the line of small letters

beginning from R in the column to the left. At the point of intersection we find *z*, which becomes the first letter in the ciphered text (see p. 28).

To decipher the word " kik " by the aid of the key-word REX, we first look for *k* in the horizontal line beginning

*Letters of plain text*

*Letters forming the Key-word (Ciphering Line)*

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

*Letters forming the Key-word. Reserve*

*Letters of plain text. Reserve*

at R, and at the top of the column in which the *k* occurs we find T, which is the first letter of the plain word. Proceeding in like manner with the others, we obtain:

k i k
R E X
=t e n

## NUMBER OF POSSIBLE COMBINATIONS.

| With— | *Number of Combinations.* |
|---|---|
| 3 letters[1] | 6 |
| 4 ,, | 24 |
| 5 | 120 |
| 6 | 720 |
| 7 | 5,040 |
| 8 | 40,320 |
| 9 | 362,880 |
| 10 | 3,628,800 |
| 11 | 39,916,800 |
| 12 | 479,001,600 |
| 13 | 6,227,020,800 |
| 14 | 87,178,291,200 |
| 15 | 1,307,674,368,000 |
| 16 | 20,922,789,888,000 |
| 17 | 355,687,428,096,000 |
| 18 | 6,402,373,705,728,000 |
| 19 | 121,645,100,408,832,000 |
| 20 | 2,432,902,008,176,640,000 |

## BRITISH SURNAMES.

*Frequency of Terminations* (*compiled by Translator*).

In a list of over a thousand different surnames, numerical position was occupied by the following terminations, in order of frequency:

SON, TON, ER, ING(S), LEY, FORD, STON(E), MAN, OCK, BY, HAM, LAND, ICK, ETT, WELL, FIELD, KIN(S), LOW(S), WOOD, MORE, BURN, HURST, WORTH, DALE, SHAW, BOROUGH, STOWE, RIGHT, WAY, STEAD.

[1] *I.e.*, ABC, ACB, BAC, BCA, CAB, CBA.

## FRENCH SURNAMES.

*Frequency of Terminations (Langie).*

Out of 1,000 French surnames (approximately):

50 end in IER.
38 end in ARD.
21 end in EAU.
19 end in AUD.
15 each end in LET, LLE.
13 each end in AND, NET.
12 each end in AUX, ÈRE, ERT.
11 each end in LOT, RON, SON.
10 each end in OUX, TTE, ULT.
9 each end in CHE, GER.
8 end in LIN.
7 each end in RIN, UET.

## CRYPTOGRAPHIC MATERIAL.

One or two manuals of cryptography (see Bibliography).
Dictionaries in several languages.
English, French, German, etc., rhyming dictionaries.
Two Saint Cyr slides (see p. 110).

Two graduated rules, one numbered from 1 to 50, the other from 51 to 100.

Paper ruled in squares.
Slates ruled in squares.
Tracing paper.
Coloured pencils.
A T-square (useful for consulting Vigenère's Table).
A ready reckoner for rapidly calculating proportions.

A few hundred counters on which the letters of the alphabet are inscribed. For instance, in 100 counters, one would have 18 E's, 9 S's, 8 R's, 7 A's, 7 I's, 7 N's, etc. The use of counters from time to time rests the eyes, and enables one to try a number of combinations more rapidly than could be done with pen or pencil.

---

# BIBLIOGRAPHY

## WORKS RECOMMENDED.

*La cryptographie dévoilée*, by C. F. Vesin de Romanini. Paris, 1857.

*Die Geheimschriften und die Dechiffrir-Kunst*, by F. W. Kasiski Berlin, 1863.

*Handbuch der Kryptographie*, by Ed. B. Fleissner von Wostrowitz. Vienna, 1881.

*La cryptographie militaire ou des chiffres usités en temps de guerre*, by Aug. Kerckhoffs. Paris, 1883.

*La cryptographie et ses applications à l'art militaire*, by H. Josse. Paris, 1885.

*Essai sur les méthodes de déchiffrement*, by P. Valerio. Paris, 1893.

*La cryptographie pratique*, by A. de Grandpré. Paris, 1905.

# PART IV

## THE PLAYFAIR CIPHER SYSTEM, ETC.

By Translator

It is surprising that there is no work in cryptography in English, although M. Langie points out that there is an extensive bibliography in other languages. I have made a careful search, both in England and the United States, for a book or manual on this fascinating subject, but without success. M. Langie defines cryptography as the art of communicating thoughts secretly, and this certainly appears to me to be a better definition than the stereotyped one of "secret writing," as it is perfectly obvious that writing is not the only medium by which secret communication can be effected. It used to be a great problem to travellers and residents in various parts of Africa how news could be transmitted with almost incredible rapidity over large distances, and many were inclined to attribute this to some supernatural agency. Further investigation, however, proved that the news was transmitted by beating a drum in a certain manner, as provided for in a prearranged code, the message being relayed from one post to another.

Cryptography, in some form or other, has a surprisingly great bearing upon the everyday events of ordinary life. You will find upon your handkerchief a mysterious little symbol which to you is meaningless, but which in your laundry indicates your name and address, and many a fugitive criminal has been brought to justice by such a

slender clue as a laundry mark upon some garment which he has had to leave behind at the scene of his crime.

Racegoers may have noticed individuals standing on the top of a cab or on some coign of vantage, semaphoring energetically, in the intervals between the races. This process is called "tictacking," and I understand that the men operating it have various codes, which they do their best to keep secret, for transmitting prices from Tattersalls' ring to the outside bookmakers.

The marking of cards by sharpers is a form of cryptography in which an amount of ingenuity is exhibited worthy of a better cause. Playing cards, ostensibly for conjuring purposes, are sold publicly in the United States, each card being marked in such a manner that any one with a little practice can as readily read the card from the back as its face. One of the commonest forms of indicating the face of a card on its back is in the form of a clock, as shown in the following diagram:

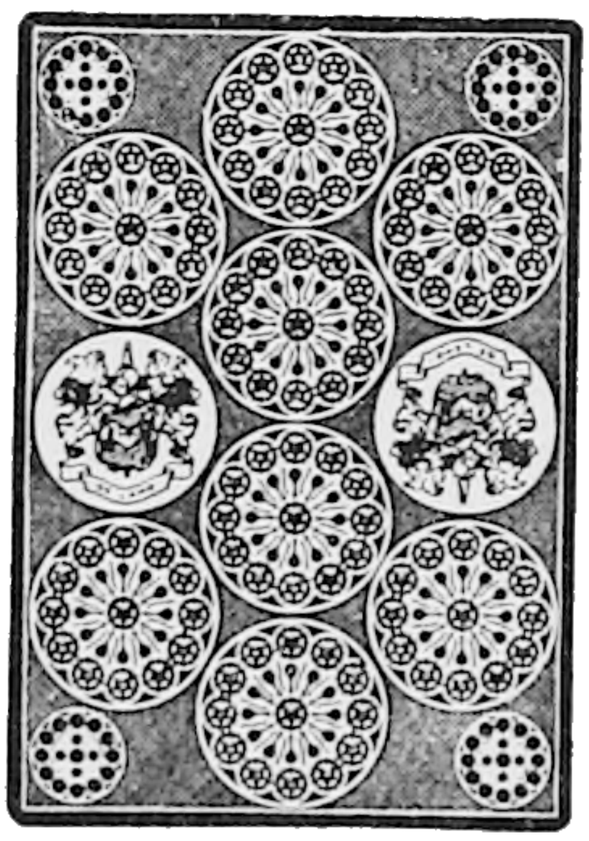


FIG. 1.

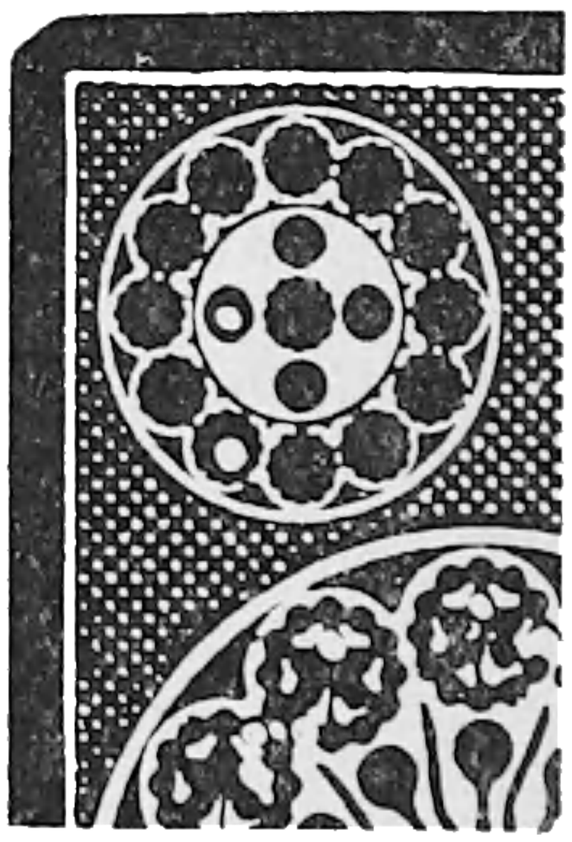


FIG. 2.

Fig. 1 shows the back of the card. At the four corners of Fig. 1 will be observed four small rings, an enlargement of which is shown in Fig. 2. This is intended to represent a clock and the twelve outer rings represent the hours. A small white dot at one o'clock represents

an ace, and so on until eleven o'clock, which indicates a Jack, while twelve o'clock denotes a Queen, and a dot in the centre spot represents a King. The suit is indicated by a small white dot in one of the four small circles around the centre spot. The top dot represents diamonds, the one on the right clubs, the one on the bottom hearts, and the one at the left spades. Even after you are informed that the cards are marked, it is surprisingly difficult for the uninitiated to detect these marks and, in passing, I cannot refrain from repeating the advice so often given that great care is essential when playing cards with strangers!

Business men find it necessary to make extensive use of some form of secret writing to indicate the price of the various goods they sell. This is most commonly done by means of some easily remembered word of ten different letters which are used to denote figures. For instance, the word "bankruptcy" might be employed, B to represent 1, A 2, and so on. An extra letter is generally used in the case of a figure which is repeated. For instance, 11 shillings would be expressed as BX/- or BZ/-. Certain firms use a variety of signs such as circles, rectangles, triangles, etc., but obviously it would not be a difficult task for anyone to break this code. It is sometimes most important for manufacturers and merchants that their prices should be strictly secret, and I have frequently been asked for advice and assistance in this respect, but it is extremely difficult to devise any system which can be easily written and read, that will at the same time defy the efforts of inquisitive rivals to discover the real figures.

The recent Great War stimulated the general interest in cryptography, and many and devious were the methods

adopted by spies in the various countries involved in the war to transmit information secretly. It would be impossible in the scope of this work to give more than passing mention to the many and ingenious devices that were adopted or to show how these efforts were almost invariably defeated by the ingenuity and resources of the cryptographers in the various censors' departments.

Secret communication is by no means confined to naval and military requirements or to diplomatic offices. Many important financial houses are well aware that unprincipled rivals would stick at nothing in order to be able to tap their messages and to break their cipher. It is obvious that the transfer by telegraph of large sums of money must be done with very great care and secrecy, and all the great banks employ elaborate methods to insure that their secrets will not fall into dishonest hands.

It is well known that tramps in all countries have their methods of communicating with each other. This is usually done by means of chalk marks on the door or wall of a house which one of the fraternity has visited. The French Police recently captured a copy of the code used by tramps, full particulars of which were published in the London *Sunday Express* of October 9, 1921.

M. Langie apparently considers that the use of invisible or sympathetic inks is of no value, and is almost certain to be detected. I do not altogether agree with this, as it frequently happens that it is of vital importance to the recipient of a secret message that he should be certain that his are the only eyes to see this message. When a person has to employ any means of secret communication, it must necessarily follow that someone is anxious to obtain possession of the secret information. In case of an ordinary cipher, the letter may be opened and photo-

graphed and the cryptogram solved without the rightful recipient being aware of the fact, and he fondly imagines that he alone is the custodian of the secret. If a suitable form of invisible ink is used, the recipient has at least the satisfaction of being absolutely certain that his are the only eyes to read the concealed message. There are many varieties of these sympathetic inks, the most widely known being milk, orange or lemon juice, dilute sulphuric acid, etc., which are all revealed by the application of heat. A very simple, although not very well-known form of sympathetic ink, is to moisten a clean pen with either saliva or water and write the message either upon an envelope between the lines of the address, or between the lines of a letter or inside the wrapper of a newspaper, as may be arranged. The recipient then pours a little ink on the arranged section and promptly rubs it off with water. The scratching of the pen with moisture has removed the glaze on the paper in such a way that it is invisible even with a powerful magnifying glass; but when ink is deposited on the surface it attacks those portions where the glaze has been removed, thereby making the words written stand out quite distinctly, while the surrounding glazed surface is merely slightly soiled by the application of the ink.

There are certain inks which can be made to appear and disappear at will. A solution of chloride of copper and water may be used as ordinary ink, and when the water evaporates the writing will disappear and can be revealed by the application of heat. A solution of nitric acid may also be used, and this can only be revealed by wetting the paper. After it dries, however, it again becomes invisible, so that the above-mentioned objection renders it unsuitable. A 2 per cent. solution of acid of

lead when used as an ink is quite invisible, and can only be made readable by immersion in hydrogen sulphide gas. This would appear to be a comparatively safe ink to use, but in the course of some experiments I made in New York at the Ledoux Laboratory, Mr. Albert M. Smoot, their technical director, made the discovery that after the writing had been made visible by means of exposure to hydrogen sulphide gas, it could be made to disappear again by slightly moistening it with peroxide of hydrogen. Writing done with a solution of potassium ferrocyanide can only be made visible by the application of some ferric salt. Probably the safest form of secret ink is a fairly strong solution of potassium nitrate or common nitre. Writing done with the resultant ink is absolutely invisible, and can only be revealed by the application of a flame which will run along the characters traced on the paper. Many readers will doubtless have seen this form of sympathetic ink in Christmas crackers. When making use of this form of secret ink, the writing should begin at the extreme end of the paper at a pre-arranged spot. I would recommend that anyone who is desirous of using this form of secret ink should first make some experiments to see that they get the exact strength of solution required and the right quality of paper. There is a counterpart to sympathetic inks in the form of disappearing inks which, however, are of very little practical value. The best known of these is a solution of starch with a few drops of tincture of iodine. The resultant ink is blue and to the uninitiated appears like ordinary ink. Within a short time, however, the iodine evaporates, and the starch becomes quite dry so that it leaves the paper without any trace of writing whatever.

M. Langie states that the cipher invented by Francis Bacon is extremely easy to break, but I am of the opinion that this system used with certain variations could be made extremely difficult. A well-known Baconian enthusiast, Colonel Fabyan of Chicago, believes that Bacon interpolated a great deal of secret information into the manuscripts of his various works by means of his cipher. The method supposed to be employed is the use of different kinds of type, but although a tremendous amount of research work has been done by Colonel Fabyan and his assistants I have been unable to obtain any concrete evidence which would prove that Bacon did employ his cipher in this manner, and the various claims that have been made up to the present appear to me to be based merely upon conjecture.

Students of cryptography should make themselves conversant with the Morse Code or Alphabet. The following table is used by all countries of the world except America, where a slightly different form is employed for inland telegraphy. In practice a dash is equal in length to three dots, and a space between two elements or signals in a letter is equal in length to one dot. The space between letters in a word is equal in length to three dots, while the space between words in a sentence is equal in length to five dots.

It will be seen that there is a liability to error in transmission of messages if the foregoing rules are not strictly adhered to. Bad spacing will convert A into E T or N into T E, and a slight examination of the following table will show many other telegraphic identicals, which all have to be borne in mind when endeavouring to decipher a cryptogram which has been telegraphed.

## International Morse Code Signals.

| *Letters.* | | | | *Figures.* | |
|---|---|---|---|---|---|
| A | . - | N | - | 1 | . – – – – |
| B | – . . . | O | – – – | 2 | . . – – – |
| C | – . – . | P | . – – . | 3 | . . . – – |
| D | – | Q | – – . – | 4 | . . . . – |
| E | . | R | . | 5 | . . . . . |
| F | . . – . | S | . . . | 6 | – . . . . |
| G | – | T | - | 7 | – – . . . |
| H | . . . . | U | . | 8 | – – – . . |
| I | . | V | . . . – | 9 | – – – – . |
| J | . – – – | W | . – – | 0 | – – – – – |
| K | – | X | – . . – | | |
| L | . – . . | Y | – . – – | | |
| M | – – | Z | – – . . | | |

M. Langie has omitted to give any reference to the "Playfair" cipher, which has been extensively used for military purposes. This cipher is one of the substitution variety, and may be operated with one or more key-words, which may be located in the cipher square by pre-arrangement. This square is divided into twenty-five separate compartments, and the letter J is always represented by I.

Suppose the key-word to be "BANKRUPTCY"—to be distributed between the first and fourth lines of the square. Fig. 1 will show their position:

| | | | | |
|---|---|---|---|---|
| b | a | n | k | r |
| | | | | |
| | | | | |
| u | p | t | c | y |
| | | | | |

Fig. 1.

The other letters of the alphabet which are not included in the above ten letters of the key-word are then added in alphabetical order, beginning at the first vacant square, as shown in Fig. 2:

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

Fig. 2.

The rules for enciphering by the Playfair method are as follows:

1. Divide the plain text of the message to be sent into groups of two letters. When there is an odd number of letters, say 21, complete the last odd letter by the addition of X or Z.

2. In the case of repeated letters, such as EE or LL, divide these by inserting X or Z.

3. Each pair of letters in the square, when filled in by agreement, must be either in the same vertical line, the same horizontal line, or at the diagonally opposite corners of a rectangle formed by the smaller squares within the whole square.

4. When the pair of letters to be enciphered occurs in a vertical column, substitute letters immediately below the letter of the plain text. When this letter is at the foot of a column, substitute for it the letter at the top of any column—*e.g.*, to encipher U S, which occurs in

the first vertical column of Fig. 2, the substitution would be S B.

5. When the pair of letters to be enciphered occurs in the same horizontal column, substitute the letter at the right of the plain text letter. When this letter is at the end of a column, substitute the letter at the extreme left of that column—*e.g.*, to encipher T Y, which are in the fourth horizontal column of Fig. 2, the substituted letters would be C U.

6. When the letters to be enciphered are at opposite corners of a rectangle, substitute each letter of the pair by the letter in the other corner of the rectangle on the same horizontal line with it—*e.g.*, on Fig. 2, A C would be enciphered K P, D O would be represented by G I, and R L by A Q.

7. The enciphered message may be written in groups of three, five, or eight letters, and the letter agreed upon for the purpose of dividing repeated letters may be used to fill up a group. Should more than one letter be required to complete a group, as many letters as are required may be taken from a prearranged word, such as STOP, FINISH, etc.

To decipher a message sent in this code, you simply divide the letters into pairs and reverse the writing according to the preceding rules. The decipherer should never neglect to write down the X or Z, as the case may be, when used as a divisory letter. This simple precaution will often save a lot of time in decoding a lengthy message.

The following example will show the method of enciphering in accordance with the foregoing rules, with "bankruptcy" as the key-word, distributed in the first and fourth columns of the square.

Suppose the message required to be enciphered to be: "You may expect relief in three days," and that X is to be used to divide duplicated letters. Divide the plain text into groups of two letters each, as follows:

YO UM AY EX PE CT RE LI EF IN TH
CQ TI RP GV VL YC AH ML FG MB YF
RE XE DA YS
AH VG EB UZ

and then underneath each group of substituted letters, as shown above. This being done, the message should be divided into groups of five, and sent as follows:

CQTIR PGVVL YCAHM LFGMB YFAHV GEBUZ

In the same manner, the message "Sell all you have immediately" may be sent, on the understanding that the cipher is to be divided into groups of eight letters, for which Z is to be used to divide repeated letters, and STOP to complete an unfinished group. The resulting cipher will be as follows:

VDQVPEQV QPICERAL LOWQFELB PFQPWULC

The Playfair system is one of the best forms of ciphering, for several reasons. It is very simple to commit to memory, after which all that is necessary for the sender and receiver to bear in mind are the key-words or sequence of key-words, and the position they are to occupy in the square. The key may consist of one or more words, provided they contain different letters—*e.g.*, FAIR CUSTOM or A JURY OF MEN. The key-word may be changed in alternate words or at certain intervals. For instance, a message might be sent using as key-words BANKRUPTCY in the first and fifth columns of the

square, CUMBERLAND in the second and fourth, and TICHBOURNE in the first and third, and many other variations will readily suggest themselves to the student. The message may also be sent in groups of three, four, five, or eight letters, so there are abundant opportunities for throwing obstacles in the way of a decipherer who is not in possession of the keys.

An indication of the difficulties to be overcome by the decipherer will be seen in the first example, where the six E's in the plain text are represented in the cipher by G V H F H and G, and in the second example the four E's are transcribed D L F and F.

That these difficulties can be overcome is proved by the fact that I sent a message ciphered by the Playfair method to my friend Lieut.-Commander W. W. Smith, one of the most skilful cryptographers in the U.S. Navy, who has kindly given me the following account of the steps he took to solve the cipher, which will be of great assistance to the student. We are both of the opinion that when important messages have to be sent they should be enciphered with more than one key-word, as by this method less time is required to cipher the message than would be necessary if you endeavour to avoid the use of the commonest digraphs, or to split them by means of divisory letters.

## Solution of the Playfair Cipher.

*By Lieut.-Commander W. W. Smith, U.S. Navy.*

The Playfair cipher may be recognised by the following characteristics:

(*a*) It is a substitution cipher.

(*b*) It always contains an even number of letters.

(*c*) When divided into groups of two letters each, no group contains a repetition of the same letter, as NN or EE.

(d) Unless the message is very short there will be recurrence of groups, and this recurrence will, in general, follow the order of normal frequency of digraphs.

(e) In messages of length, unless encipherment has been made from several squares of different keys, whole words are likely to recur in the form of repeated groups.

In the solution of the Playfair, we need not consider the normal frequency of individual English letters, E, T, O, A, N, etc. We are, however, very much concerned with the normal frequency of pairs or digraphs: *th*, er, *on*, *an*, re, etc., as will be shown later.

Before taking up the actual solution of a test message, let us examine the system for its inherent weaknesses: From the square of the key-word BANKRUPTCY shown on page 167, it is seen that the cipher letters YF represent *th* of plain text, and so long as this same key is in use, *th* plain can only be represented by YF in cipher. Likewise, *on* is always MK, and *an* NK. (NOTE: Throughout this discussion we will represent cipher letters by capitals and plain text by small letters. Also, in referring to equations as above, we may designate the letters of the equation as 1, 2, 3, and 4. Thus 1, 2=3, 4, where 1 and 2 are letters of the cipher group, and 3, 4 are plain text letters.)

Case 1. Letters at opposite corners of a rectangle:

If YF=th
then FY=ht
TH=yf
HT=fy

Case 2.—Two letters in the same line or column:
In line 1 of the square,

NK=an
and KN=na

But AN is not equal to *nk*, and NA is not equal to *kn*, and reciprocity is only partial.

We may therefore note Rule I. as follows:

Rule I.—Regardless of the position of the letters in the square, if the assumption is made that 1, 2=3, 4, the following equation will also hold: 2, 1=4, 3; while if the letters 1 and 2 form opposite corners of a rec*tangle*, the additional equations may be assumed:

3, 4 (cipher)=1, 2 (plain),
and 4, 3 (cipher)=2, 1 (plain).

Now, as each letter of a line or column can be combined with but four other letters of its own line, and with four letters of its own column, and as each letter when employed at the corner of a rectangle can be combined with each of 16 letters to form a group, it would appear that Case 1 is twice as probable as Case 2.

Now, in the square, note that:

| | | |
|---|---|---|
| NK=an | | FA=en |
| FK=gn | | FL=em |
| MK=on | also | FP=et |
| TK=cn | | FV=ew |
| WK=xn | | FG=ef |

From this it is seen that of the twenty-four equations that can be formed when each letter of the square is employed either as the initial or final letter of the group,

five will indicate a repetition of a corresponding letter of plain text.

Hence, Rule II.—After it has been determined, in the equation 1, 2=3, 4, that, say, FA=*en*, there is a probability of one in five that any other group beginning with F indicates *e*–, and that any group ending in A indicates –*n*.

After such combinations as er, or, and *en* have been assumed or determined, the above rule may be of use in discovering additional digraphs and partial words.

Rule III.—In the equation 1, 2=3, 4, 1 can never equal 3, and 2 can never equal 4. Thus, KR could not possibly indicate er, or AY=*an*. This rule is of use in eliminating possible equations when the cipher is under investigation.

Rule IV.—In the equation 1, 2=3, 4, if 1 and 4 are identical, the letters are all in the same line or column and in the relative order 3, 4, 2, – –. In the square shown, NK=*an*, and the order is ANK– –, which is equivalent to –ANK–, or – –ANK. This is a very useful rule.

Rule V.—If 2=3, the letters of the equation are in the same line or column, and in the relative order 2, 1, – – 4, which is equivalent to 4, 2, 1, – –, or – 4, 2, 1, –. Thus it is seen that in the square, BR=*rk*, and the order is RB– –K, which is the same as KRB– –, or B– –KR.

Some cryptographers claim that from an analysis of the cipher message, the letters which are found to combine in groups with the greatest variety of other letters will very likely be the letters of the key-word. This may be of some value provided the key were contained in the first two lines of the square, and if the key-letters

could positively be eliminated it would be possible to solve the message and reconstruct the square. Unfortunately, these letters cannot be positively eliminated, and the square is not always constructed in a regular manner. The disadvantage of this system is that it tempts the student toward guessing the key-word. A false and usually unsuccessful method of attack.

Rule VI.—Analyse the message for group recurrences. Select the groups of greatest recurrence and assume them to be high-frequency digraphs. Substitute the assumed digraphs throughout the message, testing the assumptions in their relation to other groups of the cipher.

The reconstruction of the square proceeds simultaneously with the solution of the message and aids in hastening the translation of the cipher. Let us now take up the solution of the actual test message given below:

| | | | |
|---|---|---|---|
| APBNOH | RNAORA | GIOREB | WQGRUD |
| ANNSXR | OUUADT | BNOARP | NIYERB |
| KBSNHL | DYPYHS | NYSIQC | WRCSFQ |
| ENPFVB | NVOBNX | GNXROU | OAFLIG |
| OAEYSC | SOKTDN | KNXDTF | CIRNOM |
| FRTACS | HGQROA | BHNSRS | ECOROT |
| VSBNOH | RNRARB | INTHXU | QNFLRN |
| RUXUUO | QENSXU | GRGBTR | CNORLC |
| NESCSD | VNNSGR | ARGBIZ | RAREHN |
| RARGCI | YCNIVK | DADYPY | RXXUUY |

In working with the cipher, disregard the above grouping and rearrange the message in pairs of letters.

We will first analyse the above message by drawing a chart of group recurrences (Fig. 1.)

FIRST LETTERS OF PAIRS.

SECOND LETTERS OF PAIRS.

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

This chart shows that the following groups occur in the cipher four times each:

| | | |
|---|---|---|
| OA | RN | GR |
| RA | NS | XU |

No group occurs more than four times. This is unusual. The groups BN, CI, and OR occur three times each. All of the above groups must represent common pairs of letters in English text. It is well known that the order of frequency of common pairs of letters is as follows (from a count of 2,000 semi-military letters):

| | | | | | |
|---|---|---|---|---|---|
| th | 50 | at | 25 | st | 20 |
| er | 40 | en | 25 | io | 18 |
| on | 39 | es | 25 | le | 18 |
| an | 38 | of | 25 | is | 17 |
| re | 36 | or | 25 | ou | 17 |
| he | 33 | nt | 24 | ar | 16 |
| in | 31 | ea | 22 | as | 16 |
| ed | 30 | ti | 22 | de | 16 |
| nd | 30 | to | 22 | rt | 16 |
| ha | 26 | it | 20 | ve | 16 |

The above table and the frequency chart of Fig. 1 must be kept constantly available throughout the attack on the ciphered message.

Of the most commonly occurring groups of the cipher, OA, RA, RN, NS, GR, and XU, we note from Fig. 1 that the reciprocals AO, AR, SN, RG occur only once each, while NR and UX do not appear in the message. This is unfortunate, for had one of these reciprocals occurred, say, three times, we might have begun by assuming the groups to be *er* and re (see above table).

Now, as has been shown, the group GR cannot mean er or *or*, for the second letter of an equation cannot equal the fourth. Nor can RA or RN symbolise re or rt (Rule III.). Thus we can eliminate a few of the possible

meanings of the groups. But any one of the six groups may represent *th*. The most common four-letter group in English is known to be THER, while such groups as INTH, ENED, TION, etc.. are very often encountered.

Hereafter, in referring to the groups of the cipher, let us indicate by a small figure the number of times that the group occurs, thus $XU_4$.

Note that in lines 1 and 7, the following combination recurs: $BN_3\ OH_2\ RN_4$, and that in lines 2 and 4 we have $XR_2\ OU_2$, and in lines 3 and 10 we have $DY_2\ PY_2$. But it will be useless to attempt to guess the meaning of the two last mentioned groups, as the individual groups are not frequently used in the cipher, and occur only with each other. Thus XROU and DYPY *may* indicate four unusual letters that recur in the cipher, or they may be caused by the insertion of nulls between repeated letters. To guess their meaning would not greatly assist in extending our investigation. Likewise, it is best not to begin our assumption at the beginning or end of the cipher, as the sender of the message often purposely begins and ends with unusual words. The repeated groups $BN_2\ OH_2\ RN_4$, however, present opportunities.

Also, note the combinations in the cipher of our most common groups:

$$RN_4RA_4$$
$$GR_4OA_4$$
$$NS_4GR_4$$
$$NS_4XU_4$$

We must first assume each of these groups in turn to be *ther*, which is the most common four-letter combination in English text. Failing to establish this relation, other combinations of common digraphs will be assumed.

$NS_4$ may be *th*, but $XU_4$ is probably not er, as it occurs

at the end of the cipher, in XUUY. However, it must be considered as a possibility. $NS_4$ $GR_4$ cannot be *th*er, as GR cannot be er (Rule III.).

Suppose $GR_4$ $OA_4$ to be *th*er. This is an excellent assumption, as reciprocals of both groups occur in the message, and if GR=*th* and OA=*er*, RG=*ht* and AO=*re*.

Now *ht* is an uncommon digraph, and can occur only in *w–it–ht–he* or in a combination of *ght*, as in "eight" or "thought." Pursuing this assumption, we assume in line 10, for the combination HN–RA–RG, *–w–it–ht*. Then RA=*it*, and AR=*ti*. Substitute these values throughout the message and we get for AO–RA in line 1, re*it*, and for GR AR in line 9, *thti*. These do not appear promising, and after carrying the investigation farther it was decided to abandon the original assumption that $GR_4$ $OA_4$=*ther*.

NOTE: In all work of this nature false assumptions will be made, but as the investigation proceeds they will eventually be proved false. In this case a great many false starts were made due to unusual conditions, and *th*er was abandoned in favour of such combinations as *tion*, *ered*, etc., before the investigation resulted in success. For the sake of brevity, these steps will be omitted.

| | |
|---|---|
| Assume | $RN_4RA_4$ to be *th*er (line 7). |
| Then | RN=th |
| and | RA=er |
| | NR=ht |
| | AR=re. |

Unfortunately, we have no NR in the cipher, and but one AR. Make these substitutions throughout (Fig. 2).

AP BN OH RN AO RA GI OR EB WQ GR UD
. th er he

AN NS XR OU UA DT BN OA RP NI YE RB
r–

KB SN HL DY PY HS NY SI QC WR CS FQ

EN PF VB NV OB NX GN XR OU OA FL IG
r– h–

OA EY SC SO KT DN KN XD TF CI RN OM
th

FR TA CS HQ GR OA BH NS RS EC OR OT
–r he

VS BN OH RN RA RB IN TH XU QN FL RN
th er e– –r th

RU XU UO QE NS XU GR GB TR CN OR RC
he –t

QN ZS SD VN NS GR AR GB IZ RA RE HN
he re er é–

RA RG CI YC NU VK DA DY PY RX XU UY
er eh

First step not underscored. Substitutions of 2nd and 3rd steps, pages 180 and 181, are underscored —. (Message divided into pairs.)

FIG. 2.

There is also a possibility (Rule I.) that TH=*rn*, and RE=*ar*, but these occur only once each, and the reciprocals ER and HT do not occur at all.

Now, if RA=*er*, we know, from Rule IV., that the three letters are in the same line or column of the square and in the order ERA– –.

As RN is assumed to be *th*, the partial square must be,

depending whether this equation is formed from a rectangle or a line:

(1)

E R A – T
–
H – – N

or, (2)

T
E R A – –
H
N

In either case, we have established the fact that H is somewhere in the same column with R, regardless of the position of T and N, and we have for certain:

(3)

–
E R A – –
–
H

Now note other groups containing R. We know from Rule II. that if RA=*er*, there is a chance of one in five that RB=*e*–, and RE=*e*–, and GR=–*e*.

Now GR is used four times in the cipher, and as there is a good chance that it may be –*e*, let us assume it to be the highest digraph ending in e in the frequency list. This digraph is *he*.

Then GR=he
RG=eh

Make these substitutions in the cipher (Fig. 2), at the same time adding to the square.

(4)

–
–
E R A – –
G H –

Going back to (1) and (2), if we combine (2) with (4) we have:

(5)

| | | |
|---|---|---|
| – | T | – |
| E | R | A |
| G | H | |
| – | N | – |

From the above we may obtain some partial equations, such as TH=–*r*, TA=–*r*, AN=–*r*, EN=*r*–, etc. Substitute these values in Fig. 2.

As we have as yet no substitutions that can be extended, we must attempt to find common digraphs to be substituted for more of the common groups. In line 9 we have the groups NS – GR – AR or NS – *he–re*. NS is used four times, and must be a common pair. Turning back to the list of normal frequency of digraphs, we find that *on* is the group of highest frequency next to *th* and er. Assume NS to be *on*.

If this assumption is correct, then by Rule IV., since 1=4, these three letters are in the same line, and in the order ONS– –. It is evident from our partial square that ONS – – cannot form a column. We may therefore build up the square as follows:

(6)

| | | | | |
|---|---|---|---|---|
| | T | | | |
| E | R | A | – | – |
| G | H | – | – | – |
| O | N | S | – | – |

NOTE: In the partially completed square the horizontal lines are definitely fixed as shown, for RA=*er*, and NS=*on*. We also know that in the column TRHN, R follows T and N follows H, for RN=*th*. But we are not certain that RH=*Tr*, as there is a fifth letter to be placed in the column, and it can only come below R or below N.

Now substitute in Fig. 3, *on* for NS and *no* for SN, and also the new groups that we get from the square above, namely:

| | | | |
|---|---|---|---|
| NG=oh | SR=na | SE=oa | SH=n– |
| GN=ho | OH=ng | EN=ro | HS=–n |
| RS=an | HO=gn | NE=or | GS=–o |
| AN=rs | OA=se | RO=en | SG=o– |
| NA=sr | AO=es | OR=ne | |
| | ES=ao | ON=–o | |

AP BN OH RN AO RA GI OR EB WQ GR UD
ri ng th es er –o ne –t he

AN NS XR OU UA DT BN OA RP NI YE RB
rs on sq su ri se o– e–

KB SN HL DY PY HS NY SI QC WR CS FQ
no –n n– rt

EN PF VB NV OB NX GN XR OU OA FL IG
ro ho se o–

OA EY SC SO KT DN KN XD TF CI RN OM
se n– th

FR TA CS HQ GR OA BH NS RS EC OR OT
–r se r– on

VS BN OH RN RA RB IN TH XU QN FL RN
ri th er e– –o nw th

RU XU UO QE NS XU GR GB TR CN OR RC
on he nt ne

QN ZS SD VN NS GR AR GB IZ RA RE HN
on he re er e– wh

RA RG CI YC NU VK DA DY PY RX XU UY
er eh

Step on page 183 underlined —.
Step on page 184 underlined twice =.

FIG. 3.

In the last two lines of Fig. 3 we now have *er**e*– HN er *eh*. HN cannot be *th*, and if taken from square 6 it would be *rh*. This would spell nothing, and as the word "where" suggests itself, we may assume HN=*wh*, which would give us an addition to the square as follows:

(7)

T
E R A – –
W
G H –
O N S –

Substitute TR=*nt*, TH=*nw*, and HN=*wh* in Fig. 3, also WR=*rt*.

Line 1 now shows a first word evidently ending in *ing*, but it cannot be the word "having" as the square does not permit *ha* to be represented by AP.

BN occurs three times, and must be a common group. *Ti* was tried, but was soon found not to be satisfactory. After a few similar suppositions *ri* was decided upon, and BN=*ri* substituted throughout.

If BN=*ri*, we see from the square that i cannot follow GH in line 3, and that B and *i* must be in the same separate column as below:

(8)

T
E R A – B
W –
G H –
O N S – I

It is evident now that lines 2 and 5 of the square form the key.

We are not able to determine whether the column B – – – I is as shown or is adjacent to the column A – – – S, but will place it as shown in (8) to avoid confusion.

Substitute in Fig. 3 the equations taken from the new square: HB=*r*–; IG=*o*–; IN=–*o*; GI=–*o*; NI=*o*–; SI=*n*–.

Note the first line. The word revealed is not "these" as at first supposed, but is "The ser–on." Few letters can fill the blank space, and we decide the word is "sermon." Thus GI=*om* and IG=*mo*.

We have but one of our six commonly-used groups left undeciphered—namely, $XU_4$. In line 7 we have –*o nw* XU. Returning to the partial square, X and Z, being uncommon letters, are probably not in the key. If not in the key, X probably follows W, and if U likewise follows T in the first line, XU="as," a common digraph, and *w*XU="was."

Also, as R and S are already in the key-lines, we may assume Q to precede T in line 1 of the square, and as *i* already appears, GH in line 4 is probably followed by K. Building up the square as above, we have:

(9)

| | | | | |
|---|---|---|---|---|
| Q | T | U | | |
| E | R | A | – | B |
| | W | X | | |
| G | H | K | – | M |
| O | N | S | – | I |

Many new groups now result. Fill in these substitutions in Fig. 4 and we see that more new groups are evident to complete the words. Such groups are underscored in Fig. 4.

In line 8, CN is evidently *io*, and this gives us the letter lacking in line 5 of the square. If CN=*io*, line 5 must read ONSIC, and the column BMI must adjoin UAXKS.

| | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|
| AP | BN | OH | RN | AO | RA | GI | OR | EB | WQ | GR | UD |
| du | ri | ng | th | es | er | mo | ne | | –t | he | pa |
| AN | NS | XR | OU | UA | DT | BN | OA | RP | NI | YE | RB |
| rs | on | wa | sq l | su | rp | ri | se | dt | o– | | ea |
| KB | SN | HL | DY | PY | HS | NY | SI | QC | WR | CS | FQ |
| ma | no | | | | –n | | n– | | rt | | |
| EN | PF | VB | NV | OB | NX | GN | XR | OU | OA | FL | IG |
| ro | | | | ie | s.w | ho | wa | sq | se | | om |
| OA | EY | SC | SO | KT | DN | KN | XD | TF | CI | RN | OM |
| se | | | n– | hu | | hs | | | | th | ig |
| FR | TA | CS | HQ | GR | OA | BH | NS | RS | EC | OR | OT |
| | ur | in | g.t | he | se | rm | on. | an | | ne | nq |
| VS | BN | OH | RN | RA | RB | IN | TH | XU | QN | FL | RN |
| | ri | ng | th | er | ea | so | nw | as | to | | th |
| RU | XU | UO | QE | NS | XU | GR | GB | TR | CN | OR | RC |
| at | as | qs | oq | on | as | he | me | nt | io | ne | d– |
| QN | ZS | SD | VN | NS | GR | AR | GB | IZ | RA | RE | HN |
| to | | | | on | he | re | | | er | e– | wh |
| RA | RG | CI | YC | NU | VK | DA | DY | PY | RX | XU | UY |
| er | e.h | | | st | | | | | a.w | as | |

FIG. 4.

Thus, building up the square from the pairs underscored in Fig. 4, we have:

Q T U – P
E R A B D
– W X – –
G H K M –
O N S I C

It is apparent that column 5 of the square should be transposed to left of column 1 (this does not at all affect the equations obtained), and the fifth and second lines are seen to yield the key-word "considerab."

P Q T U –
D E R A B
– – W X –
– G H K M
C O N S I

The letters now remaining to be placed are V, F, Z, L, and Y.

Carrying this process farther, we come to YE=*eq*, and may safely fill in the square:

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

We now complete the solution (Fig. 5). The key-word is "considerably."

So long as the relative order remains the same, we may transpose line 5 to the top of the square without affecting the equations obtained in enciphering or deciphering. This would give us:

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

or

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

All of the above squares are equivalent, and it is probable that the key was used in the second and fourth lines as in the last square.

It is now interesting to note how the Rules held true in a message not prepared by the writer. All of the commonly used groups of the cipher are listed below, with

their equivalent digraphs. It is seen that the digraphs follow normal frequency very closely, and that in no case does a repeated group indicate an uncommon pair:

$RN_4$ = th
$RA_4$ = er
$NS_4$ = on
$GR_4$ = he
$XU_4$ = as

$BN_3$ = ri
$CI_2$ = is
$OR_3$ = ne

| | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|
| AP | BN | OH | RN | AO | RA | GI | OR | EB | WQ | GR | UD |
| Du | ri | ng | th | es | er | mo* | ne* | da* | yt | he | pa |
| AN | NS | XR | OU | UA | DT | BN | OA | RP | NI | YE | RB |
| rs | on | wa | sq | su | rp | ri | se | dt | os | eq | ea |
| KB | SN | HL | DY | PY | HS | NY | SI | QC | WR | CS | FQ |
| ma | no | fw | el | ql | kn | ow | ns | po | rt | in | gp |
| EN | PF | VB | NV | OB | NX | GN | XR | OU | OA | FL | IG |
| ro | cl | iv | it | ie | sw | ho | wa | sq | se | ld | om |
| OA | EY | SC | SO | KT | DN | KN | XD | TF | CI | RN | OM |
| se | qe | ni | nc | hu | rc | hs | la | ph | is | th | ig |
| FR | TA | CS | HQ | GR | OA | BH | NS | RS | EC | OR | OT |
| hd | ur | in | gt | he | se | rm | on | an | do | ne | nq |
| VS | BN | OH | RN | RA | RB | IN | TH | XU | QN | FL | RN |
| ui | ri | ng | th | er | ea | so | nw | as | to | ld | th |
| RU | XU | UO | QE | NS | XU | GR | GB | TR | CN | OR | RC |
| at | as | qs | oq | on | as | He | me | nt | io | ne | dn |
| QN | ZS | SD | VN | NS | GR | AR | GB | IZ | RA | RE | HN |
| to | xi | ca | ti | on | He | re | me | mb | er | ed | wh |
| RA | RG | CI | YC | NU | VK | DA | DY | PY | RX | XU | UY |
| er | eh | is | lo | st | um | br | el | ql | aw | as | qx |

* Evidently a group left out, meant for "One day."

Q was used as a null.

FIG. 5.

One claim made in favour of the Playfair is that common pairs, such as *th*, er, *on*, etc., will not be enciphered in their normal frequency, due to their chance of being split up when the message is divided into two-letter groups prior to enciphering. This claim is well based, but when *th* is split up it will probably yield another common digraph, *he*. Furthermore, even though a large percentage of these digraphs is split, their frequency in the cipher is still relatively great. It is interesting to examine the following table prepared from the above problem:

| Digraph. | Times Occurring in Message. | Times Represented in Cipher. | Times Split. |
|---|---|---|---|
| *th* .. | 6 | 4 | 2 |
| *er* .. | 6 | 4 | 2 |
| *on* .. | 8 | 4 | 4 |
| *he* .. | 7 | 4 | 3 |
| *as* .. | 7 | 4 | 3 |
| *ri* .. | 4 | 2 | 2 |
| *re* | 4 | 1 | 3 |
| *is* .. | 3 | 2 | 1 |
| *in* .. | 5 | 2 | 3 |

## Codes

Closely allied to cryptography is the use of codes. In naval, military, and diplomatic circles, secrecy is the principal objective, and the utmost care is exercised to secure the codes from inspection by unauthorised persons. In commercial codes, the chief aim of the compiler is to provide an economical means of intercommunication with overseas business houses. It frequently happens, however, that important firms have to send messages where secrecy is essential.

One rough-and-ready method is to substitute for the actual code word opposite the required phrase another

code word—so many forward or back as may be arranged. This system, however, would present very little difficulty to anyone who wished to break the message, and a much safer method is to cipher the numbers which appear against the code words.

This may be done simply by means of a key-word. For instance, if the numbers of the code words you wish to cipher are:

22350 49861

and the key-word selected is

Buy another
123 4567890

with Z for repeated figures, the message would be ciphered:

UZYNRAEHOB

A more elaborate system of ciphering is to have a series of tables for the conversion of the figures with letters, compiled as follows:

00=AB
01=AC
02=AD
03=AE

and so on, up to 99.

It is obvious that any pair of letters in the alphabet may be used to represent any pair of figures, so that the variations of this form of ciphering run into millions, even when, in order to comply with the International Telegraph rules with regard to pronounceability, vowels and consonants are used alternately. Where economy in transmission is not an important factor, these variations can, of course, be increased to an enormous extent, and, without a knowledge of the code used, a message ciphered on this system is practically unbreakable.

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

T D R I Q U G H N A Z A J G B U P B R G I D

Z X F N O K K W I T I B M D A S J Y Z N F E

D W I M C G K O W T F X E N Z Y H D R A J X

W O C M T U Z E C W T G O S J H P U D F N D

I M J D T O L B V C U S U D Q A W M W X E K

B L N E K U V J G S I T V A H B A R D T U Z

W Q V A V L D U N C D L O X D F B Y R G P G

Z V C P A V F E B N J C U F G X A P M O Q

N Y F L Z E Q B U N C S I J K S U L V Q F

H G U V G R S E W L F A J A V J B O K Y M

L M X J O Z T C B A T R L U B A C R T I M

G I F X O Z C Z L E G L M Y Z F I G L A S

D K V Y N P S O J L C D E S F S W O T K M

I B S G E N C D L I W D X O T L D N A J T

F L I C H C L A T C N D U F R L J Y D A J

A S W E L T Z U K B P F A R Z L J O Q U V

H I T V O S R C W I C H B Y R T E D O Q U

G P B Y N C T R E Z C V J A K J M B O V Q

I B Y C X Z D A R V K I N M C M E Z L T V Y

K R X J E P L U C K M R I G F E Z J F M O T

A Z H Z Y G V I R V D U X C J F A N F E S G

I N Y S P Y N C H U V E Q R J T O F T S A R

C H K B E Z B U T S U C R L J A F Y B L S

L B Y V W O N D E J S Q F I L M E R J V U

V H C Y Z N E F C T O G K B M U R T L I S

G L S E T C L Y R T O C L H D I V S A Q M

S M A C K V Y C F L N O L B U V L B N I G

Y F L O N L C X O D I G F H R O B E T Z C

R H B Y B N H O X D L J U G H V D A N C D

A X V W Y

## Conclusion

I should hesitate to say that a cryptogram can l invented that will defy solution, provided it is of reasc able length and is not so involved and intricate as make its use inexpedient. For practical purposes cipher should be upon some system which can easily b committed to memory, and it should not involve an great expenditure of time in coding messages. Th cryptogram on page 190 has been ciphered in accordanc with these rules on what I believe to be a novel principle and will, I venture to think, require a great deal of pain and patience to solve. In the event of failure to solv the cipher, at a reasonable time after publication th method of ciphering and the solution may be obtainec from the Marconi International Code Co., Marconi House London, W.C. 2, or the Marconi International Code Corporation, 2236, Park Row Building, New York, or receipt of a stamped and addressed envelope.

PRINTED IN GREAT BRITAIN BY
BILLING AND SONS, LTD., GUILDFORD AND ESHER

UNIVERSITY OF CALIFORNIA LIBRARY
Los Angeles
This book is DUE on the last date stamped below.

DIS
AL
DISCH
OCT
RECD LD-URL
AUG 0 9 1988
REC
OCT 17

41584