THE

SIGNAL CORPS BULLETIN

▼

APRIL–JUNE 1940

WAR DEPARTMENT
OFFICE OF THE CHIEF SIGNAL OFFICER
WASHINGTON, D. C.

THE SIGNAL CORPS BULLETIN

APRIL–JUNE 1940

Published Quarterly by the Chief Signal Officer of the Army

CONTENTS

proofs against his retained copy of the draft. It is not infrequent that changes may have to be made in the galley proofs. The corrected galley proof is returned to the printer. A page proof is now prepared by the printer and process of the galley proof is again repeated. Finally after an appreciable time the technical regulation is printed, asssembled, and distributed by the Publications Division of The Adjutant General.

It must be borne in mind when the cry goes up—"Why can't we get these technical regulations in time to use with this new equipment? We're taking the stuff out on an Army maneuver next month, and no one knows how to use it!"—that a considerable period of time has elapsed from the inception to the final distribution of the technical regulation, no small part of which was consumed in the various departments of the War Department and Government Printing Office (which have many other prior tasks to perform). As a bynote, in many cases equipment is changed in production, in design and detail, to facilitate its manufacture by mass-production technique, or to take advantage of later improvements in theory or technical design, making the coincident issue of the technical regulation impossible.

While it is true that a technical regulation is rarely issued jointly with new types of equipment, particularly where field troubles, their diagnoses and repair are to be included in the publication, after its eventual distribution, it is of invaluable help thenceforward. In the training of large masses of recruits in the use of standard military equipment, especially during a mobilization, it may well be the only text available to the new officer. And when such time occurs, the technical regulation will have contributed its part to "effectiveness in war," which is the purpose of all military training.

A famous novelist turns
to cryptography

Jules Verne as Cryptographer

By Lt. Col. William F. Friedman, Signal Reserve

We may suppose, with some degree of assurance that Jules Verne, unlike Edgar Allan Poe, by no means regarded cryptography as one of the many fields of abstruse science in which he had attained proficiency or of which he claimed more than a layman's knowledge.[1]

[1] See an article by the present author, entitled "Edgar Allan Poe, Cryptographer," in American Literature, vol. VIII, No. 3, November 1936. This article was reprinted in the SCB No. 97 (July–Sept., 1937); an addendum thereto will be found in the SCB No. 98 (Oct.–Dec., 1937).

For Verne never assumes the air of omniscience to be found in some of Poe's more serious work, for example, in his article "A Few Words on Secret Writing." On the other hand it is undoubtedly true that Verne is indebted to Poe for certain of his devices, especially that in which the unraveling of a cryptogram forms a more or less vital element in the romance which he unfolds.

Three of Verne's stories forming the series known as Extraordinary Journeys, employ this device. They are, in chronological order, A Journey to the Center of the Earth (1864), The Giant Raft or 800 Leagues on the Amazon (1881), and Mathias Sandorf (1885). All three stories use different types of cryptograms. In only one of them does Verne attempt, in the character of one of his heroes, to solve the cryptogram by straightforward cryptanalytic methods, as Poe did in The Gold Bug, and it is with considerable regret that I find it necessary to say that in this one attempt he failed to do justice to his own ingenious mind. And, furthermore, the solutions which he obtains in the other two cases come very close to violating one of the tenets of the code of ethics imposed upon themselves in these days by all good detective story writers—never (to use a current idiom) "put over a fast one on the reader." That is, no "trick solution" is admissible.

1. THE CRYPTOGRAM IN A JOURNEY TO THE CENTER OF THE EARTH

In this romantic tale a German savant, Professor Lidenbrock, discovers in an Icelandic manuscript he has picked up in an old bookshop a piece of parchment on which appear "in transverse lines, cabalistic characters," and Verne, through the mouth of the professor's nephew, who is telling the story, says:

> Here is the exact facsimile of it. I insist upon presenting these singular characters, for they lead Professor Lidenbrock and his nephew to undertake the strangest expedition of the nineteenth century:

FIGURE 1.

The Professor looked for a few moments at this series of characters; then he said, raising his spectacles:

> "They are Runic characters; these type are absolutely identical with those of Snorre Turleson's manuscript! But—what can that signify?"

As the Runic seemed to me to be an invention of savants to mystify the poor world, I was not sorry to see that my uncle did not comprehend it at all. At least so it seemed to me, from the movement of his fingers, which commenced to tremble terribly.

"It is, however, old Icelandic!" he murmured between his teeth * * *.

Evidently a Runic inscription. "But there is a secret, and I will discover it—or else!" A violent gesture finished his thought.

"Put yourself there," he added, indicating the table with his fist, "and write."

I was ready in an instant.

"Now, I am going to dictate to you each letter of our alphabet corresponding to one of these Icelandic characters. We will see what that will give. But, by St. Michael, take good care that you don't make a mistake!"

The dictation commenced. I did my best; each letter was called one after the other, and formed the incomprehensible succession of the following words:[2]

mm.rnlls	esreuel	seecJde
sgtssmf	unteief	niedrke
kt,samn	atrateS	Saodrrn
emtnaeI	nuaect	rrilSa
Atvaar	.nscrc	ieaabs
ccdrmi	eeutul	frantu
dt,iac	oseibo	KediiI

When this work was finished, my uncle eagerly took up the sheet upon which I had just written, and attentively examined it for a long time.

"What does that mean?" he repeated mechanically.

Upon my word, I would not have been able to tell him. Besides, he did not question me for that purpose, and he continued to talk to himself, saying:

"That's what we call a cryptogram, in which the sense is concealed under letters purposely jumbled, and which properly arranged would form an intelligible sentence!"

Because the message on the parchment was written by one Arne Saknussemm, an Icelandic savant and celebrated alchemist of the seventeenth century, the professor concludes that the plain language of the cryptogram is Latin. His reasoning is quite clear, as can be noted in what follows.

* * * * * * *

"And first of all," said my uncle, "we must find the language of this 'cipher.' That ought not to be difficult."

At these words I quickly raised my head. My uncle continued his soliloquy as follows:

"Nothing is easier. There are in this document 132 letters, which give 79 consonants to 53 vowels. Now, it is nearly according to this proportion that the words of Southern languages are formed, whilst the idioms of the North are infinitely richer in consonants. A Southern language must then be in question.

"But what language is it?"

---

[2] The first two characters of the initial group are *m m*, to correspond with the symbol ⁑. This makes the first group contain 8 characters, whereas the other groups down to about halfway in the message regularly contain only 7 characters, and the rest of the groups, only 6. In some editions this first group is made to contain only 7 characters by dropping out one of the *m*'s. Verne evidently intended the double *m* to act as a single character.

That is what I expected of my savant, in whom I discovered, however, a profound analyst.

"This Saknussemm," he replied, "was a learned man; but as soon as he wrote in a language other than his mother tongue, he would choose by preference the language in vogue among the cultivated minds of the seventeenth century—I mean Latin. If I am mistaken, I can try Spanish, French, Italian, Greek, or Hebrew. But the savants of the seventeenth century generally wrote in Latin. I have then the right to say, *a priori*, that this is in Latin."

I jumped in my chair. My recollections of Latin revolted against the pretension that this succession of bizarre words could belong to the smooth language of Virgil.

"Yes! in Latin," continued my uncle, "but in jumbled Latin."

"So much the better!" I thought. "Uncle, if you unravel it you are sharp."

"Let us examine it carefully," he said, taking up again the sheet on which I had written. "Here is a series of 132 letters presented in an apparent disorder. There are words in which the consonants are met alone, like the first 'mrnlls',[3] others in which, on the contrary, the vowels abound, the fifth, for example, 'unteief,' or the next to the last, 'oseibo.' Now, this arrangement has evidently not been combined; it is determined *mathematically* by the unknown rule which governed the succession of these letters. It seems certain to me that the original sentence was written regularly, then turned about in accordance with the law which we must discover. Whoever possesses the key to this 'cipher' could read it fluently. But what is this key?"

* * * * * * *

The professor decides to try an experiment.

"Let us see," said he; "the first suggestion which would occur to one, for mixing up the letters of a sentence, it seems to me, is to write the words vertically instead of horizontally."

* * * * * * *

While making his great experiment, the eyes of Professor Lidenbrock flashed like lightning through his spectacles, his fingers trembled when he took up the old parchment again, he was very much affected. Finally, he coughed violently, and, in a grave tone, reading out successively the first and then the second letter, of each word, he dictated to me the following series:

mmessunkaSenrA.icefdoK.segnittamurtn
ecertserrette,rctaivsadua,ednecsedsadne
lacartniiiluJsiratracSarbmutabiledmek
meretarcsilucoYsleffenSnI

In finishing these letters, named one by one, which presented no sense to my mind, I was moved, I will confess; I then expected that the Professor would pompously roll out from his lips a sentence of most magnificent Latin.

But who could have forseen it? A violent blow from his fist shook the table. The ink jumped out of the stand, and my pen fell out of my hands.

"That's not it," cried my uncle. "That's not common sense!"

Then, shooting across the room like a cannon ball, and rushing down the staircase like an avalanche, he rushed into Konigstrasse, and fled with all his might.

* * * * * * *

[3] This should be *mmrnlls*, since Verne treats the double *m* as a single character.

The nephew then decides to try his own ingenuity on the parchment.

I endeavored to group these letters so as to form words. Impossible. By joining them by twos, threes, or fives or sixes, absolutely nothing intelligible was obtained; there were the fourteenth, fifteenth, and sixteenth[4] letters which formed the English word "ice," the eighty-fourth, the eighty-fifth, and the eighty-sixth formed the word "sir." Finally, in the body of the document, and on the third line, I observed the Latin words "rota," "mutabile," "ira," "nec," "atra."

"The deuce!" I thought, "these last words would seem to justify my uncle as to the language of the document." And also on the fourth line I perceive, besides, the word 'luco,' which is translated by 'sacred wood.' It is true that on the third we read the word 'tabiled,' of perfect Hebrew form, and on the last, the words 'mer,' 'arc,' which are purely French.

Here was something over which to lose one's head. Four different idioms in this absurd phrase! What relation could there exist between the words "ice, sir, anger, cruel, sacred wood, changing, mother, bow, or sea?" The first and the last alone readily go together; there was nothing astonishing that, in a document written in Iceland, a "sea of ice" should be spoken of. But to understand the rest of the cryptogram from that was another thing.

I debated then with myself against an insoluble difficulty; my brain became heated; my eyes were fixed upon the sheet of paper; the 132 letters seemed to jump around me like those silver drops which glide in the air around our heads when we have an attack of vertigo.

I was a prey to a sort of hallucination; I was stifled; I wanted air. Mechanically, I fanned myself with the sheet of paper, the two sides of which presented themselves successively to my gaze.

What was my surprise, when in one of these rapid movements, at the moment that the back of the sheet turned towards me, I thought I saw some perfectly legible words appear—Latin words, among others "craterem" and "terrestre"!

Suddenly, a light broke in upon my mind; from these few indications I saw the truth; I had discovered the law of the cipher. To read this document it was not even necessary to read it through the leaf reversed! No. Just as it was, just at it had been dictated to me, so it could be spelled out readily. All the ingenious combinations of the professor were realized; he was right as to the disposition of the letters, right as to the language of the document! There was a "something" needed to be able to read this Latin phrase from one end to the other, and this "something" chance had just given me!

The extent of my emotion may be understood! My eyes were affected. I could not make use of them. I had thrown the sheet of paper on the table. It was sufficient for me to cast one look at it to become possessor of the secret.

Finally I succeeded in calming my imagination. I compelled myself to walk around the room twice to quiet my nerves, and I returned to bury myself in the enormous armchair.

'Let us read," I cried to myself, after having filled my lungs with a fresh supply of air.

I leaned over the table; I placed my finger successively on each letter, and, without stopping, without hesitating a moment, I pronounced the entire sentence in a loud voice.

* * * * * * *

[4] The double *m* is counted as one character; the period is omitted in the count.

The professor returns but his nephew is reluctant to disclose the secret for fear he will have to accompany his uncle on a perilous journey. During the course of this wrestling with the problem Verne presents some calculations dealing with the chances of finding the solution by trying out all possible combinations. The nephew feels reassured that nothing will come of these experiments, for—

> I knew very well that if he succeeded in arranging these letters according to all the relative positions which they could occupy, the sentence would eventually be found. But I also knew that 20 letters alone can form two quintillion, four hundred and thirty-two quadrillion, nine hundred and two trillion, eight billion, one hundred and seventy-six million, six hundred and forty thousand combinations. Now there were 132 letters in the sentence which would give a number of different sentences composed of at least 133 figures—a number which is almost impossible to enumerate, and which is entirely beyond comprehension.
>
> I was reassured as to this heroic method of solving the problem.

And well he might be—for that is hardly the way in which a cryptanalyst would approach the matter!

Finally, the nephew acquaints the professor with his discovery and discloses the solution to the mystery of the cipher.

> "Ah! You ingenious Saknussemm!" he cried, "you first wrote your sentence reversed!"
>
> And rushing at the sheet of paper, his eye disturbed, his voice trembling with emotion, he read the whole document, going backward from the last letter to the first.
>
> It was composed as follows:
>
> In Sneffels Yoculis craterem kem delibat umbra Scartaris Julii intra calendas descende, audas viator, et terrestre centrum attinges. Kod feci. Arne Saknussemm.
>
> Which bad Latin may be thus translated:
>
> Descend, bold traveller, into the crater of the Yokul of Sneffels which the shadow of Scartaris caresses before the calends of July, and thou shalt reach the centre of the earth. Which I have done. Arne Saknussemm.

* * * * * * *

In analyzing the elements of Verne's solution of this cryptogram, the first thing noted is that Verne was obviously aware of the cryptographic aspects which the writing by means of runes assumes for the uninitiated. Indeed, characters very similar to them even today constitute a form of cipher writing frequently adopted by novices in the art of cryptography. The uninitiated believe that by the use of symbols which do not at all resemble the letters of our established orthography they have imparted an air of impenetrable mystery to their cryptograms. But Verne knows more than this: he tells us, indeed, a few interesting facts about the strange symbols. "They are Runic characters," he says through his mouthpiece, Professor Lidenbrock,

"Old Icelandic—evidently a Runic inscription." Then he proceeds to give for each character of the cabalistic writing the letter of our alphabet to which it corresponds. Now Verne does not concoct these equivalents out of his fertile imagination; he actually takes pains to be scientifically accurate in his work, for if the reader will consult any standard treatise on runes, which represent the oldest form of Germanic writing and which were used for purposes of writing throughout a vast area of northern Europe from the third to the fourteenth century, he will find that Verne is substantially correct in his assignment of letter values to the runic symbols. Incidentally, considering the carelessness of the authors and especially the publishers of romantic tales in which cryptograms play an important role, it is gratifying to find that Verne's runic inscription and his transliteration of it into characters is comparatively free from errors, for I have found but four of them in the whole cryptogram. That is, if one confirms the transliteration Verne gives of the runes into letters, one finds that in only four cases has he made an error in the rune—the letters themselves are entirely correct.

The professor realizes, as soon as he has transliterated the runes into letters, that the writing confronting him is a cryptogram. "That's what we call a cryptogram, in which the sense is concealed under letters purposely jumbled and which properly arranged would form an intelligible sentence." From the cryptanalytic point of view, it is to be noted that the reasoning here is a bit hasty, for until he has ascertained the type of cryptogram the professor has no warrant for saying that "the sense is concealed under letters purposely jumbled" and that if "properly arranged (they) would form an intelligible sentence." This description applies only to the primary class of ciphers designated as *transposition*, in which the letters of the plain text are all present but have merely been rearranged according to some scheme previously agreed upon between correspondents. The other primary class of ciphers is that designated as *substitution*, in which other letters, or characters, have been substituted for the letters of the original message. Had Verne merely mentioned that in a cipher in which the letters have only been shifted about the normal proportions of vowels and consonants as found in ordinary plain language still hold true, and that these normal proportions exist in the cryptogram, he would have given a technically adequate reason for saying that the "sense is concealed under the letters purposely jumbled." Incidentally, the first step that the professor took was one of substitution, for he replaced each rune by a letter of the alphabet, and, as we have noted above, the runes in this case serve merely as substitutive symbols for the letters of the underlying message.

When we come to Verne's analysis leading to the conclusion that the language of the cryptogram is that of a southern European land and specifically Latin, we find some excellent and valid reasoning. It is evident that Verne really knew a good deal about the proportions that normally exist between the vowels and consonants of various languages. However, just why Verne jumps to the conclusion that it is in "jumbled Latin" remains obscure. Certainly there is nothing to justify such an assumption at this stage in the analysis. Likewise obscure is the reasoning which follows this unwarranted conclusion. "Now, this arrangement has evidently not been combined;[5] it is determined *mathematically* by the unknown rule which governed the succession of these letters. It seems certain to me that the original sentence was written regularly, then turned about in accordance with a law which we must discover." It is too bad that Verne did not place this matter before that in which he sets forth the reason for concluding that the message is in Latin, for had he done so he would have been able to show how he reached the conclusion that the cryptogram is a transposition and not a substitution cipher, a step which logically precedes that of deducing that the cryptogram was written in Latin.

When the professor decides to experiment with various regular types of rearrangements of letters he is on firm ground, for it is only too true, as many a cryptanalyst will ruefully admit, that in transposition ciphers solution is often a matter of trial and error. (Most cryptanalysts detest them because their solution affords few opportunities for the use of the scientific tools he can apply in the case of substitution ciphers.) The first experiment the professor makes is a logical one. "Let us see," he says, "the first suggestion which would occur to one, for mixing the letters of a sentence, it seems to me, is to write the words vertically instead of horizontally." And since the text of the cryptogram is written in groups of six and seven characters, he decides to reverse the operation he conceives to have been performed originally and writes the 1st, 2d, . . . letter of each group successively. The result is what is shown on p. 73—still unintelligible text.

We may forgive Verne for his drama in causing the professor to fly from his study in chagrin, rage, and puzzlement. He could, of course, as readily have led the professor to the solution, just as he led the professor's nephew to it. In fact, it would have been easier—and it would not have looked, as it now does, like "pulling a rabbit out of a hat." Moreover, Verne made a slip in his explanation of how the professor's nephew stumbled upon the solution. For he has the nephew fanning

[5] The meaning of this first sentence is problematical, even in the French text. Perhaps Verne means that the arrangement is not the result of a combination, using the latter word in the same way as we do in referring to the "combination" to the lock on a vault door.

himself with the sheet of paper upon which the cryptogram had been transcribed as dictated by the professor, "when in one of these rapid movements, at the moment that the back of the sheet turned toward me, I thought I saw perfectly legible words appear—Latin words, among others 'craterem' and 'terrestre'!"

If the reader will try the experiment, writing the letters "meretarc" on a transparent piece of paper and viewing the writing from the back of the sheet he will see that far from causing the letters to become perfectly legible and disclosing the word "craterem," the writing when viewed from the back of the sheet upon which it is written becomes if anything more cabalistic in appearance than ever. Indeed, a very simple type of cipher writing is that called "mirror writing," which consists in forming the characters in such a manner as to make the writing unintelligible and mystifying—until it is held before a mirror. (Mirror-writing is a trick often practiced by children.)

Verne could just as easily have given the professor credit for a little more intelligence than he does when it comes to this last step in the interpretation of the cryptogram. After all, a man of the scholarship he attributes to the professor would surely have seen through this last and simplest phase of the disguise assumed by the message in cryptographic form, especially since he had enough intelligence to accomplish the first and much more difficult part of the solution, namely, the transcription of the original groups of letters into the final form shown. Casual inspection of "reversed writing" is all that is necessary to uncover the mystery.

It is noteworthy to add that Verne apparently had a weakness for this type of transposition, reversed writing, for two of the three cryptograms encountered in his stories involve this form of disguise.

2. THE CRYPTOGRAM IN MATHIAS SANDORF

In this tale Verne introduces a cryptogram which has been enciphered by means of a very old cryptographic device termed a "rotating grille." This consists of a small square sheet of thin metal or cardboard divided up into smaller squares, in some of which apertures have been cut at definite locations. An example of a grille is shown in figure 2. This is a grille with 6 squares per side, making an area of 36 small squares. Nine of these small squares have been cut out, so that they present openings or apertures through which letters may be written on an underlying surface. If this grille is superimposed upon a piece of cross-section paper the cells of which are identical in their dimensions with those of the apertures of the grille, these apertures will disclose 9 cells of the underlying cross-section paper and in these cells the first 9 letters of the message to be conveyed may be written. If the grille is then turned 90° and again placed over the

cross-section paper at exactly the same spot, 9 more cells will be disclosed by the apertures in the grille and 9 more letters of the message may be written in those cells. Twice more the grille may be turned and the same procedure executed, whereupon every one of the 36 cells of the underlying cross-section paper will have been disclosed and each of these 36 cells will be occupied by a letter. When the grille is removed, there will be 36 letters in a disarranged sequence on the piece of underlying cross-section paper. These letters may now be transcribed in groups or in an unbroken sequence, taking them in the normal order (left to right and top to bottom) from the square. All the original letters of the message are there, in unchanged form, but because their original order has been changed they will be unintelligible, that is, we will have produced a cryptogram. If the

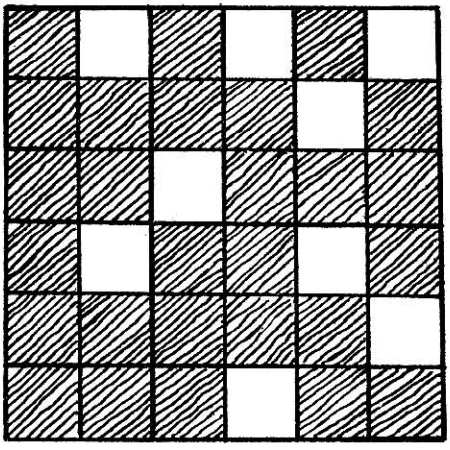


FIGURE 2.

message is longer than 36 letters, another 6 by 6 area of the cross-section paper is treated the same way, with the same grille, making another cipher square of 36 letters. Thus, a long message would be enciphered in successive sets of 36 letters until completed.

In case there are not enough letters to fill up the last square of 36 letters, meaningless or null letters are used to complete the square. A person not having the grille will be unable to read such a message—so the theory runs. The recipient of such a cryptogram, having an identical grille, writes out the cryptogram on a 6 by 6 piece of cross-section paper in the normal order of writing, and applies the grille to the 36 letter squares in the same fashion. But he takes the letters out of the squares in the order disclosed by the apertures in the grille, turning the latter in the same direction as it was turned in encipherment, the direction being previously agreed upon between the correspondents.

Now the solution of a cryptogram prepared by means of an unknown grille is by no means a simple matter, but it can be done. Verne was perhaps aware that a solution is possible, but he did not try it in Mathias Sandorf, and I am quite sure that he was technically on the right side in not trying, for the exposition would be much beyond the understanding of the casual reader of romantic detective stories.

However, let us see how Verne got around the problem he set for himself when he introduced this sort of cryptogram in Mathias Sandorf. A few brief extracts from the story are necessary.

"A message?" exclaimed Sarcany. "Wait, Zirone! This warrants a reprieve!" He stopped the hand of his companion as it was about to close on the neck of the carrier pigeon. Then taking the small bag which was attached to its wing he opened it and withdrew a message written in cipher language.

The message contained only 18 words, disposed in three vertical columns, as follows:

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

There was neither a point of origin nor a point of destination indicated on the message. Would it be possible to understand the meaning of these 18 words, without knowing the cipher?

* * * * * * *

"From a careful examination of this dispatch," said Sarcany, "it is clear to me that the key is based neither upon a number nor upon a conventional alphabet which would assign to each of the letters a significance other than its true one. Yes, in this message an *s* is an *s*, a *p* is a *p*, but the letters have been arranged in an order which can only be reconstructed by means of a grille!"

"Perhaps," said Toronthal, "but without the grille it is impossible to reconstruct the message."

* * * * * * *

In the fourth drawer which Sarcany examined, among some papers he had not encountered before he found a sort of a card irregularly perforated. This card attracted his attention immediately. "The grille!" he said.

He was not mistaken.

This grille was a simple cardboard square, 6 centimeters long on each side and divided into 36 equal squares, each measuring about a centimeter. In the 36 squares disposed in 6 horiontal and vertical lines, as in a Pythagorean table which has been based upon 6 numbers, 27 were filled and 9 were empty; that is, in place of the 9 squares the card was perforated and open in 9 apertures.

One could establish first of all that the 6 first words of the message, composed of 36 letters, had been successively obtained from the 36 squares.

In effect the disposition of the openings was so ingeniously combined in the mechanism of this grille that by making four turns of a quarter turn each (Verne really means three turns after the first placement of the grille), the perforated squares would successively occupy the positions of the unperforated squares without duplication at any place.

* * * * * * *

Sarcany wrote on a blank sheet the letters of the 6 first words. This give the following series:

i h n a l z
a r n u r o
o d x h n p
a e e e i l
s p e s d r
e e d g n c

Then the grille was applied on this set of letters in such a manner that the side marked by a small cross was placed at the top. And then the 9 perforated cells disclosed the 9 following letters while the other 27 remained hidden by the unperforated cells of the cardboard:

h a z r x e i r g

Sarcany then made a quarter of a turn with the grille from left to right in such a manner that the upper side now became the right. In this second application there were the following letters which appeared through the openings:

n o h a l e d e c

In the third and fourth applications the visible letters were the following, the writing of which was observed with care:

n a d n e p e d n
i l r u o p e s s

which signified absolutely nothing. "Let us continue," exclaimed Sarcany. He commenced experimenting on the 6 words forming the second column of the message. Four times he applied the grille on the words, each time making a quarter of a turn. He obtained only the following series of letters, absolutely devoid of meaning:

a m n e t n o r e
v e l e s s u o t
e t s e i r t e d
z e r r e v n e s

And here are the words which were given by the last 4 applications of the grille:

u o n s u o v e u
q l a n g i s r e
i m e r p u a t e
r p t s e t u o t

"Well," exclaimed Sarcany, "what are we going to make of this indecipherable logogriph!"

"Now write all the words one after the other," replied the banker very simply, "and then what? Let us see."

Sarcany obeyed and obtained the following sequence of letters:

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

No sooner had these letters been written when Silas Toronthal wrested the paper from Sarcany's hands, read it and gave vent to a cry, "Don't you see?" he exclaimed, "that before composing the words by means of the grille the correspondents of Count Sandorf had previously written the sentence they had drawn up, backwards!" Sarcany took the paper and here is what he read, going from the last letter to the first:

"Tout est prêt. Au premier signal que vous nous enverrex de Trieste, tous se lèveront en masse pour l'indépendance de la Hongrie. Xrzah."

"And the last 5 letters?" he cried.

"A conventional signature," replied Silas Toronthal.

* * * * * * *

Now Verne does not show the grille which was used in preparing the crytogram, yet a criticism of the cryptographic features of the story involves an attempt to reconstruct the grille from the solution Verne gives. I confess that as I was about to embark upon this experiment I was a prey to certain fears—I was not sure that the cryptogram had been prepared by means of a grille, for it would have been just as easy for Verne to set down the letters of the original cryptogram in some purely random fashion and then merely bring up the letters in their proper order. But it was indeed gratifying to find that the cryptogram is really authentic insofar as its having been prepared by means of a grille is concerned. For the grille shown in fig. 2 is identical with the one Verne used and the sceptical reader may verify the decipherment if he so desires. He will find that every letter which Verne gives as coming successively from each placement of the grille upon the 36-letter squares is correct, and that the entire decipherment, from beginning to end, is correct in every particular.

Of course, Verne might have refrained from including the additional step involving the writing of the original plain text backwards and then inscribing the letters on a checkerboard through the apertures of a grille. The grille alone would have been quite sufficient for the average reader!

There is only one more point which calls for comment. It concerns the reasoning by means of which Verne has Sarcany arrive at the definite conclusion that a grille was employed in enciphering the cryptogram. To have Sarcany say that "in the message an *s* is an *s*, a *p* is a *p*, but the letters have been rearranged," would really have been valid reasoning only after at least some attempt to demonstrate how he arrives at even this conclusion. He should, of course, have noted that the proportions of vowels, high-frequency and low-frequency consonants in the cryptograms conform to the proportions found in intelligible French, and therefore it is highly probable than an *s* is an *s*, a *p* is a *p*. But since the letters do not form intelligible sequences, therefore the original letters must have been rearranged so as to destroy the intelligence conveyed by them.

From this point in the reasoning to that wherein Verne has Sarcany reach the conclusion that "the letters have been disposed in a sequence which can only be reconstructed by means of a grille" is quite a jump. An unwarranted elision in logical thought was made by Verne. He could, of course, have remedied this deficiency in exposition had he called attention to the fact that the original cryptogram came in blocks of 36 letters—and 36 is a perfect square. For it is one of the characteristics of grille encipherment that when the sides of the grille are of even dimensions, such as 4 by 4, 6 by 6, 8 by 8, etc., the "capacity" of the grille, that is, the total number of letters that can be enciphered by the four positions the grille may assume, is always a perfect square. When the sides of the grille are of odd dimensions, such as 5 by 5, 7 by 7, 9 by 9, etc., the capacity of the grille is always 1 less than a perfect square. In the case of the cryptogram in Mathias Sandorf, since the 3 blocks of letters contain 36 letters each, there are some grounds for assuming that a revolving grille 6 by 6 was used. Note that I merely say that there are some grounds for assuming that this is the case, for there are literally hundreds of methods of transposition which could be employed, other than that involving the use of a grille, and which might produce blocks of 36 letters. Indeed, there is nothing in the story as it stands to warrant the hypothesis that the arrangement in blocks of 36 letters is anything more than purely an arbitrary selection from among scores of methods of writing out the letters of a cryptogram after a transposition has been effected. However, it is true that the arrangement in groups of 6 letters and in sets of 6 lines, making blocks of 36 letters is today not a usual practice, for 5-letter, not 6-letter groupings are standard today. In Verne's day, however, this practice was just coming into usage and we may readily overlook this small defect in his reasoning. I have by no means made an exhaustive survey of the various types of cryptograms the authors of romances and detective tales have employed, but of the many authors examined Verne is the only one who has employed the interesting device of a grille.

Incidentally, Toronthal's (that is, Verne's) conclusion that the last 5 letters which do not make any sense constitute a conventional signature is unwarranted. For these letters are merely nulls or nonsignificants, necessary to make a complete set of 36 letters in the third section of the message. Indeed, one could readily surmise that since Verne fails to give a plausible explanation of these 5 final letters, he really did not know or understand their function. The evidence might point to the surmise that Verne had aid from some friend who was a cryptographer in the preparation of the grille and the cryptogram. This would hardly be a source of astonishment, for the method of preparing a grille of the sort here involved, while a simple matter, is

known to only a very few persons, and even among cryptographers this knowledge is perhaps not common. Further, it is a matter of record that Verne consulted technical experts in various fields and utilized the information they gave him in the interest of accuracy.

3. THE CRYPTOGRAM IN THE GIANT RAFT, OR EIGHT HUNDRED LEAGUES ON THE AMAZON. (FRENCH TITLE: LA JAGANDA)

Although chronologically this tale is the second in which Verne introduces a cryptogram into his work and attempts to weave an account of methods for solution into his story, I have left the cryptogram involved in The Giant Raft to be discussed last for several reasons. First, Verne devotes much more time, thought, and space to its elucidation than he does to the solution of the cryptograms in the two preceding tales. Secondly, the cryptogram in this case is of much more importance as an example of a practical method of secret writing than is either the cryptogram in A Journey to the Center of the Earth or that in Mathias Sandorf. Thirdly, because Verne's novels achieved astonishing success and enjoyed very wide popularity, the type of cryptogram Verne adopted in The Giant Raft became quite well known among laymen and is even sometimes referred to in cryptographic literature as "The Jules Verne Cipher"—although Verne did not "invent" it nor, to be perfectly fair, did he make the slightest pretense at being its inventor. Fourthly, the solution of a cryptogram of this type, that is, its translation without the "key," was, at the time Verne wrote, deemed probably by all laymen and certainly by a few who possessed reputations as cryptographers to be an impossibility. Certainly Verne believed the solution to be impossible; yet he not only undertook to achieve an answer to the enigma without introducing any "tricks" but, what is more, he actually did achieve a solution by having recourse to a method which is perfectly legitimate so far as the professional cryptanalyst is concerned but which strangely enough may be regarded as a "trick solution," by many laymen. This may on first consideration be thought by the reader to redound to Verne's credit, and so it does, as a weaver of interesting romances, but unfortunately it does not redound to his credit as an ingenious thinker, or even as an amateur scientist. For had he really devoted some study to the matter, and had he not accepted blindly the common but erroneous notion that this type of cipher is indecipherable without the key, he might possibly have arrived at the straightforward and really simple method of solution which was devised many years before his time and which is still applicable today.

The hero in The Giant Raft, Joam Dacosta, alias Joam Garral, stands falsely accused of having committed murder. He can only

be exonerated and his life saved by solving a cryptogram the key to which was unknown to him or to any of his friends. A certain Judge Jarriquez, before whom Dacosta must establish his innocence, undertakes to solve the cryptogram, the secret of which must be "miraculously divined or revealed" before the end of 8 days. By the time that Jarriquez gets around to trying to solve the cryptogram 4 or 5 days have already gone by, leaving the feat to be accomplished in but 3 days. Verne devotes three entire chapters and parts of two more to the elucidation of the cipher, and in a rather painstaking manner goes into the matter with considerable detail, no doubt in an attempt to interest the reader in the abstruse science of cryptography, just as Poe did in The Gold Bug. But Poe used as his vehicle practically the simplest type of cipher known, that designated technically as monoalphabetic substitution, whereas Verne uses as his vehicle a much more complicated method designated technically as polyalphabetic substitution, or, as the French have it, "substitution by double key." In monoalphabetic substitution, each different letter of the original or intelligible text is replaced by some other character, which is always the same for that letter. Hence in the cryptogram every symbol always represents the same letter in the plain text and conversely, no letter in the plain text has more than one representative in the cipher. But in polyalphabetic substitution this invariant relationship between a plain-text letter and its cipher equivalent no longer holds true: letters which are the same in the plain text may have different equivalents in the cipher text depending upon their position in the text with respect to a key. This key, it is true, may be repeated many times in the course of enciphering the message but if it is unknown it produces varying and (to the uninitiated) quite mystifying results.

In appraising Verne's attempts at unraveling a cryptogram of this sort it will be best to begin by giving an example to show the mechanics of the method, which incidentally is very old.[6]

Let us suppose that the following message is to be enciphered: DACOSTA WAS MY ENEMY BUT HE IS INNOCENT OF THE MURDER. THE PROOF IS IN MY HANDS. A key consisting of a series of digits is agreed upon between the correspondents, say 46548973. This key means merely that the successive letters of the message to be enciphered will be replaced by those standing 4, 6, 5, * * *, places beyond them in the ordinary alphabet. Since the key consists of but eight digits in this case, and

[6] In cryptographic literature this method is attributed in Schott's Magia universalis (Nuremberg, 1659) to a Count Gronsfeld, with whom Schott had made a journey from Mayence to Francfort.

the message contains 62 letters, the key is repeated as many times as may be necessary to encipher the entire message. Thus:

```
Message...DACOSTA  WAS  MY  ENEMY  BUT  HE  IS  INNOCENT  OF  THE
Key.......4654897  346  54  89734  654  89  73  46548973  46  548
Cipher....HGHSACH  ZEY  RC  MWLPC  HZX  PN  PV  MTSSKNUW  SL  YLM
Message...MURDER  THE  PROOF  IS  IN  MY  HANDS
Key.......973465  489  73465  48  97  34  65489
Cipher....VBUHKW  XPN  WUSUK  MA  RU  PC  NFRLB
```

The cipher letters are then written out either in an unbroken series of letters (as is the case in Verne's story) or in regular groups (in these days, five letters per group), so as not to disclose the length of the key.

To the reader who is perhaps acquainted only with the most simple types of ciphers this method of cryptography may well appear to be inscrutable without possession of the key, which in this case is a series of 8 digits selected at random. He reasons somewhat as follows: Since there are 10 digits to choose from and repetitions are permissible, such a key of 8 digits may be any one of 10^8 or 100,000,000 different permutations, only one of which will serve to decipher the cryptogram. The chances of guessing the right key is obviously only one in a hundred million—too small to be of practical importance. Moreover, he reasons, if you should try to solve the cryptogram by the well-known principles of frequency, you can't get very far. For note how one and the same letter in the plain text is represented by different letters in the cipher. For example, E, which occurs seven times is represented by M (twice), L, N (three times), and K; N, which occurs six times, is represented by W, T, S, U (twice), and R. On the other hand, look at the cipher letter H; it occurs five times and it stands for the letters D (twice), C, A, and B. How in the name of commen sense could anyone not in possession of the key straighten out such inconsistencies and irregularities by any principles of frequency, which in their very nature require some modicum of consistency to mean anything?

This is the sort of reasoning that Verne himself employs, as may be noted in the following extracts, which not only are interesting in themselves but also are quite essential to a criticism of his accomplishments as a cryptographer.

The cryptogram in The Giant Raft was, says Verne, a document

"written in a disguised form in one of the numerous systems used in cryptography. But in which of them? To discover this would require all the ingenuity of which the human brain was capable. [It] contained a hundred lines, which were divided into half a dozen paragraphs."

"Hum" said the judge, after a little reflection; to try every paragraph, one after the other, would be to lose precious time, and be of no use. I had better select one of these paragraphs, and take the one which is likely to prove the most interesting. Which of them would do this better than the last, where the

recital of the whole affair is probably summed up? Proper names might put me on the track, amongst others that of Joam Dacosta; and if he has anything to do with this document, his name will evidently not be absent from its concluding paragraph."

Here follows the last paragraph of the document.

Phyjslyddqfdzxgasgzzqqehxgkfndrxujugiocytdxvksbxhhuypohdvyrymhuh puydkjoxphetozsletnpmvffovpdpajxhyynojyggaymeqynfuqlnmvlyfgsuzmq iztlbqgyugsqeubvnreredgruzblrmxyuhqhpzdrrgcrohepqxufivvrplphonth vddqfhqsntzhhhnfepmqkyuuexktogzgkyuumfvijdqdpzjqsykrplxhxqrymvkl ohhhotozvdksppsuvjhd.

At the outset, Judge Jarriquez noticed that the lines of the document were not divided either into words or phrases, and that there was a complete absence of punctuation. This fact could but render the reading of the document more difficult.

"Let us see, however," he said, "if there is not some assemblage of the letters which appears to form a word—I mean a pronounceable word, whose number of consonants is in proportion to its vowels. And at the beginning I see the word *phy;* farther on the word *gas.* Hallo! *ujugi.* Does that mean the African town on the banks of Tanganyika? What has that got to do with all this? Farther on here is the word *ypo.* Is it *Greek,* then? Close by here is *rym* and *puy,* and *jox,* and *phetoz,* and *jyggay,* and *mv,* and *qruz.* And before that we have got *red* and *let.* That is good! those are two English words. Then *ohe—syk;* then *rym* once more, and then the word *oto.*"

Judge Jarriquez let the paper drop, and thought for a few minutes.

"All the words I see in this thing seem queer!" he said. "In fact, there is nothing to give a clue to their origin. Some look like Greek, some like Dutch; some have an English twist, and some look like nothing at all! To say nothing of these series of consonants which are not wanted in any human pronunciation. Most assuredly it will not be very easy to find the key to this cryptogram."

The magistrate's fingers commenced to beat a tattoo on his desk—a kind of reveille to arouse his dormant faculties.

"Let us see," he said, "how many letters there are in the paragraph."

He counted them, pen in hand.

"Two hundred and seventy-six!" he said. "Well, now let us try what proportion these different letters bear to each other."

This occupied him for some time. The judge took up the document, and, with his pen in his hand, he noted each letter in alphabetical order.

In a quarter of an hour he had obtained the following table:

a= 3	f=10	k= 9	p=16	u=17
b= 4	g=13	l= 9	q=16	v=13
c= 3	h=23	m= 9	r=12	x=12
d=16	i= 4	n= 9	s=10	y=19
e= 9	j= 8	o=12	t= 8	z=12

Total 276

"Ah, hah!" he exclaimed. "One thing strikes me at once, and that is that in this paragraph all the letters of the alphabet are used. That is very strange. If we take up a book and open it by chance it will be very seldom that we shall hit upon two hundred and seventy-six letters with all the signs of the alphabet figuring amongst them. After all, it may be chance," and then he

passed to a different train of thought. "One important point is to see if the vowels and consonants are in their normal proportion."

And so he seized his pen, counted up the vowels, and obtained the following result:

a= 3
e= 9
i= 4
o=12
u=17
y=19

Total---------- 64 vowels

"And thus there are in this paragraph, after we have done our subtraction, 64 vowels and 212 consonants. Good! that is the normal proportion. That is about a fifth, as in the alphabet, where there are six vowels, amongst 25 letters. It is possible, therefore, that the document is written in the language of our country, that is, in Portuguese, but that only the signification of each letter is changed. If it has been modified in regular order, and a *b* is always represented by an *l*, an *o* by a *v*, a *g* by a *k*, a *u* by an *r*, etc., I will give up my judgeship if I do not read it. What can I do better than follow the method of that great analytical genius, Edgar Allan Poe?"

Verne has committed a rather serious error here. It is true that 6 vowels correspond, in an alphabet of 25 elements, to approximately a fifth of the number of letters—a proportion that is true not only of Portuguese but also of French, German, Spanish, English, and in fact of practically all alphabetic languages. Verne was warranted in drawing no conclusions from this fact, least of all that "only the signification of each letter is changed." However, he soon gets on the right track again when he devotes several paragraphs to an explanation of how Poe, in The Gold Bug, solved the cryptogram involved in that "masterpiece,"—this is Verne's own characterization of Poe's great tale. Of course, he brings out quite clearly the basis for Poe's analysis, which is that of frequency.

"What did Edgar Poe do?" he repeated. "First of all he began by finding out the sign—here there are only letters, let us say the letter—which recurred the oftenest. I see that that is *h*, for it is met with twenty-three times. This enormous proportion shows, to begin with, that *h* does not stand for *h*, but, on the contrary, that it represents the letter which recurs most frequently in our language, for I suppose the document is written in Portuguese. In English or French it would certainly be *e*, in Italian it would be *i* or *a*, in Portuguese it will be *a* or *o*. Now let us say that *h* signifies *a* or *o*."

After this was done, the judge found out the letter which recurred most frequently after *h*, and so on, and he formed the following table:

h =23 times
y =19 times
u =17 times
d, p, q =16 times
g, v =13 times
o, r, x, z =12 times

f, s	=10 times
e, k, l, m, n	= 9 times
j, t	= 8 times
b, i	= 4 times
a, c	= 3 times

"Now the letter *a* occurs thrice!" exclaimed the judge, "and it ought to occur the oftenest. Ah! that clearly proves that the meaning has been changed. And now, after *a* or *o*, what are the letters which figure oftenest in our language? Let us see," and Judge Jarriquez, with truly remarkable sagacity, which denoted a very observant mind, started on this new quest. In this he was only imitating the American romancer, who, great analyst as he was, had, by simple induction, been able to reconstruct an alphabet corresponding to the signs of the cryptogram and by means of it to eventually read the pirate's parchment note with ease.

The magistrate set to work in the same way, and we may affirm that he was no whit inferior to his illustrious master. Thanks to his previous work with logogriphs and squares, rectangular arrangements, and other enigmas, which depend only on an arbitrary disposition of the letters, he was already pretty strong in such mental pastimes. On this occasion he sought to establish the order in which the letters were reproduced—vowels first, consonants afterwards.

After 3 hours' work, in which "he had only to apply successively the letters of his alphabet to those of the paragraph," the judge gives up in disgust. What he did was to assign to each cipher letter a plain-text value in strict accordance with the principles of frequency; that is, since *a* is the most frequently used letter in Portuguese, and *h* is the most frequently appearing letter in the cryptogram, ergo $h=a$. Likewise *y*, the next most frequent letter in the cryptogram, must be *o*, and so on. No wonder that Judge Jarriquez failed! Even had the cryptogram been of the very simple, monoalphabetic type, such procedure would hardly ever result in success. We may be inclined to be charitable and give Verne credit for knowing better than to have his man adhere so slavishly to what is well recognized as only a rather flexible generalization; we might say that he had the judge go through this futile procedure only for the sake of dramatic emphasis. But somehow I feel that Verne actually believed that had the cryptogram been of this simple type, solution must have come by the method indicated—a wholly erroneous notion. No wonder the Judge cries "Confound the thing!"

Next we listen to some dialogue between a young friend, Manoel, and Judge Jarriquez, after the former inquires as to what success has attended the latter's efforts. The judge tells Manoel that he has had no success, but that he is certain that the document is governed by the law of a number.

"Well, sir," answered Manoel, "cannot a document of that kind always be read?"

"Yes," said Jarriquez, "if a letter is invariably represented by the same letter; if an *a*, for example, is always a *p*, and a *p* is always an *x*; if not, it cannot."

"And in this document?"

"In this document the value of the letter changes with the arbitrarily selected number which necessitates it. So a *b*, which will in one place be represented by a *k*, will later on become a *z*, later on a *u*, or an *n*, or an *f*, or any other letter."

"And then?"

"And then, I am sorry to say, the cryptogram is indecipherable."

"Indecipherable!" exclaimed Manoel. "No, sir; we shall end by finding the key of the document on which the man's life depends."

Manoel had risen, a prey to the excitement he could not control; the reply he had received was too hopeless, and he refused to accept it for good.

At a gesture from the judge, however, he sat down again, and in a calmer voice asked, "And in the first place, sir, what makes you think that the basis of this document is a number, or, as you call it, a cipher?"

"Listen to me, young man," replied the judge, "and you will be forced to give in to the evidence."

The magistrate took the document and put it before the eyes of Manoel and showed him what he had done.

"I began," he said, "by treating this document in the proper way, that is to say, logically, leaving nothing to chance. I applied to it an alphabet based on the proportion the letters bear to one another which is usual in our language, and I sought to obtain the meaning by following the precepts of our immortal analyst, Edgar Poe. Well, what succeeded with him collapsed with me."

"Collapsed!" exclaimed Manoel.

"Yes, my dear young man, and I at once saw that success sought in that fashion was impossible. In truth, a stronger man than I might have been deceived."

"But I should like to understand," said Manoel, "and I do not."

"Take the document," continued Judge Jarriquez; "first look at the disposition of the letters, and read it through."

Manoel obeyed.

"Do you not see that the combination of several of the letters is very strange?" asked the magistrate.

"I do not see anything," said Manoel, after having for perhaps the hundredth time read through the document.

"Well! study the last paragraph! There you understand the sense of the whole is bound to be summed up. Do you see anything abnormal?"

"Nothing."

"There is, however, one thing which absolutely proves that the language is subject to the law of a number."

"And that is?"

"That is that you see three *h*'s coming together in two different places."

What Jarriquez said was correct, and it was of a nature to attract attention. The two hundred and fourth, two hundred and fifth, and two hundred and sixth letters of the paragraph, and the two hundred and fifty-eighth, two hundred and fifty-ninth, and two hundred and sixtieth letters of the paragraph were consecutive *h's*. At first this peculiarity had not struck the magistrate.

"And that proves?" asked Manoel, without divining the deduction that could be drawn from the combination.

"That simply proves that the basis of the document is a number. It shows *a priori* that each letter is modified by virtue of the digits of the number and according to the place which it occupies."

"And why?"

"Because in no language will you find words with three consecutive repetitions of the letter h." [7]

Manoel was struck with the argument; he thought about it, and, in short, had no reply to make.

"And had I made the observation sooner," continued the magistrate, "I might have spared myself a good deal of trouble and a headache which extends from my occiput to my sinciput."

"But, sir," asked Manoel, who felt the little hope vanishing on which he had hitherto rested, "what do you mean by a number?"

"Tell me a number."

"Any number you like."

"Give me an example and you will understand the explanation better."

Judge Jarriquez sat down at the table, took up a sheet of paper and a pencil, and said, "Now, Manoel, let us choose a sentence by chance, the first that comes; for instance—'Judge Jarriquez has an ingenious mind.'"

Then the judge proceeds to encipher this message with the key 234 exactly as we enciphered our example on page 86, with the longer key 46548973. The result he obtains is as follows:

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

The judge concludes his demonstration of the mechanics of the cipher thusly:

"Now you see that if you do not know the number 234 you will never be able to read the lines, and consequently if we do not know the number of the document, it remains undecipherable!

Then he demonstrates with his own example how if one can guess a word in the message one can recover the key, and indeed the demonstration is made with great clarity. But, amazingly, Verne discards this method as unutilizable unless the first digit of the key number should happen to be that which enciphers the very first letter of the word, the presence of which is assumed! This sort of reasoning does little credit to a man of Verne's intelligence. Let us examine the reasoning.

Judge Jarriquez says that he is convinced that the name Joam Dacosta will be found in the paragraph in cipher. He goes on:

"Well, if the lines had been divided into words, in trying the words one after the other—I mean the words composed of seven letters, as the name of Dacosta is—it would not have been impossible to evolve the number which is the key of the document."

"Will you explain to me how you ought to proceed to do that, sir?" asked Manoel, who probably caught a glimpse of one more hope.

"Nothing can be more simple," answered the judge. "Let us take, for example, one of the words in the sentence we have just written—my name, if

---

[7] The reasoning here is quite fallacious. Since the cryptogram is a substitution cipher, even if it were monoalphabetic, *h* could represent some letter other than *h* in the plain text. Suppose it represented an *l;* there are many words which end in double *l*, which might be followed by a word beginning in *l*, making three consecutive *l*'s, which would be represented by *hhh* in the cipher.

you like. It is represented in the cryptogram by this queer succession of letters, *ncuvktygc*. Well, arranging these letters in a column, one under the other, and then placing against them the letters of my name and deducting one from the other the numbers of their places in alphabetical order, I get the following result:

Between *n* and *j* we have 4 letters
Between *c* and *a* we have 2 letters
Between *u* and *r* we have 3 letters
Between *v* and *r* we have 4 letters
Between *k* and *i* we have 2 letters
Between *t* and *q* we have 3 letters
Between *y* and *u* we have 4 letters
Between *g* and *e* we have 2 letters
Between *c* and *z* we have 3 letters

"Now what is the column of digits made up of that we have got by this simple operation? Look here! 423, 423, 423, that is to say, of repetitions of the numbers 423, or 234, or 342."

"Yes, that is it!" answered Manoel.

"You understand, then, by this means, that in calculating the true letter from the false, instead of the false from the true, I have been able to discover the number with ease; and the number I was in search of is really the 234 which I took as the key of my cryptogram."

"Well, sir!" exclaimed Manoel, "if that is so, the name of Dacosta is in the last paragraph; and taking successively each letter of these lines for the first of the seven letters which compose his name, we ought to get—"

"That would be impossible," interrupted the judge, "except on one condition."

"What is that?"

"That the first digit of the number should happen to encipher the first letter of the word Dacosta, and I think you will agree with me that that is not probable."

Now I shall not unduly tax the reader's patience, I hope, but will merely call attention to the fact that "guessing a word"—the "probable-word method," as it is called technically—is a procedure which has been used successfully for at least a couple of centuries. Its mechanics are well known. If the assumed word is present it will yield, in the cipher system under consideration, either the whole key or a portion of it. In either case, the application of this key to other portions of the text will yield good plain text, provided only that the key is applied at the correct point in the cycles or periods into which the cipher may be divided. To make clear just what is meant, let us take the example which was enciphered on page 86, and let us assume that we did not know the plain text but imagine that it contains the words "The murder." If we assume that the message begins with these words, apply them to the cipher letters, and derive the key numbers which will produce H G H S A C H Z E from "The murder" we find the following:

```
If---------- H G H S A C H Z E
Equals------ T H E M U R D E R
The key is---14-25--3--6--11--4-21-13
```

Since the system is such that the key must be composed of single digits, it is obvious without further investigation that H G H S A C H Z E cannot be the cipher equivalent of "The murder." In fact, if we were making this sort of attempt at finding the key, we would be warranted in stopping with the very first letter, where T is enciphered by H, because the key for this encipherment would be 14, which is impossible since the enciphering key digit can in no case exceed 9. We would then shift the assumed words, "The murder," one space to the right in the cryptogram and try again. Thus:

If	H G H S A C H Z E Y
Equals	T H E M U R D E R
The key is	13 . . . . .

We stop with the very first encipherment, for the key number exceeds 9. Thus we would shift the assumed words step-by-step until the following point is reached:

If	Y L M V B U H K W
Equals	T H E M U R D E R
The key is	5–4–8–9–7–3–4–6–5

The reader will recognize that we have here the complete key, plus one digit of a second cycle of that key. Had the assumed phrase been longer, the reconstructed key sequence would continue on the second cycle, producing 5–4–8–9–7–3–4–6–5–4–8–9– . . . etc.

Now, of course, we know that the key in this case does not begin with 5–4–8; as a matter of fact it begins with 4–6–5. But since this key is repetitive in character as regards its application in the encipherment, it is not essential that we know what the initial digit in the actual key is, for if we merely apply the reconstructed key to the text at any correct point in the keying cycle, we shall obtain good plain text. Thus, if we take the key reconstructed by assuming that Y L M V B U H K W represents "The murder," *viz*, 5–4–8–9–7–3–4–6, and apply it to our illustrative message not at the very beginning, but at the third letter, we obtain intelligible text. Thus:

Cipher	H G H S A C H Z E Y R . . .
Key	5–4–8–9–7–3–4–6–5 . . .
Plain text	C O S T A W A S M . . .

It is only necessary that we recognize the fact that we have plain text here and divide up the letters properly. Thus: . . . costa was m . . . .

So Verne was decidedly in error when he said that the procedure of assuming the name Dacosta would work only if "the first digit of the key number should happen to encipher the first letter of the word Dacosta." If the assumed word is really there it makes no difference at all with which digit of the key its first letter is enciphered. In-

cidentally, it is very interesting to note, first, that the very example Verne uses in his attempt to prove that the key can be discovered by "guessing" a word in the cryptogram only if "the first digit of the number should happen to encipher the first letter" of the assumed word, disproves his qualifying condition. For reference to his example shows that the first letter of the name Jarriquez was not enciphered by the first digit of the key, and yet Verne found the correct key or a cyclic permutation of that key by this method. Secondly, it is interesting to note not only that the name Dacosta is really present in the cryptogram which Judge Jarriquez is attempting to solve, but also that the first letter of the name is really enciphered by the first digit of the key! In other words, the very event which the judge says is improbable actually occurred in the cryptogram.

To return once more to the main theme, let us continue with Verne's solution. Manoel suggests that "chance might give us this number."

"This number," exclaimed the magistrate—"this number? But how many digits is it composed of? Of two, or three, or four, or nine, or ten? Is it made up only of different digits, or of digits in different order many times repeated? Do you not know, young man, that with the ordinary ten digits, using all at a time, but without any repetition, you can make 3,268,800 different numbers,[8] and that if you use the same digit more than once in the number, these millions of combinations will be enormously increased? And do you now know that if we employ every one of the 525,600 minutes of which the year is composed to try at each of these numbers, it would take you six years, and that you would want three centuries if each operation took you an hour? No! You ask the impossible!"

After struggling with the matter one whole day fruitlessly, the judge resolves, however,

never to leave the document until he had discovered the cipher. He set to work at it in a fury. He ate no more, he slept no more! All his time was passed in inventing combinations of numbers, in forging a key to force this lock! * * * Suppressed frenzy consumed him, and kept him in a perpetual heat. His whole house trembled; his servants, black or white, dared not come near him * * *. Never had a problem so taken possession of this character, and he had thoroughly made up his mind to get at the solution even if his head exploded like an overheated boiler under the pressure of its steam. * * * It was perfectly clear to the mind of the worthy magistrate that the key to the document was a number, composed of two or more digits, but what this number was all investigation seemed powerless to discover.

The judge decides to try the probable-word method, but because Verne had no clear apprehension of the method this attempt was futile. Here is what the judge does:

"Ah!" he exclaimed, "why did not the scoundrel who wrote this separate the words in this paragraph? We might—we will try—but no! However, if

[8] In the edition I have, this number is as given, but it should be 3,628,000. It is the product of the series of numbers from 1 to 10, inclusive. If repetitions are permissible, the total number of permutations is 10^{10}, or 10,000,000,000.

there is anything here about the murder and the robbery, two or three words must be present—'arrayal,' 'diamond,' 'Tijuco,' 'Dacosta,' and others; and in putting down their cryptological equivalents the number could be arrived at. But there is nothing—not a single break!—not one word by itself! One word of 276 letters! I hope the wretch may be blessed 276 times for complicating his system in this way! He ought to be hanged 276 times!"

And a violent thump with his fist on the document emphasized this charitable wish.

"But," continued the magistrate, "if I cannot find one of the words in the body of the document, I might at least try my hand at the beginning and end of each paragraph. There may be a chance there that I ought not to miss."

And impressed with this idea Judge Jarriquez successively tried if the letters which commenced or finished the different paragraphs could be made to correspond with those which formed the most important word, which was sure to be found somewhere, that of *Dacosta*.

He could do nothing of the kind.

In fact, to take only the last paragraph with which he began, the formula was—

P=D
h=a
y=c
j=o
s=s
l=t
y=a

Now at the very first letter Jarriquez was stopped in his calculations, for the difference in alphabetical position between the *d* and the *p* gave him not one digit but two, namely, 12, and in this kind of cryptogram only one letter can take the place of another.[9]

It was the same for the seven last letters of the paragraph, *p s u v j h d*, of which the series also commences with a *p*, and which could in no case stand for the *d* in *Dacosta*, because these letters were in like manner twelve spaces apart.

So it was not his name that figured here.

The same observation applies to the words *arrayal* and *Tijuco*, which were successively tried, but whose construction did not correspond with the cryptographic series.

After he had got so far, Judge Jarriquez, with his head nearly splitting, arose and paced his office, went for fresh air to the window, and gave utterance to a growl, at the noise of which a flock of humming birds, murmuring amongst the foliage of a mimosa tree, betook themselves to flight. Then he returned to the document.

He picked it up and turned it over and over.

"The humbug! the rascal!" he hissed; "it will end by driving me mad! But steady! Be calm! Don't let our spirits go down! This is not the time!"

And then having refreshed himself by giving his head a thorough sluicing with cold water:

"Let us try another way," he said, "and as I cannot hit upon the number from the arrangement of the letters, let us see what number the author of the docu-

[9] What Verne means to say here is that one letter can take no more than a single digit for its key in encipherment.

ment would have chosen in confessing that he was the author of the crime at Tijuco."

This was another method for the magistrate to enter upon, and maybe he was right, for there was a certain amount of logic about it.

The judge then tries his hand at guessing the key number, assuming dates of various sorts—that of the birth of Dacosta, the year the crime was committed, etc.—but to no avail. "Nothing! All the time nothing!" Then comes an amusing episode highly suggestive of the procedure adopted at times by victims of the unsuppressible game of modern times known as the "numbers racket." Let Verne tell it himself:

Judge Jarriquez had worked himself into such a state of exasperation that there really was some fear that his mental faculties would lose their balance. He jumped about, and twisted about, and wrestled about as if he really had got hold of his enemy's body. Then suddenly he cried, "Now for chance! Heaven help me now, logic is powerless!"

His hand seized a bell pull hanging near his table. The bell rang furiously, and the magistrate strode up to the door, which he opened. "Bobo!" he shouted.

A moment or two elapsed.

Bobo was a freed negro, who was the privileged servant of Jarriquez. He did not appear; it was evident that Bobo was afraid to come into his master's room.

Another ring at the bell; another call to Bobo, who, for his own safety, pretended to be deaf on this occasion. And now a third ring at the bell, which unhitched the crank and broke the cord.

This time Bobo came up. "What is it, sir?" asked Bobo, prudently waiting on the threshold.

"Advance, without uttering a single word!" replied the judge, whose flaming eyes made the negro quake again.

Bobo advanced.

"Bobo," said Jarriquez, "attend to what I say, and answer immediately; do not even take time to think, or I——"

Bobo, with fixed eyes and open mouth, brought his feet together like a soldier and stood at attention.

"Are you ready?" asked his master.

"I am."

"Now, then, tell me, without a moment's thought—you understand—the first number that comes into your head."

"76223," answered Bobo, all in a breath. Bobo thought he would please his master by giving him a pretty large one!

Judge Jarriquez had run to the table, and, pencil in hand, had made out a formula with the number given by Bobo, and which Bobo had in this way only given him at a venture.

It is obvious that it was most unlikely that a number such as 76223 was the key of the document, and it produced no other result than to bring to the lips of Jarriquez such a vigorous ejaculation that Bobo disappeared like a shot!

Verne now interrupts the account of the judge's attempts at the solution of the cryptogram to tell of a plot hatched by Dacosta's relatives to bring about the escape of the prisoner—but the prisoner thwarts these plans by vehemently protesting his innocence and refusing to escape.

Finally, one Fragoso, a trusted servant of Dacosta who had undertaken to do some sleuthing in an attempt to clear his master's name and had gone on a journey into the interior, appears in the nick of time—on the morning of the day on which the condemned man was to be hung. He bursts into Judge Jarriquez's home.

"I come from the province where Torres pursued his calling as captain of the woods!" he gasped. "Mr. Judge, Torres told the truth. Stop—stop the execution!"

"You found the gang?"

"Yes."

"And you have brought me the key to the document?"

Fragoso did not reply.

"Come, leave me alone! leave me alone!" shouted Jarriquez, and, a prey to an outburst of rage, he grasped the document to tear it to atoms.

Fragoso seized his hands and stopped him. "The truth is there!" he said.

"I know," answered Jarriquez: "but it is a truth which will never see the light!"

"It will appear—it must! it must!"

"Once more, have you the cipher."

"No," replied Fragoso, "but, I repeat, Torres has not lied. One of his companions, with whom he was very intimate, died a few months ago, and there can be no doubt but that this man gave him the document he came to sell to Joam Dacosta."

"No," answered Jarriquez—"no, there is no doubt about it—as far as we are concerned; but that is not enough for those who dispose of the doomed man's life. Leave me!"

Fragoso, repulsed, would not quit the spot. Again he threw himself at the judge's feet. "Joam Dacosta is innocent!" he cried; "you will not leave him to die! It was not he who committed the crime of Tijuco, it was the comrade of Torres, the author of that document! It was Ortega!"

As he uttered the name the judge bounded backward. A kind of calm swiftly succeeded to the tempest which raged within him. He dropped the document from his clenched hand, smoothed it out on the table, sat down, and, passing his hand over his eyes. "That name?", he said, "Ortega? Let us see," and then he proceeded with the new name brought back by Fragoso as he had done with the other names so vainly tried by himself.

After placing it above the six first letters of the paragraph, he obtained the following formula:

O r t e g a
P h y j s l

"Nothing!" he said. "That gives us—nothing!"

And in fact the *h* placed under the *r* could not be expressed by a single digit, for, in alphabetical order[10] this letter occupies an earlier position to that of the *r*.

The *p*, the *y*, the *j*, arranged beneath the letters *o*, *t*, *e*, disclosed the cipher 1, 4, 5, but as for the *s* and the *l* at the end of the word, the interval which sepa-

[10] Verne here again refers to the condition that a keying number for a single letter must not be more than a single digit. The "earlier position" in alphabetical order has nothing to do with the matter, for a plain-text letter such as Y may be enciphered by a keying digit 5, for example, and will then be represented by D. The alphabet in such a cryptographic system is regarded as partaking of the nature of a closed circle of letters.

rated them from the *g* and the *a* was a dozen letters, and hence impossible to express by a single cipher, so that they corresponded to neither *g* nor *a*.

And here appalling shouts arose in the streets; they were the cries of despair.

Fragoso jumped to one of the windows, and opened it before the judge could hinder him.

The people filled the road. The hour had come at which the doomed man was to start from the prison, and the crowd was flowing back to the spot where the gallows had been erected.

Judge Jarriquez, quite frightful to look upon, devoured the lines of the document with a fixed stare.

"The last letters!" he muttered, "Let us try once more the last letters!"

It was the last hope.

And then, with a hand whose agitation nearly prevented him from writing at all, he placed the name of Ortega over the six last letters of the paragraph, as he had done over the first.

An exclamation immediately escaped him. He saw, at first glance, that the six last letters were inferior in alphabetical order to those which composed Ortega's name, and that consequently they might yield the number.

And when he reduced the formula, reckoning each later letter from the earlier letter of the word, he obtained

O r t e g a
4 3 2 5 1 3
S u v j h d

The number thus disclosed was 432513.

But was this number that which had been used in the document? Was it not as erroneous as those he had previously tried?

At this moment the shouts below redoubled—shouts of pity which betrayed the sympathy of the excited crowd. A few minutes more were all that the doomed man had to live!

Fragoso, maddened with grief, darted from the room! He wished to see, for the last time, his benefactor who was on his road to death! He longed to throw himself before the mournful procession and stop it, shouting, "Do not kill this just man! Do not kill him!"

But already Judge Jarriquez had placed the given number above the first letters of the paragraph, repeating them as often as was necessary, as follows:

4 3 2 5 1 3 4 3 2 5 1 3 4 3 2 5 1 3 4 3 2 5 1 3
P h y j s l y d d q f d z x g a s g z z q q e h

And then, reckoning the true letters according to their alphabetical order, he read:

Le véritable auteur du vol de—

A yell of delight escaped him! This number, 432513, was the number sought for so long! The name of Ortega had enabled him to discover it! At length he held the key of the document, which would incontestably prove the innocence of Joam Dacosta, and without reading any more he flew from his study into the street, shouting,

"Halt! Halt!"

To cleave the crowd, which opened as he ran, to dash to the prison, whence the convict was coming at the moment, with his wife and children clinging to him with the violence of despair, was but the work of a minute for Judge Jarriquez.

Stopping before Joam Dacosta, he could not speak for a second, and then these words escaped his lips:

"Innocent! Innocent!"

* * * * * * *

Judge Jarriquez sat down on a stone seat, and then, while Minha, Benito, Manoel, and Fragoso stood round him, while Joam Dacosta clasped Yaquita to his heart, he first unravelled the last paragraph of the document by means of the number, and as the words appeared by the substitution of the true letters for the cryptological ones, he divided and punctuated them, and then read it out in a loud voice. And this is what he read in the midst of profound silence:

```
Le véritable auteur du vol des diamants et de
43 251343251 343251 34 325 134 32513432 51 34
Py yjslyddqf dzxgas gz zqq ehx gkfndrxu ju gi

l'assassinat des soldats qui escortaient le convoi.
32513432513 432 5134325 134 32513432513 43 251343
ocytdxvksbx hhu ypohdvy rym huhpuydkjox ph etozsl

commis dans la nuit du vingt-deux janvier mil
251343 2513 43 2513 43 25134 3251 3432513 432
etnpmv ffov pd pajx hy ynojy ggay meqynfu qln

huit cent vingt-six, n'est donc pas Joam Dacosta,
5134 3251 34325 134   3251 3432 513 4325 1343251
mvly fgsu zmquz tlb   qgyu gsqe ubv nrcr edgruzb

injustement condamné àmort, c'est moi, le misérable
34325134325 13432513 43251   3432 513  43 251343251
lrmxyuhqhpz drrgcroh epqxu   fivv rpl  ph onthvddqf

employé de l'administration du district diamantin,
3432513 43  251343251343251 34 32513432 513432513
hqsntzh hh  nfepmqkyuuexkto gz gkyuumfv ijdqdpzjq

oui, moi seul, qui signe de mon vrai nom, Ortega.
432  513 4325  134 32513 43 251 3432 513  432513
syk  rpl xhxq  rym vkloh hh oto zvdk spp  suvjhd.
```

"The real author of the robbery of the diamonds and of the murder of the soldiers who escorted the convoy, committed during the night of the twenty-second of January, one thousand eight hundred and twenty-six, was thus not Joam Dacosta, unjustly condemned to death; it was I; the wretched servant of the Administration of the diamond district; yes, I alone, who sign this with my true name, Ortega."

And thus the curtain descends with the saving of the hero's life.

By means of the number Judge Jarriquez interpreted the whole cryptogram . . . The name Ortega had afforded the means of unravelling the cryptogram, thanks to the sagacity of Judge Jarriquez.

At another point in the story Verne says:

In any case, the situation of Joam Dacosta was most hazardous. If the document were not deciphered, it would be just the same as if it did not exist; and

if the secret of the cryptogram were not miraculously divined or revealed *before the end of the* 3 days,[11] the supreme sentence would inevitably be suffered by the doomed man of Tijuco. And this miracle a man attempted to perform!

* * * * * * *

The excitement increased in Manaos as the time ran on; the affair was discussed with unexampled acerbity. In the midst of this enthralment of public opinion, which evoked so much of the mysterious, the document was the principal object of conversation.

At the end of this fourth day not a single person doubted but that it contained the vindication of the doomed man. Every one had been given an opportunity of deciphering its incomprehensible contents, for the "Diario d'o Grand Para" had reproduced it in facsimile. Autograph copies were spread about in great numbers at the suggestion of Manoel, who neglected nothing that might lead to the penetration of the mystery—not even chance, that "nickname of Providence," as some one has called it.

In addition, a reward of 100 contos (or 300,000 francs) was promised to any one who could discover the cipher so fruitlessly sought after—and read the document. This was quite a fortune, and so people of all classes forgot to eat, drink, or sleep to attack this unintelligible cryptogram.

Up to the present, however, all had been useless, and probably the most ingenious analysts in the world would have spent their time in vain. It had been advertised that any solution should be sent, without delay, to Judge Jarriquez, to his house in God-the-Son Street; but the evening of the 29th of August came and none had arrived, nor was any likely to arrive.

We may be certain that Verne thought most highly of his achievement in solving the cryptogram, in the character of Judge Jarriquez. But quite devastating are the words of one commentator,[12] who has looked into the matter and says: "to a modern expert, however, the learned judge appears as a pompous and pedantic ass. Many of his musings and observations would sound shallow even to the most casual reader who took the trouble to follow him carefully." These are pretty strong words, and we shall not accept them without due examination. So let us see how a "modern expert" would proceed to solve a cryptogram of this type.

The solution of a cryptogram of this type, wherein a repeating key is employed, resolves itself into three steps. First, the length of the key must be ascertained; this gives the number of cipher alphabets involved. Second, the letters of the cryptogram must be distributed into individual frequency tables corresponding to the separate cipher alphabets involved. Third, these frequency distributions must be analyzed to find the equivalency between plain-text and cipher-text letters in each alphabet. These steps may sound some-

[11] It will be recalled that 4 or 5 days had elapsed between the time Dacosta was arraigned and the time Judge Jarriquez began his attempt to unravel the secret. Verne says: "Joam Dacosta had been arrested on the 24th of August and examined the next day. The judge's report was sent off on the 26th. It was now the 28th. In 3 or 4 days more the minister would have come to a decision regarding the convict, and it was only too certain that justice would take its course."

[12] Hooker, Charles W. R., *The Jules Verne Cipher*, The Police Journal (British), vol. IV, No. 3, January 1931, pp. 107–119.

what complicated and formidable to the reader who has no cryptographic experience, but I assure him that they are really quite simple. They are especially so in this case.

Let us consider the first step, that of finding the length of the key. There are various ways of doing this, but only one will be considered here. If the reader will study the example on page 86 attentively, he will see that despite the fact that a number of different alphabets was employed there are still some repetitions in the cryptogram, as shown below:

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

Here we have three repetitions: CHZ occurs twice, XPN occurs twice, PC occurs twice. Let us refer back to the encipherment of the example to see how these repeated groups happened to be brought about. The first CHZ represents the encipherment of TAW by key numbers 9–7–3; the second CHZ represents the encipherment of YBU by key numbers 4–6–5. The identity of the cipher letters in these two cases is a pure accident! It just happened as a result of chance that two different sets of plain-text letters enciphered by two different sets of key numbers gave exactly the same set of cipher letters. Repetitions of this sort are called accidental, because that is what they are. But now note the two groups XPN; the first XPN represents the encipherment of THE by key numbers 4–8–9, and the second XPN represents the encipherment of another THE by the same key numbers, 4–8–9. In this case, because the same plain-text sequence falls under the same key numbers twice, the cipher resultants had to be identical. Of course, if these two THE's had happened to fall under different key numbers, the cipher resultants would not have been identical—but then there might have been brought about some other repetition, for the repetition of single letters, pairs of letters, and sets of three, four, or more letters is an all-pervading phenomenon in practically every alphabetic language. Note how the repetition of the pair of letters PC is brought about: in the first case it represents the MY of ENEMY, in the second it represents the word MY, and of course, both MY's were enciphered by the same key numbers. Repetitions of this sort are called causal repetitions because they are brought about by a definite cause, viz, the encipherment of similar sequences by identical keying characters. In such cases the letters must be enciphered by the same cipher alphabets. Now if a message is long enough, in comparison with the length of the repeating key, there will be many such cases of causal repetitions—more than sufficient to overbalance the disturbing element of accidental repetitions, because,

as said before, repetition of sequences of letters in plain language is a characteristic of plain language.

Now if the reader will count the number of letters from the first appearance of XPN to, but not including, the second appearance of this same group, he will see that this number is 24, which is an exact multiple of the length of the key. Also, if the reader will do the same thing with respect to the PC repetition, he will find the number to be 40, which is also an exact multiple of the length of the key. In fact, in the first case the key has passed through three complete cycles between the two occurrences, and in the second case it has passed through five complete cycles. In the case of the CHZ repetition, however, the interval between the two occurrences bears no relation to the length of the key: since the repetition is accidental there can be no relationship. Now in a long message one merely lists the repetitions, finds the length of the intervals between similar repetitions, and sets down the factors of those intervals. That factor which is common to most of the repetitions usually corresponds to the length of the key. The longer the repetition the more weight is to be given to the factors of the interval between its two occurrences, because the less likely is it that such a repetition is of the accidental type. All of this business has been reduced to statistical language, so that in practice the cryptanalyst can estimate pretty closely what the probabilities are that a given repetition is an accident or has been causally produced.

Applying the foregoing procedure to the Verne cryptogram, first we find all the repetitions of two or more letters. This is purely a matter of clerical work and I will not trouble the reader to perform it. Here are all the repetitions of three or more letters in the cryptogram, together with the intervals between them and the factors of those intervals:

From 1st	D D Q F to 2d	D D Q F—186 letters.	Factors: 2, 3, 6, 31.
From 1st	K Y U U to 2d	K Y U U— 12 letters.	Factors: 2, 3, 4, 6.
From 1st	H H H to 2d	H H H— 54 letters.	Factors: 2, 3, 6, 9, 18, 27.
From 1st	R Y M to 2d	R Y M—192 letters.	Factors: 2, 3, 4, 6, 8, 12, 16, 24, 32, 48, 64, 96.
From 1st	R P L to 2d	R P L— 60 letters.	Factors: 2, 3, 4, 5, 6, 12, 15, 20, 30.
From 1st	T O Z to 2d	T O Z—186 letters.	Factors: 2, 3, 6, 31.

The only factor (other than 2 and 3, which are unlikely) which is common to all the intervals between these repetitions is 6, and we may take this to be the length of the key. Great weight may be placed upon the repetition D D Q F, which shows an interval of 186; the factors of this number are 2, 3, 6, and 31. The first two are unlikely and so is the last one, leaving 6 as almost certain.

The letters of the cryptogram are now transcribed into groups of 6 letters, to correspond with the length of the key, and individual frequency distributions for all six positions in these groups are compiled. They are as follows (note that the letter W does not occur in French):

PHYJSL	YDDQFD	ZXGASG	ZZQQEH	XGKFNX	RXUJUG
IOCYTD	XVKSBX	HHUYPO	HDVYRY	MHUHPU	YDKJOX
PHETOZ	SLETNP	MVFFOV	PDPAJX	HYYNOJ	YGGAYM
EQYNFU	QLNMVL	YFGSUZ	MQIZTL	EQGYUG	SQEUBV
NRCRED	GRUZBL	RMXYUH	QHPZDR	RGCROH	EPQXUF
IVVRPL	PHONTH	VDDQFH	QSNTZH	HHNFEP	MQKYUU
EXKTOG	ZGKYUU	MFVIJD	QDPZJQ	SYKRPL	XHXQRY
MVKLOH	HHOTOZ	VDKSPP	SUVJHD		

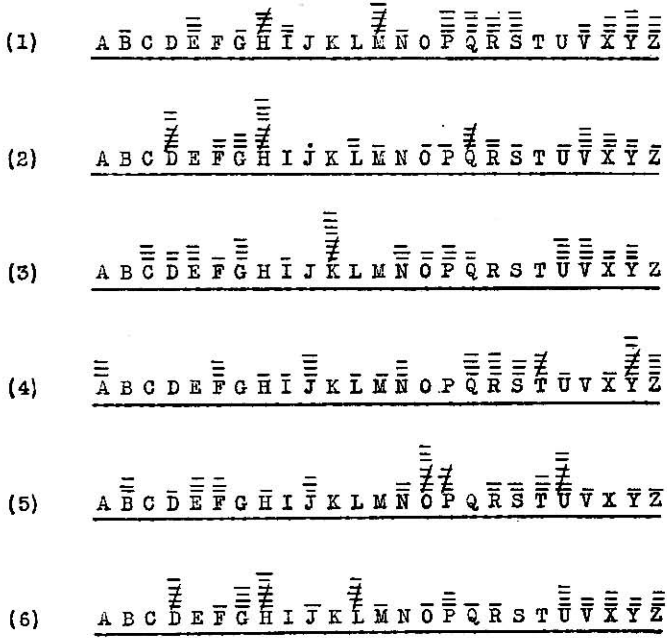
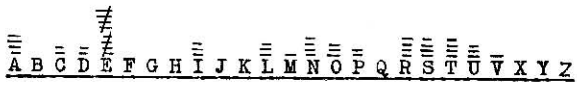


FIGURE 3.

Now in a cipher of this sort, where the digits of a key are added to numbers corresponding to the serial position of the plain-text letters in the ordinary aphabet, the effect is merely to shift all the letters enciphered by the same keying digit forward 1, 2, 3, . . . 9 letters

forward, in accordance with the keying digit. For example, in the case under consideration, the key has been found to consist of six digits and hence the cryptogram was transcribed in groups of six letters. The letters occupying position 1 in these groups have all been enciphered by the same keying digit. Suppose the latter were 3; then a D in position 1 in a cipher group would represent plain-text letter A, an E in position 1 would represent plain-text letter B, and so on. This effect can most readily be observed in the distribution labeled alphabet 2 in figure 3. Note the high frequency of D; if it represents A, then the keying digit to produce cipher D from plain-text A would have to be 3. Now how can we prove that 3 is correct? Well, it is easy enough: the high spots and low spots in alphabet 2 should all merely be shifted 3 spaces forward from the places where these high and low spots are normally found if the letters in this frequency distribution were plain-text letters. Now if one were to take 50 letters of ordinary French and distribute them under the normal French alphabet, they would theoretically form the following graph:



A comparison of this graph with alphabet 2 quickly tells us that if we will shift the latter three spaces to the left, the sequence of high and low spots will fall just where they should fall if the letters were plain-text letters. Thus:

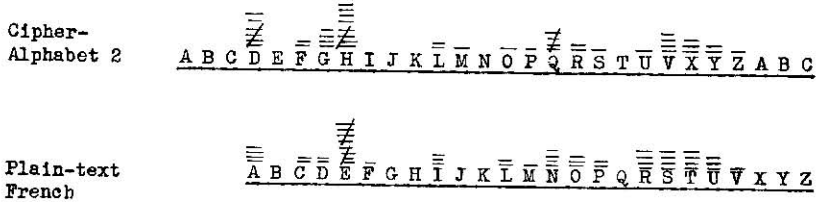


FIGURE 4.

Since we have been dealing with alphabet 2, this establishes the digit 3 as the second digit of the key, and the plain-text equivalents may be written under the letters of cipher alphabet 2. Thus:

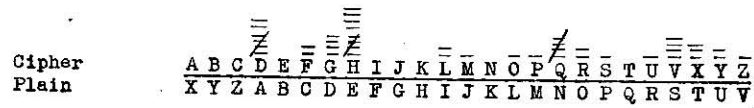


FIGURE 5.

This process is termed "fitting the cipher distribution to the normal." By proceeding in the same manner with all the other cipher

alphabets, we find that the best "fits" are obtained when the keying digits shown below are assumed:

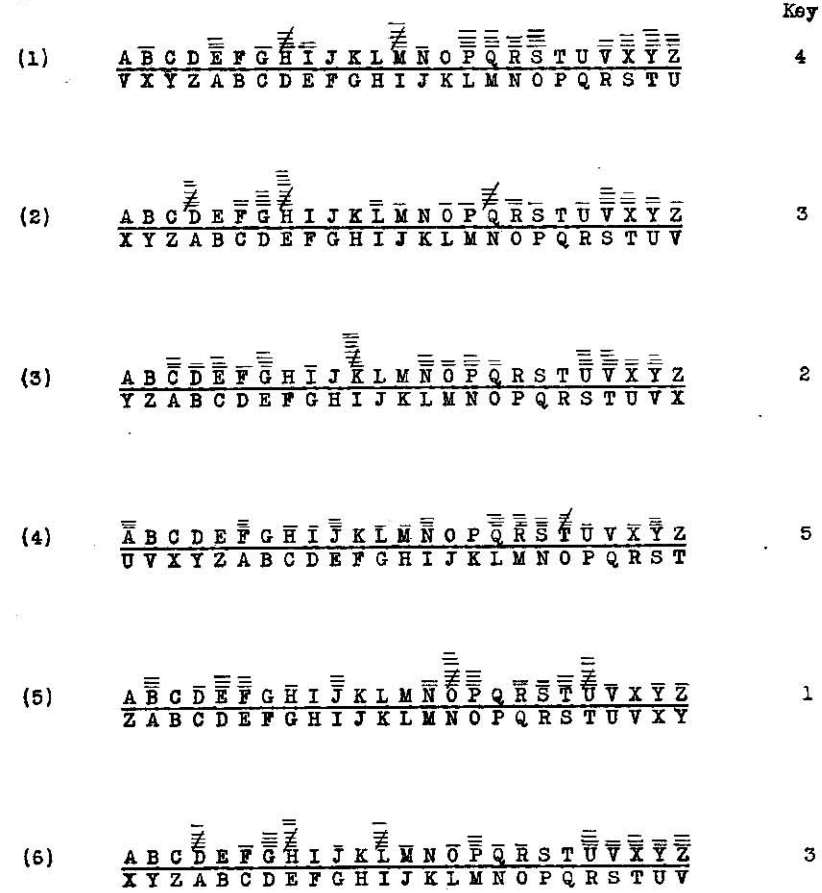


FIGURE 6.

The rest is now a mere matter of clerical work. Applying the key 4–3–2–5–1–3 to the first two or three cipher groups, we obtain plaintext immediately:

P H Y J S L Y D D Q F D Z X G A S G . . .
4 3 2 5 1 3 4 3 2 5 1 3 4 3 2 5 1 3 . . .
L E V E R I T A B L E A U T E U R D . . .

The text needs only be divided up into proper word lengths, and the solution is complete: LE VÉRITABLE AUTEUR D . . .

The reader must have noted by this time how simple and straightforward the solution of a case of this kind can be. Notwithstanding the apparent hopelessness (to the uninitiated) of the problem, it is thus seen to be solvable quite simply, following a procedure and

utilizing means known to specialists in cryptography for many years. The present author would indeed welcome an opportunity for earning the round sum of 300,000 francs (even at the current rate of exchange this would buy quite a few books) for solving so easy a cryptogram, for even an amateur cryptanalyst should be able to solve in a couple of hours or so the cryptogram with which Judge Jarriquez struggled for several days. And it is clear that Verne did not purposely exaggerate the difficulty for the sake of heightening the dramatic effect of his story, for he really believed the problem to be beyond the powers of analysis of cryptographic experts. In an interesting volume, Hommes et Choses de Science, the celebrated French engineer, Maurice d'Ocagne, reproduces in facsimile a letter from Verne of which the following is a translation:

28 Oct. 81.

My Dear Maurice: I have received your letter. I believed the document almost indecipherable. If I had known that at the École polytechnique one of your classmates could solve the cryptogram I would have added an interversion of the letters which have guaranteed it against every investigation. But after all Mr. Sommaire took 3 months to find this key. Judge Jarriquez had but 8 days for that. It would not have been astonishing had he not succeeded at all. But let's not tell him; it would make him blow his brains out.[13]

I have not seen your father for a long time. Shake his hand warmly for me. And to you,

Very cordially,

Jules Verne.

(P. S.) When I see you I want you to tell me how Mr. Sommaire succeeded in that. I vow this intrigues me."[14]

This comment establishes that while Verne had informed himself on the principles of enciphering a message by the so-called Gronsfeld method, he had not acquainted himself with the principles used by experts in solving a cryptogram produced by that scheme. The result

[13] The French is "Il se ferait sauter la cervelle," which is rendered in Larousse du XXme Siecle as I have given it. But somehow it fails to fit the context. I can hardly agree with a friend who suggests that the translation by implication is "It will cause his head to swell to the bursting point." Perhaps Verne meant to say that if Sommaire were told what had taken him 3 months to accomplish was done by Judge Jarriquez in 8 days, he (Sommaire) "might blow his brains out."

[14] That Verne was sufficiently intrigued by M. Sommaire's solution to have made an effort to learn more details is established by the following paragraph extracted from an article by d'Ocagne which appeared in Revue Hebdomadaire, Année 37, tom 9, Sept. 1, 1938:

> Devoted as he was, as if by a decree of Providence, to the task of spellbinding his contemporaries by his amazing inventions, Jules Verne himself was not lacking in the faculty of being astonished. That was plain to me the day when I communicated to him, before the appearance of vol. II of La Jaganda, a translation made by one of my classmates of the École polytechnique, of the cryptogram given at the beginning of the first volume of this novel, and which he, the author, considered as indecipherable. He purposely even came to the École in order to have my colleague explain to him how he went about successfully executing this feat of divination, and I see him yet, turning my way several times, in the course of this explanation, to exclaim. "What analytical powers! I am literally bewildered by them. What analytical powers!"

is that the method employed by Judge Jarriquez depends on a chance suggestion of a "probable word" instead of following the orderly steps of analysis which cryptanalysis shares with chemistry for example. Furthermore, when Verne states in the d'Ocagne letter that if he had known that somebody could solve the cryptogram he "would have added an interversion of the letters which would have guaranteed it against every investigation" one is led to wonder how in that case Judge Jarriquez would have been able to arrive at any solution at all—for by "interversion" Verne can only mean some form of transposition such as he used in the other cryptograms discussed herein, such as reversing the order of the letters, employing a rectangular design or a grille, and so on. Then, indeed, would Judge Jarriquez have struggled in vain and Verne would have had to adopt some other course in extricating his hero from the noose. For according to the method of solution Jarriquez finally adopted, the only way of ascertaining whether the "probable word" ORTEGA was correct was to test the key it yielded on the rest of the cryptogram. Now, if a transposition had been added, this sort of testing, without a complete knowledge of the method that had been followed in effecting the transposition, would be entirely futile.

Despite what may appear to the reader to be quite devastating criticism of Verne as a cryptographer, it is far from my wish to convey the impression that his efforts in this field are unworthy of note. For when we look into the types of cryptograms other writers of romantic tales and detective stories have employed, we must recognize that he stands head and shoulders above them all—not excluding even Poe. The latter used for his vehicle one of the very simplest types of cryptograms known; its analysis was, it is true, an excellent piece of work in The Gold Bug and I hardly think that any writer has surpassed Poe in the lucidity and excellence of the demonstration he gives of the method of solving this type of cryptogram. But Poe never attempted a tale involving anything more difficult than a simple substitution or if he did his efforts came to naught, because Poe's works include only one story involving the solution of a cryptogram. Certainly Poe knew of the type of cryptogram called a multiple-alphabet or repeating-key cipher, but there is reason to believe that he but vaguely grasped the method of solving it. Verne, on the other hand, chose three different types of cryptograms, all more difficult than simple substitution, and wove ingenious stories about them. And when we observe the puerility of the types of cryptograms even modern authors of stories employ, Verne's genius calls for admiration and respect—even on the part of professional cryptographers who know only too well the limitations imposed upon authors who desire to interest casual readers in the fascinating art of solving ciphers.