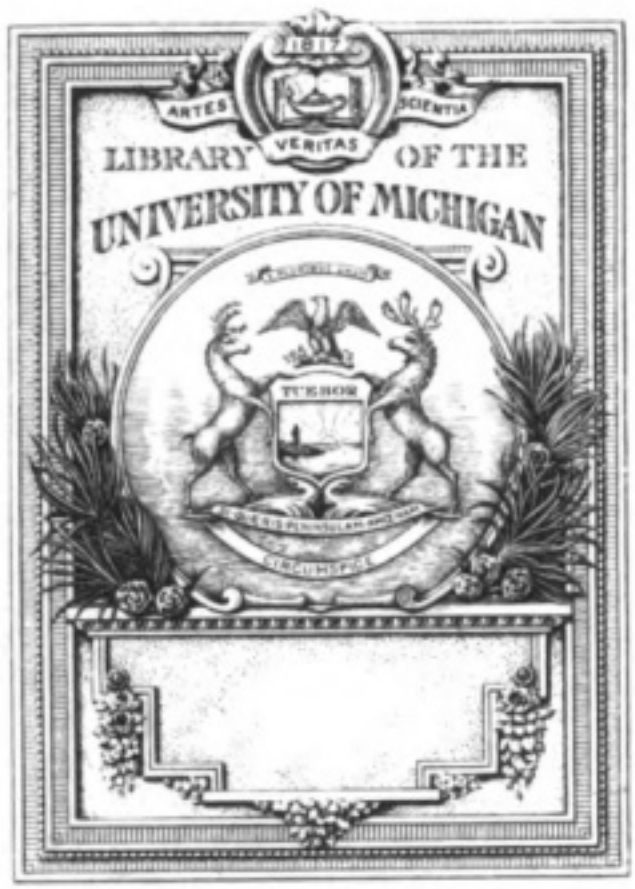


THE MILITARY CIPHER
OF
COMMANDANT BAZERIES

RESEARCHES IN CRYPTOGRAPHY AND DECRYPTING

A Series edited by Rosario Candela · Issue I ·

THE MILITARY CIPHER *of* *Commandant Bazeries*

AN ESSAY IN DECRYPTING

BY

ROSARIO CANDELA

of the American Institute of Architects

CARDANUS PRESS · NEW YORK

19 EAST 53RD STREET

1938

MADE IN U. S. A. BY HADDON CRAFTSMEN, INC., CAMDEN, N. J.

To

BASIL

my youngest son

TABLE OF CONTENTS

CONTENTS

VI. COMMENTARIES

I. RANDOM EVALUATIONS

II. FAILURES

III. ENGLISH ADAPTATION

ILLUSTRATIONS

WITH this essay we inaugurate a series of publications dealing with the science and problems of cryptography and with the fascinating art of decrypting.

Cryptography, to our day, has generally been understood to be a diplomatic or a military science. Yet, there is nothing diplomatic or military about it except that, for obvious reasons, governments and armies in the field use it extensively.

These hierarchies, however, have invariably discouraged its spread and, worse yet, they have consistently spurned outside cooperation—meddling they call it—with the naive explanation that *civilians* do not know what it is all about.

This attitude is indefensible and dangerous; indefensible, because civilian contributions to cryptography and to the younger kindred subject, decrypting, have been in the past overwhelmingly preponderant; dangerous,[1] because to restrict the pursuit of a discipline within the narrow confines of institutions whose activities are patterned within traditional moulds tends to atrophy it.

In truth, cryptography belongs to the domain of culture, and, as such, is the heritage of man. Any humble mortal may, therefore, commune with it, if his aptitudes lead him to its altars.

And we profess to approach it humbly, with the hope that our efforts will prove interesting to the intelligent reader, stimulating to the student, and perhaps of some help to its.....priests.

[1] "It seems to us," says General Givierge (*Cours de Cryptographie*, Berger-Levrault, Paris, 1932, pp. VII), "that it is of national interest to awaken cryptographic vocations. Several were aroused during the last war thanks to the happy chance which brought to us, at the Cipher Bureau, a personnel, who, although not at all versed in this subject, nevertheless, well cultured as they were, achieved brilliant successes. But it is prudent not to rely entirely on such fortuity."

Dear Reader,

Cryptograph.....itis—we are borrowing the word from Bazeries himself—is a sort of subtle, all-pervading, incurable malady. The moment it grips you, it rapidly spreads its tentacles to the most recondite corners of your nervous system and stays there, never to leave you ever after.

In a mild form, it is harmless. The solving, now and then, of a few cryptograms of the kind that our forefathers, of blessed memory, considered perfectly safe, proves to be an adequate sedative; moreover, it heightens the spirits of the afflicted to a level of self-esteem quite unbelievable and, why not admit it, out of proportion with the accomplishment.

But when virulent, it is an altogether different malady. It gives its victim delusions of grandeur. Solving the ordinary ciphers found in daily newspapers or those so dear to members of the various puzzle and cryptogram associations, he thoroughly disdains. Historical ciphers, at least, must be his diet, when not authentic state documents.

It subjects him to hallucinations. The secrets of the country are in jeopardy, *ergo*, it is his imperative duty to make them safe; in fact, he is the only one that can.

It wrecks him. And, it makes of him a sad nuisance to his family, his friends, and very often to his government.

⁂

How it came to pass that a quite harmless citizen, blessed with a rather broad practice in a calling so foreign to cryptography, became infected with this strange ailment is not difficult to set down.

"A communion of the Arts,"[1] laughingly suggested a facetious friend of ours, to whom it was earnestly being explained that decrypting is truly an art. And we are not yet sure whether he was laughing at our artistry in architecture or cipher solving! Perhaps at both.

In reality, the germs that brought the author's infection about were the appearance of a thrilling work[2] dealing with the activities of a government bureau during and after the Great War, and the economic upheaval, that almost stilled the nation's activities.

To that book and to the often cursed Depression, the Author owes his knowledge of this alluring subject: the one having been the spark that fired a restless mind, the other having provided the time. To them he is indebted for the incalculable happiness he was able to derive from its study in a period of our civilization replete with misery and abject fear.

---

[1] An historical instance of such an unusual communion goes back to the Early Renaissance. Leon Battista Alberti (1404–73) was a member, with Brunelleschi and Michelozzo, of that powerful triumvirate of artists that blazed the way for a new architecture, thenceforth the most widely followed and adapted throughout the civilized world. His skill in architecture is evidenced by the much admired Palazzo Rucellai in Florence and the Churches of S. Andrea in Mantua and S. Francesco in Rimini. His book on Architecture, "*De Re Aedificatoria*" (Florence, 1485; English translation by Leoni 3v., 1726) helped to promote the revival of the old Roman styles (Fletcher, *A History of Architecture*, London, 1896).

He was one of the great humanists of the epoch. His activities, covering a broad range of subjects, caused Dathus, the then papal secretary for ciphers, to commission him to investigate ciphers and write a treatise upon them. Lange & Soudart (*Traité de Cryptographie*, Félix Alcan, Paris, 1925) consider it, "*a classic work, susceptible of being studied fruitfully, even today.*" This treatise is reported in full in its original Mediaeval Latin, in: Meister (Dr. Aloys) *Die Geheimschrift im Dienste der Päpstilichen Kurie*, Paderborn, 1906, pp. 125–141.

He was the first to introduce *multiple representations of vowels* in order to dilute their frequencies in secret texts; he was the first to suppress the *doubling of consonants* which, in the simple substitutions then in vogue, were too evident an index to *interpreters* of ciphers; he was the first to suggest the use of a *ciphered code*—a small code of 336 words and phrases, to be sure, but nevertheless a code—obtained by the permutations of four digits, taken two, three and four at a time; he was the first to introduce a mechanical device that helped ciphering—*a circular disk*—a type of which was still being used, until not so long ago, by the U. S. Army.

Lt. Col. William F. Friedman, *Signal Reserve, U.S.A.*, points out, very correctly, that this disk gave origin to the many systems of *multiple alphabet ciphers* advanced by later Italian cryptographers. Alberti, apparently, did not realize the full possibilities of his disk, for he fails to describe them in his history-making treatise.

[2] Herbert O. Yardley, *The American Black Chamber*, Bobbs-Merrill, Indianapolis, 1931.

For many valuable and helpful suggestions he is grateful to his friends, Geraldine Pascale and St. Elmo Tower Piza and to Mr. Henry Kroul, a member of his staff.

To Major Donald D. Millikin, *M. I.-Res.*, he expresses his sincere appreciation for his stimulating criticisms and for checking the technical material of the text.

For kind permission to make quotations from the works of various authors, many thanks are due to Fasquelle Éditeurs, Paris; Éditions Berger-Levrault, Nancy; Librairie Félix Alcan, Paris; Émile Perrin, Paris; Yves Gyldén, Stockholm, General Luigi Sacco, Rome; and Henry Holt and Company, New York.

Finally, he heartily thanks the staff of his office and especially the Misses Pagano and Vogt who collated and typed the manuscript.

Harrison, N. Y.

THE MILITARY CIPHER
OF
COMMANDANT BAZERIES

Chapter I

INTRODUCTION

COMMANDANT ÉTIENNE BAZERIES of the French Army was one of the most brilliant cryptologists of the *ante-bellum* era. As a cryptanalyst, he was *l'enfant terrible* of a group of famous adepts of this art, among whom de Viaris, Valerio, Deltheil, Hermann and Angammare must be remembered. The smashing of new cipher systems as quickly as they made their appearance seems to have held for him a peculiar fascination.

His was an age of revival of cryptographic studies brought about by the emotional disturbance caused by the proceedings instituted at the High Court of Justice in Paris, in 1899, against the Duke of Orleans, for plotting against the State, and by the not less stirring Dreyfus Case, at the second Court-Martial of Rennes, in the same year. With scant material to work with, Bazeries decrypted the secret correspondence between the Duke and his agents,[1] in the first instance; and in the other, he correctly inferred that the famous Panizzardi[2] telegram was coded with a Baravelli dictionary.

These two exploits so startled an astonished public that a chorus of

---

[1] On page 6, vol. V of *Histoire de l'Affaire Dreyfus* by Joseph Reinach (Charpentier et Fasquelle, Paris, 1905) we read in note 2—the parentheses are ours:

"(2) HAUTE COUR, VII, 5, BAZERIES. He had deciphered, in 1891, the despatches of Louis XIV relating to the Iron Mask and, in 1895, those of Napoleon during the campaign of 1813. Having taken his leave (from the Army) on February 20th, 1899, he was recommended by an official of the State Department, where he had worked, to the Police Prefect and to the Director of the *Sûreté Générale*. They gave him the messages and the cryptographic table, called square cipher or Vigener (*sic*) cipher, which had been found in Chevilly's (one of the conspirators) quarters. Bazeries translated almost immediately the Chevilly messages, then those of Buffet (another of the conspirators) made with the Beaufort cipher; finally, but only after four months of work (we are shocked!) the messages of February 1898. '*The Key had been changed; these gentlemen had, without a doubt, agreed verbally with the Duc d'Orléans that they would make use as a key of Nuit de décembre (the title of a poem) by de Musset: the first day of the month, they took the first line as a key; the third day of the month, the third line . . . etc.*' These translations were acknowledged as exact by Buffet and Chevilly."

[2] Dreyfus was charged with treacherous relations with the German and Italian Governments. Upon his arrest, Panizzardi, the Italian Military Attaché in Paris, who had never had any relations with him, asked his Government to issue a strong denial of the charges in order to stop the unfavorable comments of the Press. How his telegram was garbled to suit the purposes of a *coterie* of officers bent upon ruining Dreyfus is another story.

requests was raised on all sides for a presentation of his methods of decrypting. In response, a little aureate book[1] saw the light, soon afterwards. To peruse this book and follow Bazeries in his subtle, yet sane and robust reasoning, to revel in his scintillating and often caustic wit, to partake of his gruff, typically Gallic *bonhomie* is a never-ending delight which should not be missed by cipher students.

***

His fervent patriotism led him to an incessant struggle with his Government whose official ciphers he early exposed. The weaknesses of these ciphers, as well as of those proposed for adoption by Bord, Gavrelle, La Feuillade, de Viaris, Hermann, d'Orcagne and others, were brought to light publicly for the purpose of moving the officials to action.

He was most critical of the "*competent*" authority whose shortsightedness, according to him, endangered the security of the state; and he rejoiced over the fact that France was not then at war, lest heaven knows what disasters befall the armies of the Republic.

His contempt for the "*competency*"[2] of such governmental boards, commissions, etc., that thwarted every effort of his to bring about reform and a measure of safety in the official codes, fairly oozes from the pages of his writings.

From the perspective of time, all of this simply brings to us a fresh confirmation that governmental hamstringing is everpresent, in all ages, the world over.

***

His more serious work, and he had a prodigious capacity for it, centered in the successful reconstructing of famous codes which, up to his time, had withstood the attacks of other experts.

[1] Commandant Bazeries: *Les Chiffres Secrets Dévoilés* (Charpentier et Fasquelle, Paris, 1901).

[2] The terms "competent" and "competency" when associated with a governmental body of any kind do not always carry, in French and Italian, the full meaning given to them in our dictionary. In most cases, they merely signify "having jurisdiction" although a slight implication of the truer meaning remains. But the French and Italians dislike these oft-repeated official words, and openly belittle the authority behind them upon the least provocation, and with great zest.

From five ciphered dispatches of Louis XIV and two of his Minister of State Louvois to Marshal of France Catinat, in command of operations in Northern Italy—containing a little over 11,000 groups of figures—he was able to recover the "Grand Chiffre de 1691"[1] used exclusively by the *Grand Roi*. This cipher consisted of an extremely well-compiled code of about 600 literal, syllabic and full-worded entries, including punctuation signs and *nulls*, with numerous *homophones*,[2] used with a skill undreamed of for that age.

The epoch-making reconstitution of this code,[3] definitely settled the identity of a famous prisoner, condemned by that Monarch to wear a mask,[4] and put a stop to the legendary tales circulated by a host of romantic writers led by Voltaire, and to the ill-founded speculations of historians.[5]

Other historical ciphers that gave way before the penetrating insight of Bazeries were those of Francis I, Francis II, Henry IV, Mirabeau, and Napoleon I.[6] To the weakness of Napoleon's cipher he attributed a measure of responsibility for the Emperor's reverses in Russia.

***

Bazeries invented[7] and consistently applied in his work a new process of decrypting. It is used today very fruitfully with several special types of ciphers. It is known as "*the process of the probable word*" and postulates the

[1] The *Grand Chiffre* usually bore a date for the reason that its ciphering and deciphering lists were frequently changed. Moreover, for less important correspondence the King used a smaller cipher, the *Petit Chiffre*, containing only 367 groups.

[2] *Nulls* are letters or groups of letters having no value, inserted in secret texts to confuse would-be inquirers and to lead them astray; *homophones* are the various representations of a single letter or a group of letters used for the purpose of diluting the frequency of that particular letter or group.

[3] Émile Burgaud & Commandant Bazeries: *Le Masque de Fer* (Firmin-Didot, Paris, 1893).

[4] Of course, this was not the primary purpose for the attempted reconstruction. In 1891, Commandant Gendron of the General Staff, while preparing a study of Catinat's campaigns, came in possession of the ciphered documents described above. Sensing their historical importance he submitted them to one army expert after another for a translation and, in spite of his encouraging help and a great deal of entreating, cajoling, fretting and honest swearing, he was not able to get it until after he had despairingly consulted Bazeries who, after glancing at the documents, boldly took it upon himself to solve them.

[5] "Fifty-two writers," says Marius Topin (*L'Homme au masque de fer*, Émile Perrin, Paris, 1883) "have, one after another, tried to clarify this question without bringing any new light and it may be affirmed that a century of controversies and efforts have not yet dissipated the mysterious shadow enveloping the prisoner."

[6] Commandant Bazeries: *Les chiffres de Napoléon Ier* (M. Bourges, Fontainebleau, 1896).

[7] See Chapter VI, I, 7.

assumption that the cryptogram contains a specific word, which must be correctly guessed. This is not too difficult when one knows something of the nature of the secret text. Military communications, especially, are apt to include words like *general*, *enemy*, *ammunition*, *reinforcements*, *attack* and the like. The process is more often applied in searching for parts of words, particularly endings of long ones, as ....*ment-s* (move*ments*, develop*ments*, employ*ment*, etc.), ...*ation-s* (modific*ation*, oper*ation*, situ*ation*, combin*ation*, concentr*ation*, etc.), ...*ward-s* (for*ward*, after*wards*, south*wards*, northeast*wards*, etc.) or *empty*[1] words such as *the*, *and*, *will*, *could*, etc.

***

"*To prove that a cipher is worthless, is well enough; but one must be prepared to propose something better to take its place*," Bazeries himself declares.

Does it not seem natural that a man so versed in unraveling secret texts, some of them erroneously ciphered—with malice, to confound him—others treating of abstruse subjects, alien to military matters, should step into the field of cipher making? Would not his vast acquaintance with cipher systems of all sorts give him repeated opportunities to detect and to analyze the weaknesses of all those systems? We think so.

So did he. In fact, he unblushingly said so. He felt that his accomplishments in decrypting—indeed masterful, we add—did qualify him, better than others, to devise a foolproof system.

With unbounded energy he threw himself entirely into this field of pure cryptography in quest of the still unattainable goal. This task, the most thankless of his distinguished career, and the one that filled him with bitterness and disappointment, occupied the better part of his time from 1890 to 1892, and later in 1898.

During these periods, with dogged obstinacy in the face of persistent, monotonous rejections, he proposed for adoption four different cipher systems—the last two conforming to specific suggestions received from his admirers in the Staff.

***

[1] We recommend, for cryptographic work, this term with which Italian authors denote words that have no concrete significance such as articles, prepositions, conjunctions, auxiliary verbs, etc.

The cryptograms accompanying the first two systems, proposed in 1890 and 1891 respectively, were not solved. Nevertheless, Bazeries acknowledged as reasonable the War Department's criticisms that the ciphers were neither simple enough, nor sufficiently rapid for practical use. Both systems were elaborations, more or less complicated, of the square (Vigenère) cipher, in those days the magnetic center to which cryptography gravitated.

***

The third attempt, also proposed in 1891, produced the cylindrical cryptograph.[1] It resulted from the assumption that the War Department would welcome an apparatus upon which ciphering and deciphering could be read directly, thus avoiding the laborious written operations and the sustained attention required in the preparation and translation of messages. "*Sans cassement de tête*" as the French put it.

It was rejected.

Resubmitted the following year with slight modifications making its manual operations easier, the cryptograph was again rejected.

The reasons given by the French Government in declining this apparatus are, in both instances, puerile. They refer chiefly to objections in handling, and to difficulties in reading characters from metal disks. As a matter of fact, it is a very ingenious contrivance, extremely easy to handle and yielding rapid results. It certainly eliminates the "*cassement de tête*"[2] so cordially detested by the patient victims of cryptography: the cipherers.

The cryptograms submitted with it could not be deciphered at that time.

In 1893, de Viaris, in three different tests, showed, however, that messages ciphered with its help could be decrypted.[3]

Bazeries was not disconcerted. In defence of his apparatus, he minimized the results, pointing out that he had supplied de Viaris with numerous

[1] "Cryptograph," a mechanical apparatus which ciphers. This definition is at variance with its accepted meaning (i.e.: something written in secret characters; a cipher). It may, however, be justified in view of the fact that similar words such as: telegraph, phonograph, dictograph, etc., denote instruments.

[2] We were much attracted by the quaint Old French equivalent, *Vn rompement inestimable de teste*" used by Vigenère. (Blaise de: *Traicté des Chiffres*, Paris, 1586, pp. 34 *verso*.)

[3] Le Marquis de Viaris: *L'Art de chiffrer et déchiffrer les dépêches secrètes*, Gauthier-Villars, Paris, 1893 (pp. 50–52, 99–109). An exposition of the decrypting in English is given in Publication #20/1918 issued by the Riverbank Laboratories, Geneva, Ill. (pp. 37–58 and plates). (Out of print and not obtainable.)

indications and insisting that the initial cryptogram he had submitted, upon which de Viaris had labored very hard (*fortement travaillé*), was still undeciphered. Was not this failure, Bazeries argued, a manifest proof that his opponent's process of decrypting was fallible?

Even as late as 1901, that is, eight years after de Viaris' decrypting took place, Bazeries, referring to the apparatus, expresses himself as follows:

> "Mr. de Viaris has found *in theory* a mathematical formula for its decrypting. This *mathematical* formula was, however, not good enough to give him the translation of the late Mr. Édouard Lucas' cryptogram which concludes the description of the apparatus presented at the Congress for the Advancement of Science held in Marseille in 1891. The ciphering obtained with the cylindrical cryptograph does not fear any kind of search or investigation; it is absolutely indecipherable to anyone not possessing the secret word. It does not fear anything but the disclosure of the key-word."

And thus Bazeries' faith in the indecipherability of texts obtained with his cryptograph, the love-child of his brain, remained unshaken.

However, in spite of our admiration for Bazeries and his device, we are compelled to conclude that, by adhering STRICTLY[1] to the rules of composition as laid down by himself, the resulting cryptograms CAN be decrypted without any external help.

***

In his controversy with de Viaris, Bazeries showed, and we regret it very much, a woeful lack of that intellectual generosity which a scientist must invariably display towards an antagonist when facing the collapse of his theory, even if a cherished one. Strangely enough, it was bestowed on him with extremely good grace by Gavrelle a few years previously when, in a series of increasingly difficult tests, Bazeries proved that ciphers obtained with the apparatus that Gavrelle had proposed to the French

[1] It is our opinion that the weakness of this system lies in the simultaneous *prescribed* use of ALL the disks the instrument commands. We firmly believe that with some intelligent modifications, coupled with a few changes of practical nature, it can be made to render excellent and safe service.

Government could be decrypted. "*Accept*," Gavrelle wrote him, "all *my compliments. I confess that the results* (of Bazeries' analyses) *seem to me very scholarly.*"[1]

***

The fourth of Bazeries' attempts, proposed in August, 1898, forms the subject of our essay. This final effort produced a system conforming to a cardinal requirement advanced by the General Staff that nothing more than a pencil and paper should be used in preparing cryptographic work.

The three cryptograms sent with the proposal remained, as on the previous occasions, unsolved.

Shortly after, Bazeries was invited to disclose his system. He did so, and with the "*mémoire*" he included a fourth cryptogram, with a warning that some modifications of the ciphering rules had been made.

The General Staff were unable, according to Bazeries, to obtain from their experts a translation of this last cryptogram but they nevertheless rejected the system on the grounds that it did not possess guarantees of security sufficient for its adoption.

This statement galled our author. "How can they reconcile this decision with their failure to solve the cryptogram sent with description of the system?" he exclaimed.

This final check put a definite stop to his efforts to be helpful. He took the rebuffs philosophically and withdrew, remarking rather sententiously that "*to succeed, one must know how to amuse the conceit of the 'competents'*(?)."

***

The bibliography of cryptography shows that no attempt has yet been made to decrypt this *paper and pencil* cipher since its publication. At least, we should be allowed so to assume, if we bear in mind that every contribution of Bazeries was closely scrutinized and commented upon. Furthermore,

[1] The underscoring is ours.

his fiery temperament and unyielding nature must have aroused, in the course of his distinguished career, the petty jealousies of his *confrères*, who would certainly have welcomed a fresh opportunity to confuse him.

***

The problem looked too tempting. The absence of an official analysis encouraged our daring. Coming from an authority of Bazeries' caliber, we felt that it might earn for us, if successful, that measure of gratification which is the reward of any accomplishment.

"*Quo difficilius, hoc praeclarus*"

we remembered with a lack of modesty, and we succumbed to the temptation.

***

Was Bazeries' claim, that this cipher was practically impregnable, justifiable?

That is what we propose to discuss in the following pages.

Chapter II

THE PROBLEM

We give herein, *in extenso*, a translation of the two communications which Bazeries addressed to the French General Staff; the first, when he submitted his system; the second, after he was invited to describe it.[1]

For readers who prefer the original French, Bazeries' propositions are reproduced in Appendix II.

Those who are not familiar with cryptography and its terminology should, before acquainting themselves with the problem, read Appendix I, where the bare essentials of this science are briefly given to enable them to follow the analysis with more ease.

For general reference, the lines of the text of these two communications have been numbered.

* * *

CRYPTOGRAPHIE MILITAIRE

COMMANDANT BAZERIES

PROPOSITION of a system of military cryptography requiring only pencil and paper, easy to keep in mind.

(Copy)[2]

In 1891, I submitted to the War Department a cryptographic 1
apparatus of my invention,[3] capable of yielding a cipher, easy to

[1] They form Note VIII of his book *Les chiffres secrets dévoilés* and at the end of each are appended some connective or concluding sentences of his own.

[2] The date of this communication is not given. However, it appears to be August 28th, 1898. The place where written is also not given.

[3] See Chapter VI, I, 7.

establish, easy to translate, and requiring neither the withholding of the secret of the system nor any preparatory study.

The superior officers and generals who handled my cryptograph were surprised at the facility of its operation and praised it to me.

This cryptograph was not adopted.

***

From various conversations I have had with general officers on the subject of cryptography and of military cryptography in particular, I have gathered the impression that the deep-seated intention of the General Staff is to find a system which does not require more than pencil and paper and which can easily be remembered without the help of any written notes.

I have done research work and made various attempts in this direction. I do not flatter myself of having found an indecipherable system. However, if the three cryptograms I am giving further on, elude the efforts of the decryptors to whom they will be submitted, I shall, perhaps, have found the solution of the problem, hitherto looked for in vain.

***

Any cryptographic system betrays its method through the analysis and the breaking down of the cryptogram. As soon as the method is found, the rest of the decrypting is nothing but a game for a specialist of moderate skill.

The system I have determined upon has the advantage of leaving doubts as to the method employed; I will say more—it deceives the analyst. The researches, leading to false channels, will come to nothing.

Complicated combinations are worthless. I have adhered, as always, to the greatest simplicity possible. I have made use of some

cryptographic ruses to disguise the system. Will they prevail over cryptanalysts? I think so. It seems to me that, personally, I should have been deceived and consequently thrown off the scent and rendered powerless.

It remains to be seen whether others, abler than myself, will also be deceived. If so, the system is good.

I cannot, for the moment, reveal the method; it is of such simplicity that its secret, it seems to me, is mandatory. Nevertheless, I have not said my last word; for, by slightly modifying the method, while still preserving its original conception, we may, perhaps, not fear its divulgation.

***

I have always considered it a real danger to base the security of a cryptographic system upon the secret of the method used. Too much negligence is bound to take place to presume that the secret—the object of the enemy's covetousness and necessarily in the possession of a great number of persons—could remain unknown for any length of time. My view is that security must reside in the excellence of the system and in the secret of the key: the only secret.

All I can say at the moment is that, with respect to the rapidity of the ciphering and deciphering operations, the system leaves nothing to be desired. It is as rapid as those prevalently in use, if not more so. Furthermore, each cryptogram is made with a different key, chosen at will by the cipherer, without the need of any previous understanding with the other correspondent. In a word, the cryptogram shows and bears its own key.

It is to be remarked that I am not as affirmative as regards indecipherability as I was when I proposed my cylindrical cryptograph, since I am not as sure of this system as I was and still am of my cryptograph.

I will describe my method as soon as it will be requested of me.

CRYPTOGRAMS CIPHERED ACCORDING TO THE METHOD BAZERIES AND NEEDING FOR THEIR TRANSLATION ONLY PENCIL AND PAPER

No. 1.—85 Groups

E J A D S
L C M X F
L X S B B
X S Q C F
M O C U S
S O E U E
P X Y O C
S X S J M
J V C A O
X J X M B
C Y O J V
Q U X T E
C Y P E B
H C M L H
F S V X C
Y Y C X O
Y M C A O
J S P C O
L S J O E
Y P S J C
C B C X Y
H S A Y O ./.

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

C J A D E
E A H C X
Y M C H S
Y C X O O
L S X P X
S P S C Q
E I S L S
S H C F M
V T S C T
S C Q P V
V T S X S
X S O S A
C A E C P
S I O C L
C C H S S
L U Y S Y
H V T A E
C Y P E O
X C S H S
H S X M O
E L T H V

C E Y P E
E C J M S
L L O C C
V M H S L
S L L M C
P V O D C
J S P L O
J Y O M C
H S L J C
O D V P X
C J L C S
X C J D E
M S Y S H
I E O P G
L O M E A
A Y S O A
L L M C N
S X M B C
X L O C A
C S X A O
L H C A S

No. 2.—40 Groups

D E G S C
U A O S H
S B Q C X
B S N K S
S C G X D
Q D S S C
O G X M S
N H R S Q
Y H X S K
R H S Y A

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

O S K S A
M Q S H S
S L D S K
N D D S K
L X L Y R
H Y T Q Y
E O L Q Q
Q K Y C O
M S N O M
B A O S H

U Q O L Q
H Q O N D
C C Q C S
Q T N A O
O M C H Q
S L C S K
S O A O J
M R O S A
Q S C H X
N D Q T T./.

No. 3.—48 Groups

I A V M I
X X J Q B
M F M Q C
O M S P J
M C M B Q
M V C M I
H A L M I
Q M I I A
C Q G M J
Q T K M I
K H J H Q
X S F K R

M J M A I
M F F J Q
G M X H M
X J H M B
O H K J H
K M C T F
M C Q J S
E Q I M H
M H X M X
C S U K M
B R N K J
O O X Q T

Q C C M B
H K M J Q
C X I O O
M T X J A
A I X M H
H K X J M
T N R F A
Q O I X M
S M C R O
O K M F Q
I H R Q L
A J S H A

X H C L Q
B A I I H
S M T R S
I C Q Q K
K M R K J
I O Q B J
I M R H G
J T M F X
O K M T C
X M R K X
H Q C Q T
D H B M X./.

(Signed) Com[t] BAZERIES.

On September 14th, 1898, we were advised that our memorandum had been submitted for examination to the Board of Military Cryptography.

Some time later we were invited by General Niox to disclose our method, kept secret until then.

Here is a copy of this method.

CRYPTOGRAPHIE MILITAIRE

COMMANDANT BAZERIES

METHOD needing only pencil and paper.

(Copy)[1]

To CIPHER—Write the clear text preferably on square ruled paper, a letter in each case, in long hand,[2] leaving a blank line between lines of the clear text. The blank line is to receive the ciphering.

Let us cipher: *Envoyez un bataillon d'infanterie au Creuzot, ce soir, par voie ferrée.*

Thus:

e n v o y e z u n b a t a i l l o n d i n f a n t e r i e

a u c r e u z o t c e s o i r p a r v o i e f e r r é e

***

KEY—Select a substitution key. This key consists of any two letters. By giving each letter the value denoting its rank in

[1] The date and place of writing are not given.

[2] This is a set idea with French authors. They invariably use small letters for their clear messages, as against capitals for the crypto-equivalent. Americans do not feel that a sharp differentiation in the appearance of the two is essential and prefer the use of capitals throughout their work because they are easier to read, and fewer errors are likely to occur with them.

the normal alphabet,[1] transform these two letters into a whole number.

Example:
AB = 12
DZ = 425
BA = 21
ZF = 256
etc. etc.

When the key has been chosen, ZF, for instance, that is: "*Deux cent cinquante six*," establish a conventional alphabet where all letters appearing in the key are at the head, that is: D E U X C N T I Q A S,[2] and those that do not appear in the key follow in their alphabetical order, that is: B F G H J K L M O P R V Y Z.[3]

Write this alphabet horizontally from the beginning to the end, in the cases of a square of five.

Thus:

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

Write on the side, in a similar square, but vertically, the normal alphabet from beginning to end.

Thus:

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

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

[1] That is:

1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25
A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	X	Y	Z

[2] Omitting repeated letters is understood: D E U X C (E) N T (C) I (N) Q (U) A (N) (T) (E) S (I) (X).

[3] There is an error in the original. BFGH*T*K . . . . . is given where T has been misprinted for J.

NOTE—Do not be apprehensive if in some instances the same letters occupy corresponding cases of the two squares of five. It is the result of chance.[1]

***

CIPHERING BY SUBSTITUTION—As soon as the key is established, substitute each letter of the clear text with the letter given by the substitution key and write this letter in the blank line reserved for this purpose by using a capital.

NOTE—To expedite the operation, transform at one time all like letters by following them up in the text before passing to the transformation of the letter next following. In this manner the ciphering operation is accomplished quickly.[2]

Thus:

e n v o y e z u n b a t a i l l o n d i n f a n t e r i e
P L A V O P Z C L N D Y D K I I V L J K L E D L Y P G K P

a u c r e u z o t c e s o i r p a r v o i e f e r r e e
D C S G P C Z V Y S P M V K G X D G A V K P E P G G P P

On completion of the substitution, divide the ciphering in series of three letters by means of a line, black, red, or with pencil.[3]

Thus:

| e n v | o y e | z u n | b a t | a i l | l o n | d i n | f a n | t e r |
| P L A | V O P | Z C L | N D Y | D K I | I V L | J K L | E D L | Y P G |

| i e a | u c r | e u z | o t c | e s o | i r p | a r v | o i e | f e r |
| K P D | C S G | P C Z | V Y S | P M V | K G X | D G A | V K P | E P G |

| r e e |
| G P P |

***

[1] In the above alphabet, Q and Z occupy corresponding cases in the two squares.

[2] Namely: The first letter of the message is E. Substitute all the E-elements in the message with their equivalent crypto—P. Then do the same thing with clear—N, the second letter, and so on.

[3] This is very amusing. We can just imagine Commandant Bazeries fussing over his cryptograms with a multitude of colored pencils. Even the great have their failings. Colored pencils are used in cryptographic work, but not exactly for this simple purpose.

CRYPTOGRAM BY TRANSPOSITION—Form the cryptogram by reversing the trigrams.

***

CONVENTIONS—It is understood that the first two letters of the cryptogram indicate the substitution key and that each time the first letter of a trigram is a vowel: A.E.I.O.U.Y., this vowel is a null. Thus, we are enabled to introduce nulls whenever we wish it and as often as we wish it. Necessarily a null must be introduced when the first letter of the reversed trigram is a vowel. When such first letter is a consonant, the insertion of the null is discretionary.

***

REMARKS—It should be arranged to complete the cryptogram with a final, whole group of 5 letters, key included, which is easily done, due to the freedom of inserting nulls at will.

It is well to give, at the beginning of the cryptogram, the total number of groups of 5 letters it contains so that, if one of them is omitted in transmission, the deciphering may, nevertheless, be attempted.

***

Sample cryptogram for the message just ciphered:

FROM THE COMMANDING GENERAL OF THE 8TH CORPS
TO THE COMMANDING GENERAL OF THE TROOPS AT DIJON

13 groups Z F I A L P P O V L C Z A Y D N E I K D
L V I A L K J L D E G P Y D P K G S C A Z C P S Y
V V M P X G K A A G D P K V G P E P P G.

***

To DECIPHER—Begin by eliminating the nulls while dividing in series of 3 letters.

Thus:

13 groups. (Z) (F) (I) A L P | P O V | L C Z | (A) Y D N | (E) I K D | L V I |
(A) L K J | L D E | G P Y | D P K | G S C | (A) Z C P | S Y V | V M P | X G K |
(A) A G D | P K V | G P E | P P G |

After this operation, copy the message by interlining and reversing the trigrams.

Thus:

P L A | V O P | Z C L | N D Y | D K I | I V L | J K L | E D L | Y P G | K P D |
C S G | P C Z | V Y S | P M V | K G X | D G A | V K P | E P G | G P P.

There remains nothing more than to substitute each letter of the cryptogram with the true equivalent prepared beforehand, from the given key. We read: "*Envoyez un bataillon, etc. . . . . etc. . . . .*"

As you see, it is quickly done.

***

The cryptograms submitted for decrypting in my memorandum of last August 28th were prepared in accordance with this method.

It will be easy to translate them.

Such is the method in its greatest simplicity.

***

As I stated previously in my memorandum and as can now be realized, it is imperative that this method be kept secret. It was already imprudent to have put it in writing. It should have been communicated orally.

Nevertheless, by a slight modification of the process I hope to be able to maintain the secret.

This modification I will disclose orally. In the meanwhile it would be useful if some cryptanalysts, now acquainted with my method, tried to translate the new cryptogram which follows.

If it resists decrypting, it means that the system is really indecipherable to anyone not possessing the key.

CRYPTOGRAM—SUBJECT MATTER TAKEN FROM A NEWSPAPER DEALING WITH JUDICIAL NEWS

43 groups.																			
C	M	S	H	Q	B	C	U	P	M	C	C	V	F	S	A	K	F	L	N
F	C	V	B	R	S	N	X	F	T	K	K	R	R	N	D	D	Q	G	H
H	F	S	V	K	R	F	S	N	I	C	R	V	K	B	A	K	V	G	N
N	R	S	M	M	C	H	P	B	K	H	F	Q	U	C	F	U	N	X	R
K	H	K	R	O	D	N	R	N	B	M	R	K	F	G	G	N	C	M	C
G	S	G	C	U	R	K	G	N	V	K	D	D	Q	V	R	K	O	N	B
S	N	K	I	C	V	U	K	B	V	I	G	F	G	C	Z	F	H	U	C
U	C	X	F	F	V	F	C	R	H	K	B	F	V	C	X	N	H	G	Q.

L	M	P	C	X
B	C	U	P	M
S	N	X	F	T
R	F	S	N	I
C	H	P	B	K
D	N	R	N	B
R	K	G	N	V
V	U	K	B	V
V	F	C	R	H

B	R	L	S	Q
C	C	V	F	S
K	K	R	R	N
C	R	V	K	B
H	F	Q	U	C
M	R	K	F	G
K	D	D	Q	V
I	G	F	G	C
K	B	F	V	C

H	F	M	H	H
A	K	F	L	N
D	D	Q	G	H
A	K	V	G	N
F	U	N	X	R
G	N	C	M	C
R	K	O	N	B
Z	F	H	U	C
X	N	H	G	Q.

C	B	H	K	X
V	G	S	R	X
Q	X	N	L	M
V	C	S	G	C
V	I	G	V	T
K	S	V	H	N
N	L	G	Q	T
H	S	A	M	N

This cryptogram, as well as those previously given, bears its key.

(Signed) Com[t] BAZERIES.

The reader knows the answer. It is dated April 19th, 1899, and it is given in Chapter III of Part III.

Let us reproduce it again:

"It has been held that the method does not possess guarantees of security, of sufficient degree to be adopted."

How is it possible to reconcile this answer, decidedly affirmative, with the failure to decrypt the cryptogram of 43 groups which concludes the exposition of our method?

There lies the mystery!

Chapter III

CRITICAL ANALYSIS OF THE SYSTEM

1

Bazeries' Belief in the Indecipherability of His System

Les Chiffres Secrets Dévoilés, which Bazeries defines in the sub-title as an historical sketch on ciphers, is in reality a little more than that. Among other things it is also a critical review of the contemporary literature on the subject sprinkled with many bits of personal reminiscences, mostly dramatic ones.

His many experiences and easy victories in the field of cryptanalysis, having vested him with the necessary authority, he delivers in this book opinions far and wide. He issues them straightforwardly, without "ifs" or "ands," admitting of no refutation. He readily dissects every theory that comes to his attention and knows exactly what is right and what is wrong with each. His *aplomb* is disconcerting, his aphorisms, biting.

Yet, in presenting his fourth system to the French Staff, Bazeries, for the first time, exhibits a lack of his old self-reliance and puts himself on the defensive. For the first time, he expresses some doubts as to the worth of his system, something he had not deemed necessary with his previous three propositions. "He does not flatter himself to have found an indecipherable system" (line 15); "he is not *as* affirmative as regards indecipherability as he was . . ." (line 56).

The contrast between this late circumspection and his *ex-cathedra* attitude of not so long before is too vivid to let it pass unobserved. One is forced to raise these questions:

Were Bazeries' doubts as to the security of his cipher really sincere?

Had de Viaris' clever decrypting of the cylindrical crytograph shaken Bazeries' faith in himself? Or had it made him merely cautious?

Frankly, we cannot accept the first view. If it were not a known theory that in the very *psyche* of inventors, especially of the persistent type that Bazeries proved to be, there reigns the firm belief of the infallibility of their conceptions, we might not doubt his sincerity. Bazeries himself utters this belief repeatedly, even if veiled by vacuous doubts. "Perhaps he has found the solution to the problem so far looked for in vain" (line 18); "the system deceives the analyst" (line 31); "personally, he would be deceived and thrown off the scent" (line 32); "if it (the cryptogram) resists investigation, the system is really indecipherable" (line 143), and finally, his concluding paragraph (lines 152–154), almost an indictment, unmistakably shows that he considered the system safe from prying eyes.

Nor does it appear that his confidence had deserted him. The reassertion of faith in his cryptograph (line 58) is just another instance of that tenacity with which inventors cling to a slipping idea.

This attitude, in the face of the positive results obtained by de Viaris, is open to criticism and it stamps Bazeries as intolerant of opposition and as a rather poor loser.

Inconsistency in Bazeries' Views on Security

We are amazed at the inconsistency we note between Bazeries' stated views on the security of a cipher and his disregard of the same views in the cipher he proposes.

That it is a real danger to base the security of a system upon the secret of the method (line 41) is regarded by cryptographers as a postulate. It needs no proof. It is accepted, and rightly so, as the cornerstone upon which the edifice of a new cipher must rest.

It is not possible to keep secret the rules of a system. And it is everybody's opinion, not his alone, that the security of a cipher must reside in the excellence of the system and not in the secret of its method (line 46).

But he proposes the very thing he condemns. He declares (lines 37 and 134) that the secret of his system *imposes* itself; that it is imprudent to have put it in writing (line 135); that it should have been communicated orally (line 136).

Why did he propose it, then, if it *betrayed* a canon so vital?

The explanation is evident: he was relying on the cryptographic ruses he had introduced in the system.

He was resting on the false belief that he himself would have been thrown off the track—a belittling estimate of his own ingenuity which had detected ruses of all kinds scores of times before.

He was hoping to establish the worth of his system by the failure of others, "*abler than myself*" to solve it, and when his theory proved to be correct he was convinced of the invincibility of his cipher.

The French General Staff, despite the fact that their experts could not decrypt the last cryptogram Bazeries had submitted, rejected the cipher. Did they base their rejection on the very ground that no secret of a system must be maintained? We are convinced that such was the case. And they showed wisdom.

3

The Salient Feature of the System

It is correctly held that the possession by the enemy of a series of cryptograms, all ciphered in one system and by means of the same key-word, facilitates the task of cryptanalysts enormously. Moreover, with the lower forms of ciphers the decrypting becomes fairly mechanical.

In modern warfare the possibility of such possession is of daily occurrence. In the World War the *traffic* between two stations of communication in any active sector would reach seventy or eighty messages in a single day.[1] Even in previous wars it must have been considerable, for, beginning with Kerckhoffs,[2] every writer of cryptography envisages this very possibility and, to combat it, prescribes not only frequent changes of key-words, but also that no system not capable of an easy change of key be adopted.

Bazeries, no less than the others, is aware of this vulnerability of field ciphers, but he openly ridicules the recommendations of his predecessors.

---

[1] General Cartier tells us that during the World War, the French stations alone intercepted more than one hundred million words. (*Le service d'écoute pendant la guerre.* Review *Radio—Electricité*, No. 16 and 17, November 1923.)

[2] *La Cryptographie Militaire* (L. Baudoin, Paris, 1883).

> "*A frequent change of key*," he says, "*cannot make good a defective system. In addition to the perturbation that it brings into the service, the gravest inconvenience, as we see it, is that, if the changes of key are too frequent, it is necessary, in order to remember them, to write them down and it is said, with good reason, anyway, that a written key is a disclosed key.*"

With this view firmly in mind, he sets out to contrive a system of ciphering wherein any number of cryptograms could be made, each with a different key. A consequence of his scheme is that the initiative to establish the key-word is left entirely with the sender whose whim, at the proper moment, would decide upon it, without any previous understanding with the other correspondent.

This novel feature, the most important of Bazeries' fourth cipher system, should in theory, not only increase its resistance to cryptanalysis, but would also eliminate the hitherto widespread knowledge of the key word at both ends of the communication line, often complained of as dangerous.

Chapter IV

FIRST SKIRMISHES

I. THE UNKNOWN QUANTITIES

1

General Procedure

THE work connected with the unraveling of a cipher system or a cryptogram is divided in three distinctive phases. The first, the least attractive, consists in preparing such statistics of the crypto-elements as will allow the analyst to form some opinions as to the type and the probable language of the cipher.[1] It is a long, monotonous and grinding operation. To the person operating alone it is decidedly a bore and it robs him of much valuable time. In well organized cryptographic departments this work is assigned to various clerks specially trained for the purpose.

The second phase consists in determining, from a study of the statistical material previously prepared, and from the general appearance of the cryptogram itself, the best method of attacking it. It is the most technical phase of the three. It demands of the decryptor his greatest powers of concentration, the clearest lucidity of mind and the full application of his ingenuity, alertness and industry. The pursuit of his objective is a most taxing, feverish, relentless and, yes.....thrilling venture. His is the task of ramming at the outer defences of the cipher, incessantly, until a breach has been opened. Most of the time he is groping in the deepest night. Now and again a little flicker of light gleams across the darkness, tantalizing him with a glimpse of a path. Hopefully he dashes to it only to find him-

[1] In our case we know that the cryptogram is in French and that it is a superciphered one, that it is a substitution and a transposition combined. Researches tending to discover these known facts are unnecessary here.

self in another labyrinth. His knowledge that night is inevitably followed by day keeps his waning courage up, and he steers his course towards where the morning sun is soon to appear. Except that sometimes he is engulfed in an interminable polar night.

The third and final phase is the most attractive. Its purpose after establishing an entering wedge is to prosecute the initial success until the defense collapses completely. Good logic and patience are sufficient for this task. The moment a fragment of the cipher, however small, is satisfactorily determined, its knowledge is immediately put to use for the discovery of other fragments. And so on, until the end.

2

The "Petite Modification"

Bazeries, in the second of his communications, warned the General Staff that he had not said the last word about the system. "*Une petite modification*" (line 138) he had in mind would, when applied, make the system safe. His last cryptogram had been ciphered with the system so modified.

We never took the *singleness* of the modification too seriously. We argued that *one* modification alone would not change the system to an appreciable degree. And having lived with the French for quite a span of our early life, we set Bazeries' statement as a . . . euphemism.

Let us see what kind of modifications he could have brought to the system to make it different from the one he had thought "*imprudent*" to have set down in writing. They are all possibilities: they are our unknown factors:

1. Indicatory Elements:

   a) These need not be necessarily placed at the beginning of a cryptogram. A group *after* a prearranged letter is generally devoted to this purpose, for instance: the fifth, the twelfth, etc. Sometimes its position is linked with the date of the cryptogram. It could be so many letters from the end, etc. Surely a wide selection of schemes is available.

   b) Are the indicatory elements still two in number or have they been increased? We thought that a large

number, derived from a group of three elements, would yield a more incoherent alphabet.

2. Key-word: a) Would the values associated with the indicatory letters be the ones derived from a normal alphabet as first prescribed, or would a reverse alphabet be used or a straight alphabet beginning with a specific letter?

3. Crypto-square: a) Would the incoherent alphabet derived from the key-word be set down in the crypto-square as originally specified, that is horizontally, or would any of the following possible diagrams be followed?

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

I. Straight Horizontal

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

II. Alternate Horizontal

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

III. Straight Vertical

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

IV. Alternate Vertical

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

V. Upward Simple Diagonal

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

VI. Upward Alternate Diagonal

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

VII. Downward Simple Diagonal

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

VIII. Downward Alternate Diagonal

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

IX. Clockwise

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

X. Counter Clockwise

b) Would the alphabet begin at the upper left hand case or would any of the other three corner cases be selected?

4. Clear-square: Same observations made for the crypto-square.

5. Transposition: a) Would the *trigram* transpositional scheme be kept or would the number of elements in the groups be increased?

b) Would the groups be always the same, that is periodic, or would a cyclic period such as 3.5.4.6., 3.5.4.6., etc., be used?

6. Nulls: Would the same scheme for introducing nulls be preserved or would another plan be devised?

As we can well see, we are confronted with quite a number of possi-

bilities, enough to disconcert the lukewarm type of analyst. But we know that a great many difficulties are more formidable in appearance than in reality. Why, then, become unduly alarmed?

II. PREPARATORY STATISTICS

1

Linguistic Characteristics of the French Language

We will now give the more important characteristics of the elements of French:

A: The normal average frequencies of the alphabetic elements of any language, as given by various authors, differ in some respects. It is due to the type of texts used in the analysis and to their length. For instance, if we were to take a frequency count of the text of one of of Napoleon's addresses to his armies, we should get an inordinately high percentage of "Z" due to the large number of verbs, in the second person plural, that such text would contain. Still "Z" in French, is, otherwise, a rare letter. It is also clear that the frequencies derived from short text are apt to be jumpy, awkward—in short, less conclusive than those obtained from a very long text where the affectations of the language have an opportunity to spread more evenly.

As given by the various authors, the frequencies of the letters of the French language as derived by them from texts of different lengths are:

Authors	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
Valerio[1]	7^{72}	0^{90}	3^{58}	4^{68}	17	1^{12}	0^{07}	0^{66}	6^{63}	0^{03}	0^{001}	4^{39}	3	8^{67}	6^{60}	2^{68}	0^{07}	6^{38}	6^{88}	6^{71}	6^{71}	1^{18}	0^{001}	0^{06}	0^{03}	0^{03}
DeViaris[2]	8^{67}	0^{08}	3^{32}	4	16^{59}	1	0^{09}	0^{07}	8^{31}	0^{06}	0	6^{41}	2^{77}	7^{72}	5^{38}	3	1^{13}	7^{45}	7^{77}	6^{88}	5^{58}	1^{18}	0	0^{03}	0^{01}	0^{01}
Sacco[3]	8	0^{8}	3^{2}	4^{4}	17^{8}	1^{2}	1	0^{6}	6^{9}	0^{2}	0	6^{1}	2^{7}	7^{7}	5^{8}	2^{8}	1	6^{6}	7^{8}	7^{1}	6^{3}	1^{6}	0	0^{4}	0^{2}	0^{06}

Fig. 1—*Average Frequency Table of French*

[1] Valerio (P.) *De la Cryptographie*, L. Baudoin, Paris, 1893. Givierge (Général M.), *Cours de Cryptographie*, Paris, 1936, adopts Valerio's frequencies.
[2] Viaris (Marquis de) *Cryptographie*, Paris, 1888.
[3] Sacco (Generale Luigi) *Manuale di Crittografia*, Roma 1936—XIV.

In our analysis we shall follow Sacco's percentages, they being the newest and, presumably, the most correct.

B: For those who like graphs, these frequencies appear as follows:

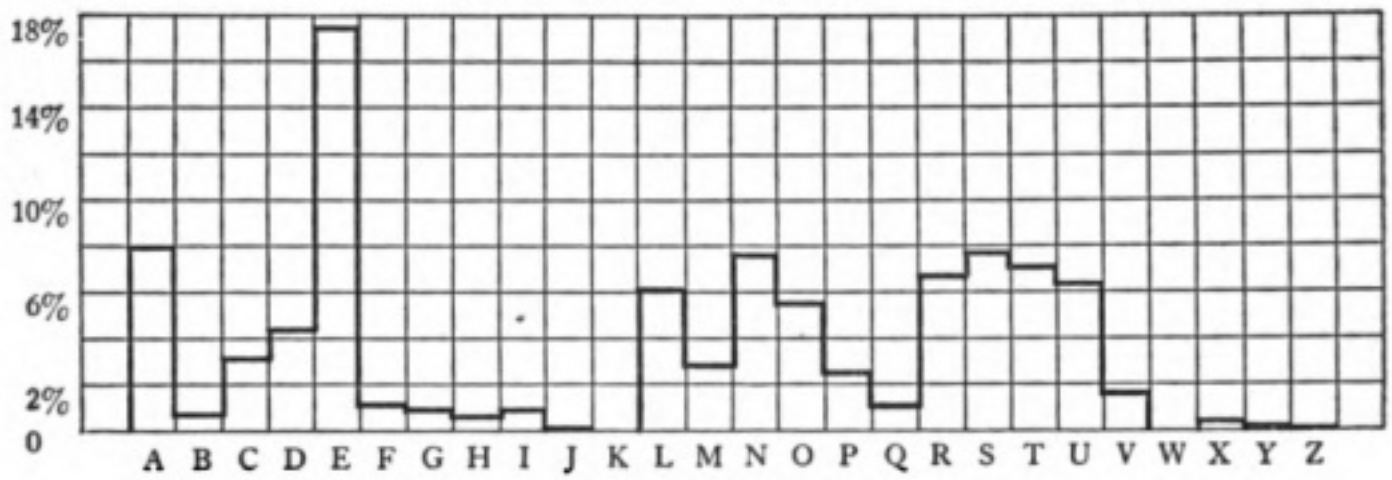


Fig. 2—*Graph of French Average Frequencies* (*Sacco*)

C: Sacco's frequencies, in descending order, from the element having the highest average to the one having the lowest, are:

E	A	S	N	T	I	R	U	L	O	D	C	M	P	V	F	Q	G	B	H	X	J	Y	Z	K	W
17^{5}	8	7^{8}	7^{7}	7^{1}	6^{9}	6^{8}	6^{3}	6^{1}	5^{5}	4^{4}	3^{2}	2^{7}	2^{5}	1^{6}	1^{2}	1	1	0^{8}	0^{6}	0^{4}	0^{3}	0^{2}	0^{06}	0	0

Fig. 3—*Average Arranged Frequency Table of French* (*Sacco*)

D: The graph for the frequencies so arranged looks as follows:

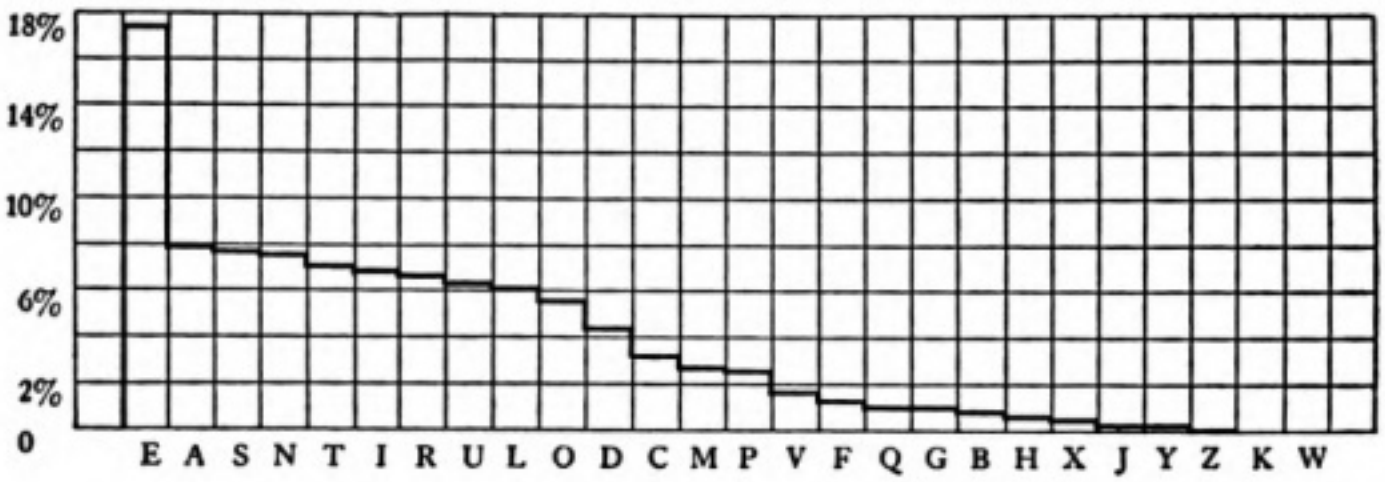


Fig. 4—*Graph of French Arranged Frequencies*

E: The most frequent bigrams are: ES, EN, LE, DE, ON, OU, NT, RE, NE, SE, EL, AI, TE, LA, IT, ER, ED, QU, ME, EM, AN, ET, EU, etc.

F: The most frequent trigrams are: ENT, EDE, LES, QUE, LLE, AIT, EME, ION, EUR, MEN, NTE, TIO, EST, DEL, TER, ONS, QUI, DES, etc.

G: The pilot-elements are: Q, always followed by U, in turn always followed by a vowel.
X, usually preceded by U.
H, frequently a part of the trigram CHE.
Z, frequently preceded by E in the verbal termination EZ.

H: In general, not more than 5 consonants will follow each other, nor more than 4 vowels.

I: The vowels add to about 44% of the elements of any text; they very rarely double except E.

J: The letter E, the most preponderant, rarely associates with other vowels.

K: A high frequency element, not E, if often doubled, is a consonant, generally L, or S, or N.

2

Statistics of the Cryptogram

For the sake of ready reference we shall write the cryptogram continuously, without any break, and give an ordinal number to every fifth

letter; so that, when we mention P-3 or F-12 we will mean, "P" the third letter of the cryptogram; "F" the twelfth one.

```
  1     5     10    15    20    25    30
  L M P C X B R L S Q H F M H H C B H K X C M S H Q B C U P M C C V

 35    40    45    50    55    60    65
F S A K F L N V G S R X F C V B R S N X F T K K R R N D D Q G H Q X N

 70    75    80    85    90    95   100
L M H F S V K R F S N I C R V K B A K V G N V C S G C N R S M M C H P B

105   110   115   120   125   130   135
K H F Q U C F U N X R V I G V T K H K R O D N R N B M R K F G G N C

 140   145   150   155   160   165   170
M C K S V H N G S G C U R K G N V K D D Q V R K O N B N L G Q T S N K

 175   180   185   190   195   200   205   210
I C V U K B V I G F G C Z F H U C H S A M N U C X F F V F C R H K B F V C

       215
X N H G Q
```

Fig. 5—*The Cryptogram*

We shall now prepare a frequency table of the elements in the cryptogram. We usually prefer one with affixes generally known as *trigraphic frequency table*. While it requires a little more work than the other types of tables, it is generally a more informative one.

Crypto-Element	Affixes					Total	Frequency
A	S B S K K M					3	1[4]
B	X C Q V K R H C R A	P N N K K K M N V F				10	4[9]
C	P H X B M X B M U C	C F I V G V V R S N	M U N M G H F M K U	I G U U F V Z H X R	V X	21	10
D	N D O K D D Q N D Q					5	2[3]
E						0	—
F	H V K X X M S L C T	H R H C K S S Q U G	G Z X F V G H F V C	B V		16	7[4]

Crypto-Element	Affixes					Total	Frequency
G	V Q V S I S H N C V	F G N S K G N S C N	L I F H Q F C Q			14	6^{5}
H	Q M H B S F H C K Q	G M C K K Q F P F K	V F C R N N U S K G			15	7
I	N V K V C G C G					4	1^{8}
J						0	—
K	H A T K V X F K R R	V A B T H B V H H R	R C R V R F S G D O	N U H I B B		18	8^{3}
L	– R F N N M S N M G					5	2^{3}
M	L F C P L P H S C H	S M B C A M C R C N				10	4^{8}
N	L S R X S V X D L I	G C U D R V R X R B	G H G O B C G V B L	S M X K U H		18	8^{3}
O	R K D N					2	1
P	M U H C M B					3	1^{4}
Q	S H D H F H B G X U	D G G V T —				8	3^{7}
R	B S B K R L X S R N	K C N X K F V S V O	N M U V C N K K K H			15	7
S	L M F G R Q H A R N	F F C R K V N G M V	G T H G N A			13	6
T	F V Q K K S					3	1^{4}
U	C Q F C V P C N R K	H N C C				7	3^{2}
V	C N C S R F G B K K	K N R G S G C I T H	N Q C B F K R U I F	F C		16	7^{4}
X	C K R N Q B C F F N	N C C R F N				8	3^{7}
Z	C F					1	0^{8}
			Totals.....			215	99^{8}

Fig. 6—*Cryptogram's Frequencies with Affixes*

The examination of this table disclosed the astonishing fact that the highest frequency of any element is 10% for "C," while the frequency of clear-E usually lies within the range of 15%–20%. We were sure, however, that the cryptogram was a transposed mono-alphabetic substitution and consequently, the frequencies of the crypto-elements must, as nearly as possible, be close to the clear-frequencies of the French language.

We could reach the only possible conclusion: **the letter E had been diluted** and that probably more than one crypto-element had been used to cipher it.

A comparison of the two sets of frequencies—Fig. 1 and Fig. 6—confirmed the conclusion by revealing that in the crypto-frequencies, the high frequency group had apparently one more member in it than the clear-frequencies. Otherwise, considering the presence of nulls in the cryptogram, the other frequencies were found to be within their proper respective range.

	HIGH										LOW								RARE						
French Clear	**E**	**A**	**S**	**N**	**T**	**I**	**R**	**U**	**L**	**O**	**D**	**C**	**M**	**P**	**V**	**F**	**Q**	**G**	**B**	**H**	**X**	**J**	**Y**	**Z**	**K**
Frequencies	17^5	8	7^8	7^7	7^1	6^9	6^6	6^3	6^1	5^6	4^4	3^3	2^7	2^5	1^6	1^2	1	1	0^8	0^8	0^4	0^3	0^3	0^{06}	O
Cryptogram's	C	K	N	F	V	H	R	G	S		M	B	Q	X	U	D	L	I	A	P	T	O	Z	E	J	Y
Frequencies	10	8^3	8^3	7^4	7^4	7	7	6^4	6		4^6	4^4	3^7	3^7	3^3	2^3	2^3	1^8	1^4	1^4	1^4	1	0^6	0	0	0

Fig. 7—*Comparative Frequencies*

The second fact that emerged from the examination was that the cryptogram contained very few vowels, that is 3-A, no E, 4-I, no O, 7-U and no Y, disclosing by their paucity that Bazeries had abandoned his original scheme of nulls which, as we remember, consisted of introducing vowel-nulls in front of groups beginning with a vowel.

III. DIVERSE APPROACHES

The general reader is not sufficiently interested in the momentary tribulations besetting an analyst. We will not, therefore, record here the numerous essays that were tried.

Some were abandoned for lack of sufficient material to continue the investigation further. Some were abandoned temporarily, with the reservation of reverting to them if a quest for a simpler treatment should prove

fruitless. Still others led to perfectly blank walls.

For the benefit of the younger cipher students, we will report them in Chapter VI, even though, in a way, they represent failures. But we feel no sense of humiliation in baring our failures; it is through them that ultimate success is attained. On the other hand, it is possible that one or two of them, if prosecuted with energy, might lead to the solution just the same. Some enterprising neophyte can continue them from where we left off.

Still, we must confess that the too frequent setbacks we had received at the hands of the cryptogram annoyed us; they annoyed us considerably. Perhaps Bazeries was right; his cipher was proving invincible. Thus far we had gotten the worst of any effort at unmasking we had advanced; the cryptogram had presented a stout defense and given a splendid account of itself.

We had exhausted all the ordinary leads at our disposal, commonly used for the solution of ciphers of this type.

What was there to do next? Excuse our failure on the familiar grounds that the cryptogram was not long enough for a successful investigation or go back to some of the unfinished analyses and try over again?

The perspective was not alluring.

We objected to the trial and error methods in conjunction with our previous work, still left open to us. This procedure had never held for us any particular predilection, and even at this juncture it did not have any attraction for us. Preposterous. And then, besides, what for? We were not interested in the secret meaning of the cryptogram, *per sè*; we were seeking a method of decrypting, one that could be applied quickly to ciphers of this nature.

We roamed far and wide.

The germ of an idea made its appearance, weakly at first, but assuming a shape more and more definite as it emerged.

We wondered. Could it be possible?

Chapter V

THE FINAL ATTACK

I. A FUNDAMENTAL WEAKNESS

1

The Myth of "Safety in Variation"

We decided to approach the problem by attempting the reconstitution of the ciphering alphabet on the theory that Bazeries' concept of a message bearing its own key, worthy as it really is, presents a fundamental weakness: the key-word with which the ciphering alphabet is to be composed consists of the name of a numeral.

Now, while it is true that the series of integers is infinite, it is equally true that, in any language, only a few words are required to denote all the elements of our number system. In fact, in languages we are familiar with, all that is needed is a short series of different words to denote the *unit numbers*, a few others for the series bounded by *ten* and *twenty*, another short series of words to denote the *units of tens*—in most languages derived from the unit series and preserving the same roots—and the words for *hundred*, *thousand*, *million*, *billion*, etc.

Was Bazeries aware of the fact that the endless immensity of numbers, could, for the purpose of decrypting, be reduced to a mere handful of basic forms? And that his objective—"safety in variation"—would prove ephemeral? We do not think so. As was the case with his cylindrical cryptograph, these very possibilities of variations and permutations, often ex-

pressed in astounding terms[1] would lay bare the unprotected ramparts of the cipher's defense.[2]

The detection of this fundamental weakness provided the entering wedge that finally led to the breaking of this interesting cipher.

2

Notation

For the sake of brevity, but principally to avoid repetitious phrases and concepts which in an exposition of this kind must, of necessity, be fairly numerous, we wish to resort to an easy symbolism which,[3] while mathematical in appearance, does not inject into our discussion mathematical operations of any kind.

We shall adopt the following notation.

1. A ciphering transformation will be indicated with the symbol (τ).
2. A deciphering transformation will be indicated with the symbol (τ^{-1}); (τ) and (τ^{-1}) are inverse operations.
3. The symbols $(\tau)\text{A}\rightarrow\text{N}$ and $(\tau^{-1})\text{N}\rightarrow\text{A}$, will be read: the ciphering of A yields N and the deciphering of N yields A, respectively.
4. The symbols $\text{A} \equiv \text{N}$ and $\text{B} \not\equiv \text{M}$ will be read: A coincides with N, and B does not coincide with M, respectively. Also: A can be assumed to coincide with N, or B cannot be made to coincide with M.
5. The symbols *clear* $\frac{-\text{A}}{8}$ and *crypto* $\frac{-\text{N}}{1^2}$ will simply mean that the element A of the clear message has an average frequency of 8% in the language

[1] To what an extent Bazeries relied on permutations can be judged by reading these two excerpts from his *Les chiffres secrets dévoilés;* the one awe-inspiring, the other a curious and unconvincing argument. Page 250: "The number of interchangeable alphabets being 20, the number of combinations is given by the formula . . . $1 \times 2 \times 3 \times \ldots \times 18 \times 19 \times 20$ = TWO QUINTILLIONS, in round numbers, that is the number 2 followed by 18 zeros; *c'est inimaginable, mais cela est.*" And we add, it sounds very final.

Pg. 251: "A safe having 4 alphabets of 25 letters gives as a number of combinations, 25 raised to 4th power = 390,625. In comparing the safety of the safe to that of the cylindrical cryptograph, the reader can easily ascertain that it is 5 trillion times easier to open the safe of which we do not know the combination than to decipher a cryptogram made with the cylindrical cryptograph, of which we do not know the key-word."

[2] "The degree of safety possessed by a cipher system is not dependent upon any theoretical calculations nor upon its complications . . . . . there are systems possessing permutative possibilities that can be expressed in millions and billions which, nevertheless, can be solved in a few hours—often less—in a purely mechanical way." Yves Gyldén: *Chifferbyråernas Insatser I Världskriget Till Lands.* (Stockholm, 1931.)

[3] . . . . . "by the aid of symbolism we can make transitions in reasoning almost mechanical by the eye which otherwise would call into play the higher faculties of the brain." A. N. Whitehead: *An Introduction to Mathematics.* (Henry Holt & Co., New York, 1911.)

(French in our case) and that the element N of the cryptogram has a frequency of 1.2% in the cryptogram, respectively.

6. Salient facts or conclusions derived from the analysis, to which we must often refer, will be given the appellation of PROPOSITIONS and will be abbreviated as Pp., followed by a Roman numeral, the whole in square brackets.
7. On the other hand, salient pseudo-equations, of the type shown in 3 and 4 above, will be simply followed by an Arabic numeral in square brackets.
8. Such phrases as *crypto-row-one*, *clear-row-five*, etc. will mean: the first row of the crypto-square, the fifth row of the clear-square, etc.
9. The phrase *key-word-numeral*, that is, the name of the numeral with which the key word is formed, will be abbreviated as, **kwn**.

3

French Numerals

Some of our readers may not be acquainted with the French numerals. Others may wish to brush up their knowledge of the rules of cardinal number formation. The following table and the few notes appended to it are sufficient for the purpose.

TABLE I: FRENCH NUMERALS

1 un, une	17 dix-sept	77 soixante-dix-sept
2 deux	18 dix-huit	80 quatre-vingts
3 trois	19 dix-neuf	81 quatre-vingt-un
4 quatre	20 vingt	82 quatre-vingt-deux
5 cinq	21 vingt et un	90 quatre-vingt-dix
6 six	22 vingt-deux	91 quatre-vingt-onze
7 sept	23 vingt-trois	100 cent
8 huit	30 trente	101 cent un
9 neuf	31 trente et un	136 cent trente-six
10 dix	32 trente-deux	200 deux cents
11 onze	40 quarante	207 deux cent sept
12 douze	50 cinquante	1000 mille
13 treize	60 soixante	1014 mille quatorze
14 quatorze	70 soixante-dix	1500 mille cinq cents
15 quinze	71 soixante et onze	1937 mille neuf cent trente-sept
16 seize	72 soixante-douze	2000 deux mille
		1000000 un million

NOTES: I) Numbers less than 100 containing more than one word have a connective, *always:*

a) In 21, 31, 41, 61, and 71 *only*, it is the conjunction ET;

b) elsewhere it is the hyphen, (-).

II) Numerals are invariable as regards *gender* except UN which becomes UNE when preceding feminine nouns.

III) Numerals are also invariable as regards *number*, except VINGT and CENT which are made plural when multiplied, if no other number follows. Compare 80 and 81, 200 and 207. Compare also 1000 and 2000.

A close examination of the above table reveals that:

Basic Forms of French Numerals

Let us remind our readers that the ciphering alphabet of this system is to be written out horizontally in a square containing twenty-five cases, five cases to each side of the square.[1]

If we could determine with accuracy the elements in the five cases of the first row which, as we are aware, represent the first five letters of the **kwn.**, we should go a long way towards the reconstitution of the ciphering alphabet.

On the other hand, the **kwn.** is, supposedly, to be derived from two indicatory letters in the cryptogram, each having a numerical equivalence varying from 1 to 25 according to their rank in the normal alphabet. Thus the **kwn.** might contain either two or three or four digits. But since Bazeries warned us of having introduced a *petite modification* in the system, we may assume that he had modified this prescription and used three letters instead of two

[1] Of course, Bazeries might have used any of the squares illustrated in Chapter IV, 2, #3, which would be tried, one by one, should the square under consideration fail to give concrete results.

to form the key, with the result that the number of digits in the key could also be five or six. At most, this assumption, should it prove unfounded, will lengthen our mechanical work a little more.

Let us, therefore, tabulate all the possible *initial pentagrams* of *all* numbers with two, three, four, five and six digits. It is easily accomplished with the help of Table I and by keeping in mind that repeated elements must be eliminated.[1]

Two digit numbers must begin with:

Form	1	ONZE·	for 11.
	2	DOUZE	12.
	3	TREIZ	13.
	4	QUATO	14.
	5	QUINZ	15.
	6	SEIZ·	16.
	7	DIXSE	17.
	8	HU	18.
	9	NE	19.
	10	VINGT	20–29.
	11	TREN·	30.
	12	U	31, 39.
	13	D	32.
	14	O	33.
	15	Q	34.
	16	C	35.
	17	S	36, 37.
	18	H	38.
	19	QUARN	40–49.
	20	CINQU	50–59.
	21	SOIXA	60–79.
	22	QUATR	80–99.

Three digit numbers must begin with:

Form	23	CENT·	for 100.
	24	U	101.
	25	D	102, 110, 112, 117–119.
	26	R	103, 113, 130–139.
	27	Q	104, 114, 115, 140–149, 180–199.
	28	I	105, 150–159.
	29	S	106, 107, 116, 160–179.
	30	H	108.
	31	N	109.
	32	O	111.
	33	V	120–129.
	34	DEUXC	200–299.

[1] In forms shorter than pentagrams the lacking elements have been replaced with dots; in the right hand column, pairs of numbers connected with a hyphen include all the numbers of the natural series intervening between them as limits. The full series between 11 and 999.999 is represented—the reader can follow the numbers one by one if he wishes to do so.

35	TROIS	300–399.
(22)	QUATR	400–499.
36	CINQE	500–599.
37	SIXCE	600–699.
38	SEPTC	700–799.
39	HUITC	800–899.
40	NEUFC	900–999.

Four digit numbers must begin with:

Form 41	MILE·	for	1000.
42	U		1001.
43	D		1002, 1010, 1012, 1017–19.
44	T		1003, 1013, 1030–39.
45	Q		1004, 1014, 1015, 1040–49, 1080–99.
46	C		1005, 1050–59.
47	S		1006, 1007, 1016, 1060–79.
48	H		1008.
49	N		1009.
50	O		1011.
51	V		1020–29.
52	DEUXM		2000–2999.
(35)	TROIS		3000–3999.
(22)	QUATR		4000–4999.
53	CINQM		5000–5999.
54	SIXML		6000–6999.
55	SEPTM		7000–7999.
56	HUITM		8000–8999.
57	NEUFM		9000–9999.

Five digit numbers must begin with:

Form 58	DIXML	for	10,000–10,999.
59	ONZEM		11,000–11,999.
			12,000–12,999: use form (2)
			13,000–13,999: " " (3)
			14,000–14,999: " " (4)
			15,000–15,999: " " (5)
60	SEIZM		16,000–16,999.
			17,000–17,999: use form (7)
			18,000–18,999: " " (8)
			19,000–19,999: " " (9)
			20,000–29,999: " " (10)
61	TRENM		30,000–39,999.
		from	40,000–99,999. forms (19), (20), (21), (22) will be used appropriately.

Six digit numbers must begin with:

Form 62	CENTM	for 100,000–100,999.

From 101,000 to 999,999 the appropriate forms from (34) to (40) will be used.

We will now prepare a more condensed table, classifying the 62 forms thus obtained in three groups: those beginning with elements of low frequency, (H, Q, V); those beginning with letters of middle frequency, (C, D, M); and finally those beginning with high frequency elements, (N, O, S, T). The forms in each group have been arranged alphabetically, and similar groups have been sub-classed.

TABLE II. BASIC FORMS OF FRENCH NUMERALS

GROUP I

I	HUITC	(39)
	M	(56)
II	QUARN	(19)
	TO	(4)
	TR	(22)
III:	QUINZ	(5)
IV:	VINGT	(10)

GROUP II

V	CENT·	(23)
	D	(25)
	H	(30)
	I	(28)
	M	(62)
	N	(31)
	O	(32)
	Q	(27)
	R	(26)
	S	(29)
	U	(24)
	V	(33)
VI	CINQE	(36)
	M	(53)
	U	(20)
VII	DEUXC	(34)
	M	(52)
VIII	DIXHU	(8)
	ML	(58)
	NE	(9)
	SE	(7)
IX:	DOUZE	(2)
X	MILE·	(41)
	C	(46)
	D	(43)
	H	(48)
	N	(49)
	O	(50)
	Q	(45)
	S	(47)
	T	(44)
	U	(42)
	V	(51)

GROUP III

XI	NEUFC	(40)
	M	(57)
XII	ONZE·	(1)
	M	(59)
XIII	SEIZ·	(6)
	M	(60)
XIV	SEPTC	(38)
	M	(55)
XV	SIXCE	(37)
	ML	(54)
XVI:	SOIXA	(21)
XVII	TREIZ	(3)
	N·	(11)
	NC	(16)
	ND	(13)
	NH	(18)
	NM	(61)
	NO	(14)
	NQ	(15)
	NS	(17)
	NU	(12)
XVIII:	TROIS	(35)

II. THE RECONSTITUTION OF THE CIPHERING ALPHABET

1

A Preliminary Assumption

We have seen that the clear-alphabet of Bazeries' cipher is a normal

one, written down vertically, column by column, a letter in each cell, in the 25 cells of a square of five.

We have also seen that, without any doubt, the cipher must contain a rule prescribing the diluting of the very high frequency of clear-E. If so, the clear-square *must* contain 2 cases filled with "E."

The question now arises: which case in the square is filled with the second representation of "E," or to put it the other way around: which clear element of the alphabet is being sacrificed to make room for a second representation of "E"?

The letter K, in French, is very rare; the two score or so words in which it appears are mostly of foreign origin. Its elimination, for the purpose on hand, should seem logical. In case of need, any word like *Képi*, *Kilo*, etc., could easily be spelled *quépi*, *quilo*, etc., without any misunderstanding arising therefrom.

We will adopt this assumption.[1]

Hence it will be:

$$\text{crypto-K} \equiv \text{clear-E} \qquad [1]$$

By calling E_1 and E_2 the double representation of clear-E, the clear-square will then become:

A	F	E_2	P	U
B	G	L	Q	V
C	H	M	R	X
D	I	N	S	Y
E_1	J	O	T	Z

Fig. 8—*Clear-square*

where E_2 has been inserted in the third case of the first row, customarily occupied by "K."

As a consequence of this important assumption, one of the two letters "E" in the above square MUST represent crypto-K, that is

$$\left.\begin{array}{ll} \text{either} & (\tau)\ E_1 \longrightarrow K \\ \text{or} & (\tau)\ E_2 \longrightarrow K \end{array}\right\} \qquad [2]$$

[1] The French usually sacrifice this element when a similar need arises: there is nothing original in our assumption.

Now, we know that the ciphering alphabet is written out horizontally in a similar square of 25 cases and is composed of two parts: the first, containing a single representation of all the elements in the **kwn.**, in the order in which they appear in the **kwn.**; the second, containing the unused elements of the alphabet, in alphabetical order.

But by [Pp. I] "K" cannot be an element of any French numeral and clear-E_2, the third element of the first row must correspond to an element of **kwn.** Therefore, clear-$E_2 \not\equiv$ crypto-K. But by [2] either E_1 or E_3 must coincide with crypto-K.

Hence it will be:

$$(\tau)\ E_1 \longrightarrow K \qquad [3]$$

and crypto-K will consequently be located in the crypto-square in the corresponding case occupied by clear-E_1 in the clear-square, that is, the first case of the fifth row.

2

The Recovery

To facilitate the reading of the analysis leading to the recovery of the ciphering alphabet, let us prepare an additional table composed of twin squares, the one on the left showing the clear-alphabet with the $K \equiv E_1$ assumption and the one on the right showing the normal frequencies of the alphabetical elements of the French language taken from the first line of Fig. 7: elements and their frequencies in corresponding cases. From this point, we shall abandon the notations E_1 and E_2: no confusion will arise in view of [3].

TABLE III. TWIN CLEAR ALPHABET

A	F	E	P	U	8	1^2	17^5	2^5	6^3
B	G	L	Q	V	0^8	1	6^1	1	1^6
C	H	M	R	X	3^2	0^8	2^7	6^6	0^4
D	I	N	S	Y	4^4	6^9	7^7	7^8	0^2
E	J	O	T	Z	17^5	0^2	5^6	7^1	0^{06}

Tables II, III; Pp. I to VI; and Fig. 7 are all we shall need to follow the analysis. For the sake of convenience they have all been printed on loose sheets which will be found at the end of the book together with other useful material.

We shall now proceed methodically, step by step.

Step I:

By equation [3] we have located crypto-K in the crypto-square. By [Pp. I] "J" and "K" cannot be a part of the **kwn.** But "J" and "K" are adjacent to each other in the normal alphabet and since both cannot be a part of the **kwn.**, it follows that they *must* be also adjacent to each other in the crypto-alphabet. The frequencies crypto $\frac{\text{-J}}{0} \equiv$ clear $\frac{\text{-Y}}{0^2}$ confirm it. It will then be:

$$(\tau^{-1})\ \text{J} \longrightarrow \text{Y} \qquad [4]$$

Therefore, rows four and five of the two squares will look as follows:

row (4)	.	.	.	.	J		D	I	N	S	Y	4^4	6^9	7^7	7^8
row (5)	K	.	.	.	.		E	J	O	T	Z		0^2	5^5	7^1	0^{06}

Crypto-square — Clear-square

Step II:

The first letter of the clear-alphabet, that is "A," is, in French, a very frequent element. Its frequency is approximately 8%. Its crypto-equivalent, that is, the initial of the **kwn.**, must be found among the elements of the cryptogram bearing high frequency ratios. The crypto-element with comparable frequencies are

$$\text{crypto } \frac{\text{-C}}{10'}\ \frac{\text{-K}}{8^3'}\ \frac{\text{-N}}{8^3'}\ \frac{\text{-F}}{7^4'}\ \frac{\text{-V}}{7^4'}\ \frac{\text{-H}}{7'}\ \frac{\text{-R}}{7}$$

The frequency range from 7% to 10% can safely be admitted on the score that variations from any average language frequency are bound to take place in a short cryptogram.

From them we can immediately eliminate crypto-K because of [Pp. I] and also because it has already been individualized in [3]. We readily eliminate crypto-F and crypto-R for the simple reason that they cannot be the

initials of any French numeral, [Pp. VI]. This leaves for examination the elements:

$$\text{crypto } \frac{\text{-C}}{10},\ \frac{\text{-N}}{8^3},\ \frac{\text{-V}}{7^4},\ \frac{\text{-H}}{7}$$

Step III:

We will now prove that:

a) clear $\frac{\text{-A}}{8} \not\equiv$ crypto $\frac{\text{-N}}{8^3}$

b) clear $\frac{\text{-A}}{8} \not\equiv$ crypto $\frac{\text{-V}}{7^4}$

c) clear $\frac{\text{-A}}{8} \not\equiv$ crypto $\frac{\text{-H}}{7}$

a) The crypto-frequencies of Forms XI–40 and XI–57, the only two beginning with "N," when juxtaposed to the normal frequencies of the elements in clear-row-one, that is:

XI–40:	N	E	U	F	C	and	XI–57:	N	E	U	F	M
	8^3	0	3^3	7^4	10			8^3	0	3^3	7^4	4^6
	A	F	E	P	U			A	F	E	P	U
	8	1^2	17^4	2^5	6^3			8	1^2	17^4	2^5	6^3

cannot be made to coincide perfectly. In fact, the fourth element alone in each, that is:

$$\text{crypto } \frac{\text{-F}}{7^4} \not\equiv \text{clear } \frac{\text{-P}}{2^5}$$

is sufficient to rule the combination out: the message could not contain such a high proportion of clear-P elements.

b) Similarly, Form IV–10, the only one beginning with "V":

Form IV–10:	V	I	N	G	T
	7^4	1^2	8^3	6^5	1^4
	A	F	E	P	U
	8	1^2	17^4	2^5	6^3

shows, by the same argument used above, that the 4th and 5th elements cannot be made to coincide and the combination must be rejected.

c) The crypto-frequencies of Forms I–39 and I–56, the only ones beginning with "H," similarly juxtaposed to clear-row-one:

I-39:	H	U	I	T	C
	7	3^3	1^8	1^4	10
	A	**F**	**E**	**P**	**U**
	8	1^2	17^5	2^5	6^3

and

I-56:	H	U	I	T	M
	7	3^3	1^8	1^4	4^6
	A	**F**	**E**	**P**	**U**
	8	1^2	17^5	2^5	6^3

show, through the third element in each, that the dilution of the clear E-element-frequency—an important defence of the cipher—would have been meaningless if so small a percentage, namely: 1.8% of the E-elements, had been so diluted. A clinching argument against this possibility is the fact that 1.8% added to the frequency of crypto-K, 8.3%, which by equation [3] coincides with clear-E, would give us a total frequency of 10.1% for the E-elements against a normal frequency of 17.5%—too large a difference for even a remote possibility.

Step IV:

On the other hand, let us consider the various forms in classes V and VI, the ones beginning with "C." These two classes are fairly dense. To narrow down the analysis we will momentarily take into account only the first four elements of the forms in these classes which are common to all. If we, as usual, juxtapose them to the first four elements of clear-row-one, we will obtain acceptable equivalences:

V-(common):	$\overset{*}{C}$	E	$\overset{*}{N}$	T
	10	0	8^3	1^4
	A	**F**	**E**	**P**
	8	1^2	17^5	2^5

VI-(common):	$\overset{*}{C}$	I	$\overset{*}{N}$	Q
	10	1^8	8^3	3^7
	A	**F**	**E**	**P**
	8	1^2	17^5	2^5

In fact, crypto $\frac{\text{-C}}{10}$. ≡ clear $\frac{\text{-A}}{8}$: they are in the same frequency range—10% frequency for clear-A, slightly higher than normal, can be explained by the presence of nulls in the cryptogram—and, crypto $\frac{\text{-N}}{8^3}$ ≡ clear $\frac{\text{-E}}{17^5}$: they showing roughly a 50% dilution of clear-E, which falls in line with a more acceptable usage of the principle of dilution. Moreover, the frequency of crypto-N, 8^3%, added to that of crypto-K, also 8^3%, gives us a total of 16^6%, very close to the 17^5 normal frequency for clear-E, which both crypto-N and crypto-K represent.

Which one of these two combinations is the correct one? We shall investigate this point a little later. Temporarily, let us observe that the first and third elements of each combination are common to both. Thus we can safely say that:

$$(\tau)\ \text{A} \longrightarrow \text{C} \qquad [5]$$
$$\text{and} \quad (\tau)\ \text{E} \longrightarrow \text{N} \qquad [6]$$

Step V:

Our attention will now be turned to clear-row-five:

E	J	O	T	Z
17^{4}	0^{2}	5^{3}	7^{1}	0^{05}

which promises some immediate results.

We will state [Pp. I] in another form:

"NO FRENCH NUMERAL, HOWEVER LARGE, CAN EVER CONTAIN, IN ITS SPELLED-OUT FORM, MORE THAN 21 ELEMENTS OF THE ALPHABET."

So that, if the **kwn.** did make use of all the 21 possible elements it can contain, there would be, at least, four elements and precisely B, J, K, Y, in their alphabetic order—according to the cipher rules—following it, to complete the crypto-square.

By one of those strange and unexplainable coincidences, beautiful to contemplate and fateful in its result, "B" and "Y," the *second* and the *penult* elements of the alphabetic family must, through no fault of their own—other than being symmetrically placed therein—perforce be the betrayers of their brethren. In fact, because of the vagaries of the French language for one thing and the architectural scheme of the cipher delineated by Bazeries for another, they MUST IRREVOCABLY be located in disastrously vulnerable spots: "B" in *first* or *second* position after the key-word-numeral array, depending on whether "A," the *vanguard*, is or is not one of its members and "Y," *mirabile visu*, in *last* or *next to last* position depending on whether "Z," the *rearguard*, is or is not, also, a member of the array.

Of the two, "Y" can be localized immediately.

Step VI:

We affirm that clear-z is an element of the **kwn.**

In fact, if it were not, "Z" would occupy the last case of the crypto-square due to the rule that all the unused elements of the alphabet in the **kwn.** must follow it in an alphabetical order. Consequently crypto-Y would lie in its adjacent case, the penult, for by [Pp. I], "Y" cannot be a part of the **kwn.** We would then have:

.	.	.	Y	Z
			0	0^{5}

Possible Crypto-row-five

E	J	O	T	Z
			7^{1}	0^{06}

Clear-row-five

an absurd result, for it is practically impossible to indite an ordinary French text totaling 215 elements without a single "T" in it.

We conclude, therefore, that crypto-Z is an element of the **kwn.** and that crypto-Y is then the last element of the crypto-square, corresponding to the clear-z, the last element of the clear-square. Hence it will be

$$(\tau^{-1}) \quad \text{Y} \longrightarrow \text{z} \qquad [7]$$

Condensing the findings thus obtained in equations [3], [4], [5], [6] and [7] we will have a better perspective of our fragmentary results.

C	.	N	.	.
.	.	.	.	.
.	.	.	.	.
.	.	.	.	J
K	.	.	.	Y

Crypto-alphabet

A	F	E	P	U	.	1^{2}	.	2^{4}	6^{3}
B	G	L	Q	V	0^{8}	1	6^{1}	1	1^{6}
C	H	M	R	X	3^{2}	0^{6}	2^{7}	6^{5}	0^{4}
D	I	N	S	Y	4^{4}	6^{9}	7^{7}	7^{8}	.
E	J	O	T	Z	.	0^{3}	5^{6}	7^{1}	.

Clear-alphabet

Step VII:

A very interesting subsequence that deserves our attention at this time is $\overline{\text{INS}}$, appearing in clear-row-four:

.	.	.	.	J

Crypto-square

D	I	N	S	Y
4^{4}	6^{9}	7^{7}	7^{8}	.

Clear-square

[8]

composed of three successive elements, bearing quite high frequencies.

Their equivalents in the crypto-alphabet:

a) are located, as we notice in the diagram, immediately ahead of "J," the first of the four elements which—by [Pp. I]—cannot be a part of the **kwn.** The three equivalents are, therefore, some of the unused elements of the alphabet not contained in the **kwn.**
b) more precisely, they can only be elements of the normal alphabet lying between "B" and "J" not used in the **kwn.**, because "B" is the first of the four elements which can never be a part of the **kwn.**
c) They must be, according to rules, elements in alphabetical order.

The crypto-elements from "B" to "J" with their frequencies, excluding "C," which has already been individualized, are:

$$\left|\begin{matrix}B\\4^4\end{matrix}\right|\begin{matrix}D & E & F & G & H & I\\2^3 & 0 & 7^4 & 6^4 & 7 & 1^8\end{matrix}\left|\begin{matrix}J\\\end{matrix}\right| \qquad [9]$$

The only three elements [9] satisfying the frequencies of [8] are F, G and H, with frequencies well within their respective ranges. We therefore conclude that:

$$(\tau)\ \text{F} \longrightarrow \text{I} \qquad [10]$$
$$(\tau)\ \text{G} \longrightarrow \text{N} \qquad [11]$$
$$(\tau)\ \text{H} \longrightarrow \text{S} \qquad [12]$$

Step VIII:

It is safe to conclude also, by a further verification of [9] that clear$\frac{\text{D}}{4^4}$ occupying the first case of clear-row-four cannot be substituted by any other element than crypto$\frac{\text{B}}{4^4}$ lying ahead of crypto-$\overline{\text{FGH}}$ not only because their frequencies are almost identical but also because the frequencies $\frac{\text{D}}{2^3}$ and $\frac{\text{E}}{0}$ are too low for any serious doubt. Hence it is:

$$(\tau)\ \text{D} \longrightarrow \text{B} \qquad [13]$$

which definitely localizes "B," the first of the four elements "B," "J," "K" and "Y" that cannot be a part of the **kwn.**

As a consequence of [13], it could be assumed that "A" is part of the **kwn.**, for, if it were not, "A" should lie in that cell of the crypto-square immediately preceding the one filled with "B," corresponding to "**x**" in

the clear-square. It can be readily seen, by examining their frequencies, that:

$$\text{crypto } \frac{\text{-A}}{3^2} \not\equiv \text{clear } \frac{\text{-X}}{0^4}$$

unless clear-**x** has been used in the text as an equivalent for the punctuation sign (.), that is for "STOP."

Step IX:

By equation [11] crypto-G has been found not to belong to the **kwn.** and by [Pp. II] it can only occur in the number VINGT. By the same [Pp. II] the element "V" can also occur only in the same word. Therefore, crypto-V is not in the **kwn.** and must consequently be located near the end of the crypto-square because "V" is the fourth from the last element of the alphabet. It must, therefore, be equivalent to one of the three elements of clear-row-five $\overline{\underset{0^2}{\text{J}} \quad \underset{5^4}{\text{O}} \quad \underset{7^1}{\text{T}}}$. The frequency of crypto-V is $7^{1}\%$ and it is safe to decide that:

$$(\tau)\ \text{T} \longrightarrow \text{V} \qquad [14]$$

Step X:

At this point it is well that we summarize our results by doing two things:

a) extending the new equivalences found in [10], [11], [12], [13] and [14, in the fragmentary crypto-square:

C	.	N	.	.	A	F	E	P	U	. 1^3 . 2^5 6^3
.	.	.	.	.	B	G	L	Q	V	0^8 1 6^1 1 1^8
.	.	.	.	.	C	H	M	R	X	3^2 0^6 2^7 6^8 0^4
B	F	G	H	J	D	I	N	S	Y	. . . . .
K	.	.	V	Y	E	J	O	T	Z	. 0^2 5^4 . .

Crypto-alphabet — Clear-alphabet

b) stating four corollaries, easily derived from our findings, which will lessen future researches:

1. **The numbers** HUIT, NEUF, **and** VINGT **are not a part of the kwn.** (From equivalences [10], [11], and [12]: "H," "F," "V," and "G" are not in the **kwn.**) [Cor. I]
2. **One of the six numbers** ONZE, DOUZE, TREIZE, QUATORZE, QUINZE **and** SEIZE **must be a part of the kwn.** (From Step VI: "Z" must be in the **kwn.**) [Cor. II]

3. **One of the three numbers** SIX, DIX **and** SOIXANTE **must be a part of the kwn.** In the crypto-square "V" and "Y" occupy adjacent cases leaving no room for "X," which should precede "Y" if it were not in the **kwn.**) [Cor. III]
4. **The kwn. must have 15 elements if** "A" **is one of them, due to the fact that** crypto-B **is in 16th position in the crypto-square. If** "A" **is not an element of the kwn., then the latter will be composed of 14 elements.** [Cor. IV]

Step XI:

Now let us go back to Step IV, where we were left in doubt as to the proper selection between the forms in Class V and Class VI. We shall now extend the elements of each class as far as we can.

In Class VI we have the following forms:

(36) C I N Q E T derived from C I N Q (C) E (N) T . . . . .
(53) C I N Q M L E " " C I N Q M (L) L (L) E . . . .
(20) C I N Q U A T E " " C I N Q U A (N) T E. . . . .

We will quickly dispose of all of them by merely observing wide differences in frequencies:

VI-36	C	I	N	Q	E	T	
					0	1^4	
clear-row 1, 2:	**A**	**F**	**E**	**P**	**U**	**B**	
					6^3	0^8	

VI-20:	C	I	N	Q	U	A	T	E
					3^2	1^4	1^4	0
	A	**F**	**E**	**P**	**U**	**B**	**G**	**L**
					6^3	0^8	1	6^1

VI-53:	C	I	N	Q	M	L	E
					4^6	2^3	0
	A	**F**	**E**	**P**	**U**	**B**	**G**
					6^3	0^8	1

Step XII:

We shall then investigate the possibilities of Form V–23: CENT.

We will prepare a table and follow up CENT with all the possible numbers forming "hundreds of thousands," that is from UN MILLE to DIX-SEPT MILLE and TRENTE MILLE to SOIXANTE-DIX MILLE. (Remember that Cor. I elimi-

nates HUIT, NEUF and VINGT). For the sake of compactness we will group in the lefthand column similar combinations.

	A	F	E	P	U 6^{3}	B 0^{8}	G 1	L 6^{1}	Q 1	V 1^{6}	C 3^{2}	H 0^{6}	M 2^{7}	R 6^{6}	X 0^{4}	
Assumed crypto-equivalents	C	E	N	T												
By adding: UN MIL(L)E					U 3^{2}	M 4^{5}	I 1^{8}	L 2^{3}								Rejected
By adding: DEUX MIL(L)E					D 2^{3}	U 3^{2}	X 3^{7}	M 4^{5}	I 1^{8}	L 2^{3}						Rejected
By adding: TROIS M(I)L(L)E					R 7	O 1	I 1^{8}	S 6	M 4^{5}	L 2^{3}						Rejected
By adding: QU ATRE MILLE / QU ATORZE MILLE / QU INZE MILLE / QU ARANTE					Q 3^{7}	U 3^{2}										Rejected
By adding: CINQ MILLE / CINQ UANTE					I 1^{8}	Q 3^{7}										Rejected
By adding: SIX M(I)L(L)E					S 6	I 1^{8}	X 3^{7}	M 4^{5}	L 2^{3}							Might have some possibilities.
By adding: SEPT MILLE					S 6	P 1^{4}	M 4^{5}	I 1^{8}								Rejected
By adding: D IX MILLE / D OUZE MILLE / D IX-SEPT MILLE					D 2^{3}											Rejected
By adding: O NZE MILLE					O 1											Rejected
By adding: T REIZE M(I)L(L)E					R 7	I 1^{8}	Z 0^{6}	M 4^{5}	L 2^{3}							Might have some possibilities.
By adding: TRENTE MIL(L)E					R 7	M 4^{5}	I 1^{8}	L 2^{3}								Rejected
By adding: SEIZE M(I)L(L)E					S 6	I 1^{8}	Z 0^{6}	M 4^{5}	L 2^{3}							Acceptable
By adding: SOIXANTE					S 6	O 1	I 1^{8}	X 3^{7}	A 1^{4}							Acceptable even though $\frac{L}{6^{1}}$ and $\frac{X}{3^{7}}$ seem far apart.

We have obtained four possible combinations. The reader may, if he fancies it, see what is wrong with CENT SIX MILLE, CENT TREIZE MILLE and CENT SEIZE MILLE. We will continue with CENT SOIXANTE: a few steps will bring us to the end of this weary *perlustration*.

Clear-rows 1, 2, 3:	A	F	E	P	U	B	G	L	Q	V	C	H	M	R	X	
										1^{6}	3^{2}	0^{6}	2^{7}	6^{6}	0^{4}	
Assumed crypto-equivalents:	C	E	N	T	S	O	I	X	A							
By adding:																
ET UN MIL(L)E										U 3^{2}	M 4^{6}	L 2^{3}				← Looks promising.
Follow up by adding CENT (No Additions to **kwn.** elements)																
DEUX CENT													D 2^{3}			← Looks promising.
Follow up again with numbers containing Z,																
ONZE insufficient to complete **kwn.**																
DOUZE insufficient to complete **kwn.**																
TREIZE														R	Z	
														7	0^{5}	← Looks like it.

We feel sure we are on the right track, and the only thing that is required to clinch the argument is to see whether the unused cases in the crypto-square can be filled acceptably, if we agree on CENT SOIXANTE ET UN MILLE DEUX CENT TREIZE, with the unused elements of the **kwn.**

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

Crypto-square

A	F	E	P	U	.	.	.	.	.
B	G	L	Q	V	.	.	.	.	.
C	H	M	R	X	.	.	.	.	.
D	I	N	S	Y	.	.	.	.	.
E	J	O	T	Z	.	0^{3}	5^{4}	.	.

Clear-square

The normal French alphabet (W omitted) with the known elements in the crypto-square checked up

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

discloses that "P" and "Q" have not yet been used. They must be taken in that order and we make:

$\frac{P}{1^4} \equiv \frac{J}{0^3}$ whence (τ) J ⟶ P [15]

$\frac{Q}{3^7} \equiv \frac{O}{5^4}$ whence (τ) O ⟶ Q [16]

which are perfectly acceptable.

These last two equations completed the ciphering alphabet which we hoped would prove correct and disclose, beside the clear sequence, the new rules of composition:

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

Complete Crypto-square

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

Clear-square

III. THE PROOF

1

The Indicators

Before exploring the secret text we were anxious for a quick proof of the correctness of our ciphering alphabet, even if not a strictly formal one. We could obtain it by an inquiry into the most likely position in the cryptogram, of the indicatory elements forming the **kwn.**, a subject previously discussed. Naturally, we first investigated the initial elements associated with the values given to them by their rank in the normal alphabet.

To our great relief we soon discovered that Bazeries had adhered to his original plan of placing the indicators at the head of the message. He had, however, TRANSPOSED their order.

The initial trigram LMP, taken in the order 3, 1, 2 that is PLM, with values derived from:

1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25
A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	X	Y	Z

gives us:

P	L	M
16	12	13

or exactly 161.213, the key word numeral CENT SOIXANTE ET UN MILLE DEUX CENT TREIZE found at the end of our analysis.

2

The Message

At this stage we felt very confident that our ciphering alphabet had indeed been correctly drawn and we hastened to lift the veil enshrouding the text of the secret message, thus far a completely neglected document. Of course, there were yet to be discovered the system of the nulls and the type of transposition resorted to, but we knew we had reached the end of our quest and that these two unknown factors of the cipher would soon reveal themselves.

The clear elements were interlined with the secret message as follows:

```
1                   5                  10                  15                  20                  25                  30                  35
(L) (M) (P) C X B R L S Q H F M H H C B H K X C M S H Q B C U P M C C V F S
            A L D R H U O S I C S S A D S E L A C U S O D A V J C A A T I U

        40                  45                  50                  55                  60                  65                  70
A K F L N V G S R X F C V B R S N X F T K K R R N D D Q G H Q X N L M H F S
Q E I H E T N U R L I A T D R U E L I P E E R R E M M O N S O L E H C S I U
•                           ←———

  75                  80                  85                  90                  95                 100                 105                 110
V K R F S N I C R V K B A K V G N V C S G C N R S M M C H P B K H F Q U C F
T E R I U E G A R T E D Q E T N E T A U N A E R U C C A S J D E S I O V A I
                    •

      115                 120                 125                 130                 135                 140                 145
U N X R V I G V T K H K R O D N R N B M R K F G G N C M C K S V H N G S G C
V E L R T G N T P E S E R B M E R E D C R E I N N E A C A E U T S E N U N A
            ←———               ←———

150                 155                 160                 165                 170                 175                 180                 185
U R K G N V K D D Q V R K O N B N L G Q T S N K I C V U K B V I G F G C Z F
V R E N E T E M M O T R E B E D E H N O P U E E G A T V E D T G N I N A X I

    190                 195                 200                 205                 210                 215
H U C H S A M N U C X F F V F C R H K B F V C X N H G Q
S V A S U Q C E V A L I I T I A R S E D I T A L E S N O
      •                                 ←———               ←———
```

It was an easy task to determine the transposition. By reading the interlines backward—*hebrew fashion*—several fragments of words, such as those we have underscored, clearly jumped to view. Nevertheless, on account of the presence in the message of three *pilot* Q-elements, we relied

on the age-old method of looking for their mates, the U-elements, to discover the transpositional scheme.

We can observe from the following diagrams that in "hebrew" transposition by periods, if QU lies within the period, its transposed equivalent will invariably be UQ inseparable, irrespective of the length of the period; but that if the period separation takes place between Q and U, that is, ..Q|U... then the transposed equivalent will take the form Q.....U, the number of elements between them depending on the period. This last case, however, yields a very important clue: two period separations, one in front of Q, the other after U:

I:

. . L	E Q U	E L .
L . .	U Q E	. L E

,

. . L A	Q U E L	L E . .
A L . .	L E U Q	. . E L

II:

L E Q	U E L
Q E L	L E U

,

. L A Q	U E L L	E . . .
Q A L .	L L E U	. . . E

It was a simple thing to bring together Q–86 and U–93

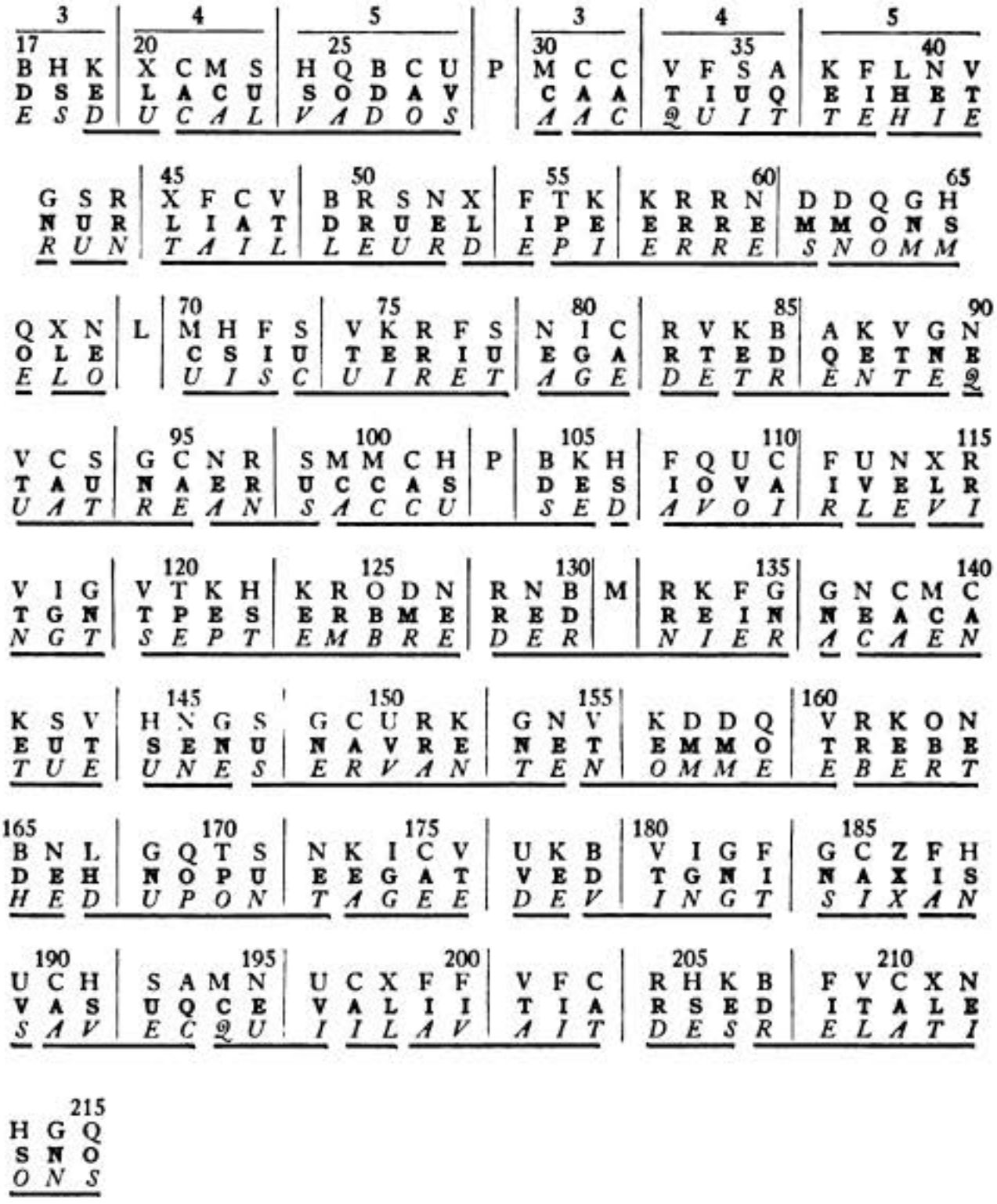
86				90				93
A	K	V	G	N	V	C	S	
Q	E	T	N	E	T	A	U	
E	*N*	*T*	*E*	*Q*	*U*	*A*	*T*	
←——5——→					←—3—→			

yielding periods of 5 and 3 and easily suggesting TRENTE QUATRE or TRENTE QUATRIÈME, which were tried by extending the above subsequence on both sides:

3			4				5				3			4			
79						85				90				95			
N	I	C	R	V	K	B	A	K	V	G	N	V	C	S	G	C	N	R
E	G	A	R	T	E	D	Q	E	T	N	E	T	A	U	N	A	E	R
A	*G*	*E*	*D*	*E*	*T*	*R*	*E*	*N*	*T*	*E*	*Q*	*U*	*A*	*T*	*R*	*E*	*A*	*N*

âgé de trente-quatre an....and giving up a cyclic periodical transposition of 3, 4 and 5 elements.

We are giving hereunder the message and its decipherment. For reasons that will soon become clear, we are beginning it with the 17th letter. The decipherment shows that the indicatory letters L, M and P were also used as nulls, inserted at will between periods with no prearranged plan. Not many of them were so used.



or .....*es du Calvados*[1] *a acquitté hier un tailleur de pierres nommé Louis Cuiret âgé de trente-quatre ans accusé d'avoir, le vingt septembre dernier, à Caen,*[2] *tué une servante, nommée Berthe Dupont, âgée de vingt-six ans, avec qui il avait des relations.*[3]

[1] One of the five administrative departments of the province of Normandy in Northern France.
[2] Principal city of the *Département du Calvados*, the seat of a *Préfet* and of an Assize Court.
[3] Rather a sordid story to illustrate a new system of cryptography.

3

The Inevitable Blunders

With the exception of the first sixteen letters, the message was correctly ciphered: the translation, as we have observed, flowing rhythmically. But in that initial fragment three ciphering errors were committed. We call them errors because we searched in vain for a plausible explanation.[1]

The deciphering from the 17th elements begins with the period 3 of the cycle. Going back from this point with periods 5–4–3 we obtain:

1							5						10						15								
(L)	(M)	(P)	C	X	B	R	L	S	Q	H	F	M	H	H	C	B	H	K
			A	L	D	R	H	U	O	S	I	C	S	S	A	D	S	
			R	D	L	A	S	O	U	H	A	S	S	C	I	E	S	D

which gives an impossible reading, although the correct beginning, "*La cour d'assises*," can easily be inferred. The only rearrangement making sense that we can suggest, in view of the null quality of "L" and "M," would be:

		2		5						6								
(L)	(M)	(P)	C	X	B	R	(L)	S	Q	H	F	(M)	H	H	C	B	H	K
			A	L	D	R		U	O	S	I		S	S	A	D	S	E
			L	*A*	*O*	*U*		*R*	*D*	*A*	*S*		*S*	*I*	*S*	*E*	*S*	

C (missing)

which is absurd, because the message would then begin with a period of 2, the only one in the cipher; it would have two nulls *inserted* in the two following periods of 5 and 6 respectively, evidencing not only a usage of the nulls different from the one followed through the major part of the message, but also a lack of rhythm in the sequence: 2–5–6. Also, the introduction of a period of 6, again, the only one in the message.

It is evident that errors took place here. Perhaps M(13) should have been placed in 4th position as an equivalent for "C" and L(8) pushed in 11th position in order to preserve the cycle unbroken, and obtain at the same time the correct reading, thus:

[1] See note at end of this section.

(L) (M) (P)	←3→			←4→				L	←5→							
	M	C	X	B	R	S	Q		H	F	H	H	C	B	H	K
	C	A	L	D	R	U	O		S	I	S	S	A	D	S	E
	L	*A*	*C*	*O*	*U*	*R*	*D*		*A*	*S*	*S*	*I*	*S*	*E*	*S*	

When the correct beginning unfolded itself, we fairly flew in honest passion. *Assises* was one of the probable words we had essayed in attempting the solution with Bazeries' own method. Apparently three stupid blunders, perhaps typographical ones, in rapid succession and within thirteen elements of the text, had deprived us of a quicker and less laborious solution. We roundly cursed our bad luck. But in subsiding we reproved ourselves

Mi vergognai di me medesmo meco

and we were again thankful that adversity had led us to a field of research replete with beauty, of that transcendental beauty which men of mathematics perceive in the symbolic evolution of abstract concepts.

NOTE:

We never felt at ease with the theory that so many errors were committed at the very beginning of the secret text. A restudy has disclosed the following possibility which seems plausible even though the rules of composition are complicated.

	←4→				←5→					←6→						←3→			←4→				←5	
(L)	M	(P)	C	X	B	R	(L)	S	Q	H	F	(M)	H	H	C	B	H	K	X	C	M	S		etc.
	C	(J)	A	L	D	R	(H)	U	O	S	I	(C)	S	S	A	D	S	E	L	A	C	U		
	L	A	(J)	C	O	U	(H)	R	D	A	S	S	(C)	I	S	E	S	D	U	C	A	L		

Rules:

1. *The first letter of the cryptogram is to be a null (an absolute one).*
2. *The secret text is to be divided into cyclic groups of 3, 4 and 5 elements.*
3. *The key-word is to be composed of three letters.*
4. *The first letter of the key-word is to be inserted anywhere in the first group, the second anywhere in the second group, the third anywhere in the third group: the sense of the decipherment determining their identity. Therefore the initial three groups after the first null are to be of 4, 5 and 6 elements, respectively.*
5. *The key-word elements are to be used as nulls inserted between groups at will.*

The above rules yield PLM, or 16, 12, 13, that is 161.213, from which the key-word-numeral CENT SOIXANTE ET UN MILLE DEUX CENT TREIZE is derived.

Chapter VI

COMMENTARIES

THIS chapter is entirely devoted to cipher students, especially to young ones—not necessarily in age—who have mastered elementary cryptanalysis.

It is not often that they are afforded the opportunity for an extended discussion of general problems of cryptography from the practical and historical points of view or for a little critical *causerie*.

The more sophisticated students are also welcome to the first section of this chapter which, it is hoped, will prove fertile ground for lively discussion.

I. RANDOM EVALUATIONS

1

On Writers' Affectations

I have grown tired of the mantle of royalty I have been wearing of late while penning the contents of this work. I suppose there must be some good reasons why writers on speculative subjects insist on using the first person plural, after the habit of pontiffs and kings. Perhaps they subconsciously feel a keen sense of proximity with their readers and are impelled to lead them through the maze of their demonstrations.

At times I have found it irksome to put down such expressions as: *we affirm*, *we confess*, and the like. I can scarcely see, even now, a plausible relation between these phrases and the reader. Somehow, this manner of address has given me on those occasions the peculiar impression of wearing a halo, and the feeling of aping someone.

For this reason, I have decided to become myself again and to chat with you on more intimate terms.

2

On the Style of This Book

The perennial guardians of propriety will undoubtedly find fault with me for having interspersed matter that, to them, may seem *fanciful* in an otherwise rigorous exposition of a cryptanalytic *technique*.

The reason for my having done so is very simple. I just wished to make the reading of this essay, my first one on the subject, more palatable, not to experts nor to serious students who are perfectly capable of thriving on arid literature, but to those of my many friends to whom my interest in ciphers will come as a surprise.

A layer of butter has always improved the taste of a slice of bread, I think.

3

On the Esthetics of Words

While we are discussing *propriety*, I myself may be labelled as a stickler for it. Major Millikin has repeatedly urged me to use the words *encipher enciphering*, *encipherer*, *etc.*, instead of the familiar ones appearing herein. It seems that experts have reached the conclusion that the two connotations of *cipher*, *ciphering*, *cipherer*, *etc.*, that is, "to reckon in figures" and "to write in occult characters" tend to mislead the reader.

Aside from the fact that the forms I prefer are perfectly adequate for the purpose and that their giving rise to misunderstandings is a very remote probability, I find it difficult to follow the suggestions for *esthetic* reasons. To me, *encipher*, *enciphering*, *encipherer*, *etc.*, look ugly and sound uglier. And what is funny about it is that I do not gain this impression through any particular appreciation of the value of English words I may possess—frankly, it is very superficial—but only by *reflex*. Whenever the suggestion is advanced, my mind instantly recoils to the French and Italian counterparts, *chiffrer* and *cifrare* and it registers a distasteful reaction to the analogous possibilities of *enchiffrer* and *incifrare*. It just could not be.

I was glad to read a few days ago, in Somerset Maugham's latest work, that words have weight, sound and appearance.

4

On Young Analysts' Mistakes

These are a few words of warning.

It is the aim of analysts to get at results in the quickest possible time, with the least expenditure of energy. I am told that the experienced ones are cool and collected and possess the uncanny faculty of doing the right thing at the right time. Perhaps it is so. The newcomers, if I am to judge them by my own impulses, are, on the contrary, nervous and fidgety. Naturally they have not had the time to acquire poise. And of course they blunder around. Their anxiety usually blinds them to the most fundamental facts of the problem confronting them.

I made the same mistakes that newcomers commit when attempting the breaking of a new cipher.

The *only* important fact that left any impression in my mind, when I first studied the problem, was that Bazeries' cipher was a simple substitution. While I was awake to the fact that the substitution had been subjected to a transposition, I still insisted that the transposition was of such an elementary nature that the ordinary approaches to simple substitutions should prove sufficient to break the cipher.

I was severely punished for my arrogant surmise that a cipher deemed unbreakable, or nearly so, by its author—a famous master in the art of cryptanalysis—could be so simple. All my trials, and they were many, were stopped dead.

Strangely enough, I do not feel that the punishment was undeserved, since I failed on one point: what at the time I deemed to be the most important fact of the cipher *was not, in fact, the most important at all.*

There is no possible excuse for my failure to detect the weakest spot earlier, except undue anxiety. It was not hiding. It was there, staring at me all the time, as plain as the shining light.

The heel of Achilles of the system was the very *device* introduced in it for the avowed purpose of confusing the analyst: it was its most *salient feature.*

As soon as it dawned upon me that I *possessed the knowledge* that the key-word of the ciphering alphabet was to be made up with the *name of a*

number—the number itself was unimportant—the cipher was as good as broken.

5

On "Reddite quae sunt Caesaris, Caesari . . ."

By the way, the technique evolved for the solution of this cipher bears some analogy to the method developed by Lieut. (now Lt. Col., U. S. Army, Retired) Frank Moorman, to discover the key-word in a *Playfair* cipher. It is described in the Manual for the Solution of Military Ciphers by Parker Hitt (Col., U. S. Army, Retired) pp. 78 *et seq.*

6

On Magnifying One's Deeds

One of my friends has been critical of my argument on Bazeries' insincerity (Chapter III–1), suggesting that it is, in effect, an attempt to magnify more than necessarily my success in breaking the cipher. My insistence that Bazeries held his system indecipherable in spite of the doubts he professed on this point seems to him tendentious.

My answer to his criticism is that it is not. While it is true that the solution elated me beyond description, I declare that I do not now attach undue weight to the feat. As I have said, it really was too obvious and it proved to be just as *mechanical* as an ordinary *Vigenère.*

I am rather wondering how it was possible that so talented a man as Bazeries could have put so much faith in his cipher, even if that faith was tempered by doubts which I hardly believe genuine. Proposing the cipher to the War Staff certainly implied a fair amount of belief.

Is it because the art of cryptanalysis stands today on a much higher plane than it did forty years ago? If it does, we all have reason to rejoice. Yet, the breaking of the cylindrical cryptograph by de Viaris—one of his contemporaries—cannot be dismissed as just an elementary piece of cryptanalysis.

It looks as if Bazeries did not possess the faculty of applying his remarkable analytical powers to his own handiwork. Self-analysis does not seem to have been his forte.

7

On Inventions

A: THE "PROBABLE WORD" PROCESS

I have stated in the introduction of this work that Bazeries was the inventor of a technique for the solution of multiple alphabet square ciphers known as the *process of the probable word.*

In a recent exhaustive and authoritative essay on Poe,[1] Lt. Col. Friedman advances the thesis that credit for this process, commonly given to Bazeries, should go to the Englishman, John Falconer, who anticipated Bazeries by 200 years.

The conclusion reached by our eminent cryptanalyst seems to me rather incidental. I shall try to give the reasons for demurring.

Falconer, an able cryptanalyst, considering the era in which he lived, reports on page 17 of his work[2] three methods of ciphering described by his fellow-countryman, Bishop John Wilkins[3] "wherein each particular *Line, Word* or *Letter,* is written by a new alphabet."

From the three examples for solution which Falconer offers it may easily be seen that, even though he makes some relevant and sometimes acute observations on the effects of this manner of ciphering, he still is hazy and not definite enough in his attacks.

To begin with, his examples consist of messages in which words are separated and, to facilitate his explanations, he sees to it that words of one, two and three letters are fairly represented.

It is interesting to show the weakness of his attacks.

> I. "When there is only one Alphabet used for a Line, the Writing might be discovered as in plain Cypher, if you make a new Operation for each line."

Falconer did not perceive that all this work was unnecessary and that a simple running-down of his crypto-line by the Julius Caesar process, as shown

---

[1] William F. Friedman (Lt. Col. Signal Reserve, U. S. Army) *Edgar Allan Poe, Cryptographer,* in Signal Corps Bulletin No. 97, July to September 1937, and *Addendum* in Bulletin No. 98, October to December 1937, Washington, D. C.

[2] *Cryptomenysis Patefacta,* Or *the Art of Secret Information Disclosed without a Key* (London, 1685).

[3] *Mercury:* or, *the Secret and Swift Messenger* (London, 1641).

in the following diagram, would immediately have given up the clear text. Note that he omitted J and U from the square table.

```
Y   P B   V D G R T S   I D   Z T T E   I X T.....
Z   Q C   W E H S V T   K E   A V V F   K Y V
A   R D   X F I T W V   L F   B W W G   L Z W
B   S E   Y G K V X W   M G   C X X H   M A X
.   . .   . . . . . .   . .   . . . .   . . .

I   A M   F O R C E D   T O   K E E P   T H E
```

But he adds, very pointedly:

> "If you find out but one Letter in a Line, (and that may certainly be done by a few Suppositions)[1] it will of it self give an Alphabet for the whole line......"
>
> II. "When the Alphabet is changed at every word, you may either make Suppositions from *Words*, or from *Letters* that fall in the end or beginning of the several Words in the Writing until you have made progress in the Letters of the Key; and then proceed as before.
>
> "You may likewise find out by Supposition, the number of Letters in the Key, &c. which will much facilitate the work."

As can be seen, he is still groping around. The running-down method would again yield the solution readily. The key he used is the word *Policy*.

Key:

```
A   Y   O A   Q Z C N P O   C X   M G G R   R F C.....
Z   Z   P B   R A D O Q P   D Y   N H   S   S G D
Y   Z   Q C   S B E P R Q   E Z   O I   T   T H E
.   .   . .   . . . . . .   . .   . .   .

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

[1] Of course, he was thinking of very short words.

> III. "To decypher this last kind of Secret Writing, you must begin with Suppositions; and 1. Extracting out of it the Monosyllables, &c. you may suppose all the Words in it of three Letters successively to stand for *the*, or *and*, &c. and you may prove your several Suppositions thus: *viz.* 1. Mark down the Powers supposed. 2. Observe in what Lines of your Counter-Table the Letters express'd in the Cypher are opposed to them in a perpendicular Line.[1] 3. Observe the first Letters of those Lines, and you will soon find whether they can be joyned to make up a part of the Key: . . ."

It is evidently a clever attempt to build up the key-word through the clear-text as we do today with *running-key* ciphers, but it is not the *definite* procedure described by Bazeries which must yield the key if a supposed word—sufficiently long for the purpose—actually exists in the cryptogram. Furthermore, the supposed word in Falconer's scheme is definitely a *short* empty word in a *divided* text, which is only considered because it might stand for "I," "A"; "TO" "ME," "BE," etc.; "THE," "AND," "FOR," etc.; whereas in Bazeries' process the supposition is arbitrary and, except in rare cases, has no relation whatever with the physiognomy of the probable word in the secret text. Still more, Falconer's process is only effective when the key-word is clear: with an incoherent key it could not be followed through. This is not true, however, when the Bazeries process is applied, since the process does not depend on the coherence of the key-word.

Why did Falconer *fail* to give a solution for a message with the added "intricacy" as he called it, "of concealing the sense of an Epistle by writing continually without any distinction between the words?" I maintain that he did not know how to tackle it, for, even in the case of the "simple cypher" with this "Intricacy," the solution he offered was *just a statement* that it could be worked out, but without telling us how. This is what he said:

> "By this Intricacy, I acknowledge those helps we mentioned from *single Characters*, *Terminations*, or the like, are deluded; but you may however *distinguish*, *between the Vowels and Consonants*, *the Vowels one from another*, *as also the Consonants amongst themselves:* nay, you may make Suppositions for Words, &c. and

[1] That is: the probable key-letter.

> having found two or three Letters, or one Word, the difficulty is over. I have often tryed it, and never found any new difficulty to arise from this *Defeating* way that requires other Rules, than what you have already for Decyphering."

It is not my contention that Bazeries was the *inventor* of the process generally attributed to him. Quite likely, the probable word process was tried soon after man first began to investigate ciphers—it must have been the most natural thing that suggested itself to him. Certainly, similar processes were used many times before by famous epigraphists in reading ancient inscriptions.

Besides, Bazeries himself is not specifically claiming credit for the invention. When he says:

> "Let us go back to the square cipher, from which we have momentarily drifted away and let us give a new process of decrypting which neither Kasiski, nor Kerckhoffs, nor Josse, nor de Viaris, nor Valerio have described.",

it seems to me that he only claims the *newness* in the approach to the process *as applied to square ciphers*, for, had he held the principle to be absolutely *new*, how could he have expected Kasiski or any one of the others to *describe* it?

The fact remains that the process, as applied today, received at the hands of Bazeries the concrete and definite shape it formerly lacked; it gained through him a recognition never attained before and rose to the dignity of an almost infallible device. For these reasons I do not hesitate to say that the process, as now understood and practiced, originated with him.

***

B: BAZERIES' MECHANICAL "CRYPTOGRAPH"

We will now discuss the case of Bazeries' cryptograph, the invention of which he claimed as his own in his first communication to the French General Staff.

Col. Friedman, in his article "Codes and Ciphers" appearing in the

14th edition of the Encyclopedia Britannica, attributes the invention to Thomas Jefferson, and in his later essay on Poe, previously mentioned, variously calls it "Jefferson's system," "Jefferson's device" and squarely "Jefferson's invention." I quote from the essay:

> "Many of my readers will recognize Jefferson's device as being practically identical in principle as well as in form with cipher device, type M-94. I will admit that when, in 1922, my friend Professor John Manly brought me a photostatic copy of the foregoing, in Jefferson's own handwriting, with all the corrections Jefferson made as he was describing his invention, I was much startled. For here was another beautiful example of the adage in cryptography that there is nothing new under the sun. Major Bazeries is credited with having been the inventor of this device, because it was described and pictured in a book written by him in 1901,.....But in 1914, Parker Hitt, now Colonel, United States Army, retired, then a captain of Infantry, independently conceived a device employing the same principle. He constructed two devices: one took the form of disks, the other took the form of a set of juxtaposed sliding strips of wood. Colonel Hitt has assured me that he had never seen or heard of Bazeries' cylinder; and it may, of course, be assumed with a high degree of probability that Bazeries had no knowledge of Jefferson's cylinder.

The description of Jefferson's "Wheel Cipher" proves to be amazingly identical with Bazeries' cylindrical cryptograph. However, I fail to read in it any reference that Jefferson claimed it as his own.

Frankly, I have no set view on the subject. Neither am I trying to detract from the accomplishments of one of our early Presidents. I am simply holding that the mere fact that a description of the device is found in his papers does not necessarily prove him to be its inventor.

To begin with, we know that Jefferson was a prolific writer who had the excellent habit of jotting down almost everything that struck him as being unusual. An insatiably curious man, he travelled widely. In his capacity as American representative abroad he came in contact with various diplomats and other notables and continually used ciphers in his official correspondence.

Is it not possible that in his European peregrinations he had come across the device, perhaps used with circumspection by some colleague of his, had made a note of it, as was his inveterate habit, and probably neglected it? Is there any trace of his making use of this cryptograph in later years, when he was President? Edmund C. Burnett in the article: *Ciphers of the Revolutionary Period*, which appeared in the *American Historical Review* (January 1917) does not list this cryptograph among the ciphers used by Jefferson.

We must take into consideration that Jefferson, in the course of years, has been invested with such glamor, partly because of our admiration for his outstanding gifts and to some extent because of his voluminous and interesting papers, that there has been a strong tendency to attribute to him inventions which obviously did not originate with him.

The two instances I am about to present may not seem relevant; still I think them worthy of attention.

Just the other day I read in the New York *Times* the review of a book, recently published, dealing with Jefferson's culinary proclivities. We are informed that he made scrupulous notations of every recipe of food prepared in a style unknown to him. It seems that he even importuned chefs and gourmets of both sexes in his eagerness to enlarge his knowledge of Vatel's science. Yet, those recipes are being attributed to him.

The second instance illustrates the point more forcefully.

Not so long ago I received through the mail the May (1938) issue of "Fact Digest," a popular magazine. I looked in vain for some sort of a marked article which, I surmised, was being sent for my personal attention. I was rewarded, however, by finding on page 14 this startling statement:

> "Thomas Jefferson, third President of the United States, invented the wheel-barrow. He also. . . . ."

Now, the invention of the wheel-barrow has very little to do with cryptography and, besides, it interests me very little. But I thought the claim to be far-fetched. Here is a perfect case of an enthusiastic, but none too critical hero-worshipper, turning some innocent notes on the subject of this particular vehicle by the writer of the Declaration of Independence into an outright invention.

Sensing that so obvious a contraption as the wheel-barrow must have

been the product of early man's needs, I spent some minutes at my few library shelves to look for information, and discovered the following references:

a) In the *Century Dictionary* (New York 1889):

> John Florio (1553–1625), an English Lexicographer, published in 1598 an English Italian dictionary entitled "A Worlde of Wordes" and republished it in 1611 with the title of "Queen's Anna New World of Words" (note the difference in spelling which occurred in the short lapse of 13 years) where this entry is to be found:
>
> "CARRIOLA, a wheel-barrow,"

showing that the wheel-barrow was known both in England and Italy long before Jefferson's birth, which took place in 1743.

b) In the *Nouveau Petit Larousse* (Paris, 1936):

> "When it is said that Pascal[1] improved the BROUETTE (wheel-barrow) one must understand the VINAIGRETTE (a man-pulled two-wheeled carriage) and not the 'brouette' properly called, which is *very ancient*."

c) Facing page 499 of H. G. Wells' *Outline of History*,[2] we can see the print of a one-wheeled "vinaigrette" resembling greatly a wheel-barrow, apparently used by the early Chinese as a means of transportation.

8

On Boasting

I felt terribly humiliated—the *tournure* of my name should explain the reason—when, several years ago, a copy of Figl's[3] handbook fell for the first time into my hands. In great consternation *I read in chapter 44, and SAW on the table accompanying it*, that the Italian Army had used in the early period of the war a "Cifrario Tascabile" (Pocket code—even the name was misleading) which consisted of....., reader, you never will

[1] Blaise Pascal (1623–1662) a famous French mathematician and philosopher.
[2] The reprint of P. F. Collier & Son Co., New York, 1922.
[3] Andreas Figl: Systeme des Chiffrierens, (Graz, 1926).

guess! It consisted of a Vigenère table with thirty-six groups of consecutive numbers from 10 to 45, twenty-six of them corresponding to the elements of the alphabet, the other ten to the unit numbers and zero. Both editions of Sacco's manual, the first of which I read some time later, confirm that it was used until 1917.

Shades of Soro, Partenio and the Argentis! They must have had good cause for being ashamed of their descendants' gullibility and incapacity.

But no less credulity was shown by General Ronge, the last Chief of the Austrian Military Intelligence, who, when boasting of the success of his bureaus in decrypting intercepted Italian messages, said:[1]

> ". . . . .and, when early in October 1915, the *Cifrario Tascabile* was put into service, it was *again* one of my peacetime purchases which was finally paying for itself."

Both the boast and the purchase were unwarranted: the one, because decrypting a Vigenère cipher is no feat whatever; the other, because paying a traitor for a copy of such a *cipher* (!) was an injudicious waste of money.

On Heresies

Any view which Bazeries would not endorse was to him a cryptographic heresy. Captain Josse was a special target of Bazeries' Olympian shafts. "We are going to point out," he says, "the cryptographic heresies of which we have been speaking and which, in our opinion, abound in *La Cryptographie et ses applications à l'art militaire.*"[2] On final analysis, however, the heresies resolve themselves into highly debatable opinions, certainly not deserving of Bazeries' excommunication.

I prefer to call a heresy—I like the word—a theory obviously contrary to fact, insisted upon by anyone who is clothed with enough authority to know better.

Heresies of this type crop up once in a while even in the best of books and one wonders whether authors are, after all, as clever in the art they expound as is permissible for us to infer.

[1] Max Ronge: Kriegs- und Industrie-Spionage, (Zürich, 1932) chap. XI.
[2] L. Baudoin, Paris, 1885.

I disclaim any pleasure in pointing out heretical propositions to the attention of a cryptographic *Index Expurgatorius*, but it is in the nature of things that published opinions should expect comment.

I will, therefore, bring to your notice a few of the more flagrant ones I have encountered in my ramblings through the works of our mentors.

***

Bazeries, always ready to shake his finger at his colleagues' heresies—was guilty occasionally of the same sins. It is only fair that he head the list of transgressors.

On page 111 of *Les chiffres secrets dévoilés* the following passage appears:[1]

> "M. Kerckhoffs, in describing the secret ciphers adopted by the Russian nihilists—a system of double transposition—says that the nihilists committed the grave mistake of using the same key for the two transpositions. We are going to show that the French anarchists were guilty of a similar fault, *a fault which made possible the discovery of the cipher*."

After saying that the cipher was practically the same as the Gronsfeld variation of the Vigenère square,[2] he continues:

> "The key being a short one (first fault), its length was determined; in spite of this, the precautions taken by the anarchists kept the analyst in check for a fortnight.
>
> "Here are the precautions adopted:
>
> "1st: The first six and the last six letters of the cryptogram were nulls. The first precaution, excellent in itself, had the effect of enclosing the secret text between two ramparts, considered by some to be unscalable.
>
> "2nd: Nulls were inserted in the text at certain intervals and were ciphered; generally they were placed between words. This second precaution, also an excellent one, was, without a doubt, taken to repulse any able but not very patient analyst.

[1] I am responsible for emphasizing some of its parts.
[2] It is the same: why he calls it *practically* the same, I cannot fathom.

"The grave error made by the anarchists was *to place at the head and tail end of the cryptogram a number of nulls equal to period of the key.*"

How, in the name of reason, is it possible to indulge in such fantastic cerebrations? Wherein do nulls—any number of them—affect periodic repetitions? Must we believe that the secret message would not have been translated had the number of nulls been greater or smaller than the elements in the key? Can one see any difference in the inter-relation of the crypto-elements in the following two diagrams where the nulls "N" and "P" differ in number?

N_1	N_2	N_3	N_4	N_5	N_6
a_1	a_2	a_3	a_4	a_5	a_6
b_1	b_2	b_3	b_4	b_5	b_6
c_1	c_2	c_3	c_4	c_5	c_6
.	.	.	.	.	.
n_1	n_2	n_3	n_4	P_1	P_2
P_3	P_4	P_5	P_6		

N_1	N_2	N_3	a_1	a_2	a_3
a_4	a_5	a_6	b_1	b_2	b_3
b_4	b_5	b_6	c_1	c_2	c_3
c_4	c_5	c_6	.	.	.
.	.	.	n_1	n_2	n_3
n_4	n_5	n_6	P_1	P_2	P_3
P_4					

Nulls so located have simply the object of masking the true position of the beginning and the ending of the cryptogram—its two most vulnerable points. But this precaution is absolutely useless in a periodic key substitution.

Moreover, why did these two series of nulls retard the decrypting a *fortnight*? It sounds incredible. And I have not yet gotten over the shock that it took Bazeries four months to decrypt the second batch of the Duke of Orleans' despatches.[1]

Finally, how can the intercalation of nulls between *words* of the *clear-text*, which must of necessity be ciphered,[2] perturb in any way the rhythm of the period?

Nonsense.

This precaution, praised as an excellent one, is perfectly useless. Periodic

[1] See page 3, note 2.
[2] Bazeries acknowledges that they were ciphered.

recurrence in a square cipher can only be broken by first ciphering the message by means of a square of 25 or less elements and then by using the elements excluded from the square as nulls and interspersing them at well-considered places, best calculated to jar out of order the periodic repetitions appearing in the cryptogram. Even then a translation is very easy.

***

Lange & Soudart,[1] paraphrasing the entire account given by Bazeries are guilty of the same heresy. It shows, at least in this particular case, that they did not probe the conclusions reached by Bazeries.

***

In the highly meritorious *Cours de Cryptographie* by General M. Givierge, at the end of an exhaustive chapter on multiple alphabet substitutions, these concluding paragraphs can be read:

"We have extended ourselves to great length on multiple substitutions with normal alphabets. It is because they have given rise, as we have said, to many ingenious works. Certain authors, as for instance, de Viaris, have introduced in their theories algebraic notations concerning the relations between the rank, in the normal alphabet, of the clear-elements, the key-elements and the crypto-elements and have generalized these equations by proposing new systems. As an example of the complications which are applicable to square tables with normal alphabets we will describe the one of Rozier, who, to cipher a letter, goes down along the column of the square corresponding to that letter until he meets the key-letter, follows then the line of this last letter until he meets the next following key-letter and goes up the column to inscribe in the cryptogram the letter at the top of the column.

"Such systems, *although difficult* (bien que difficiles) have brought forth essays showing that their decrypting is possible."

[1] André Lange et E.-A. Soudart: *Traité de Cryptographie* (Félix Alcan, Paris, 1925).

The diagram below shows exactly the process of ciphering of the so-called Rozier system and what actually happens when "THE" is ciphered with the key-word "BUS."

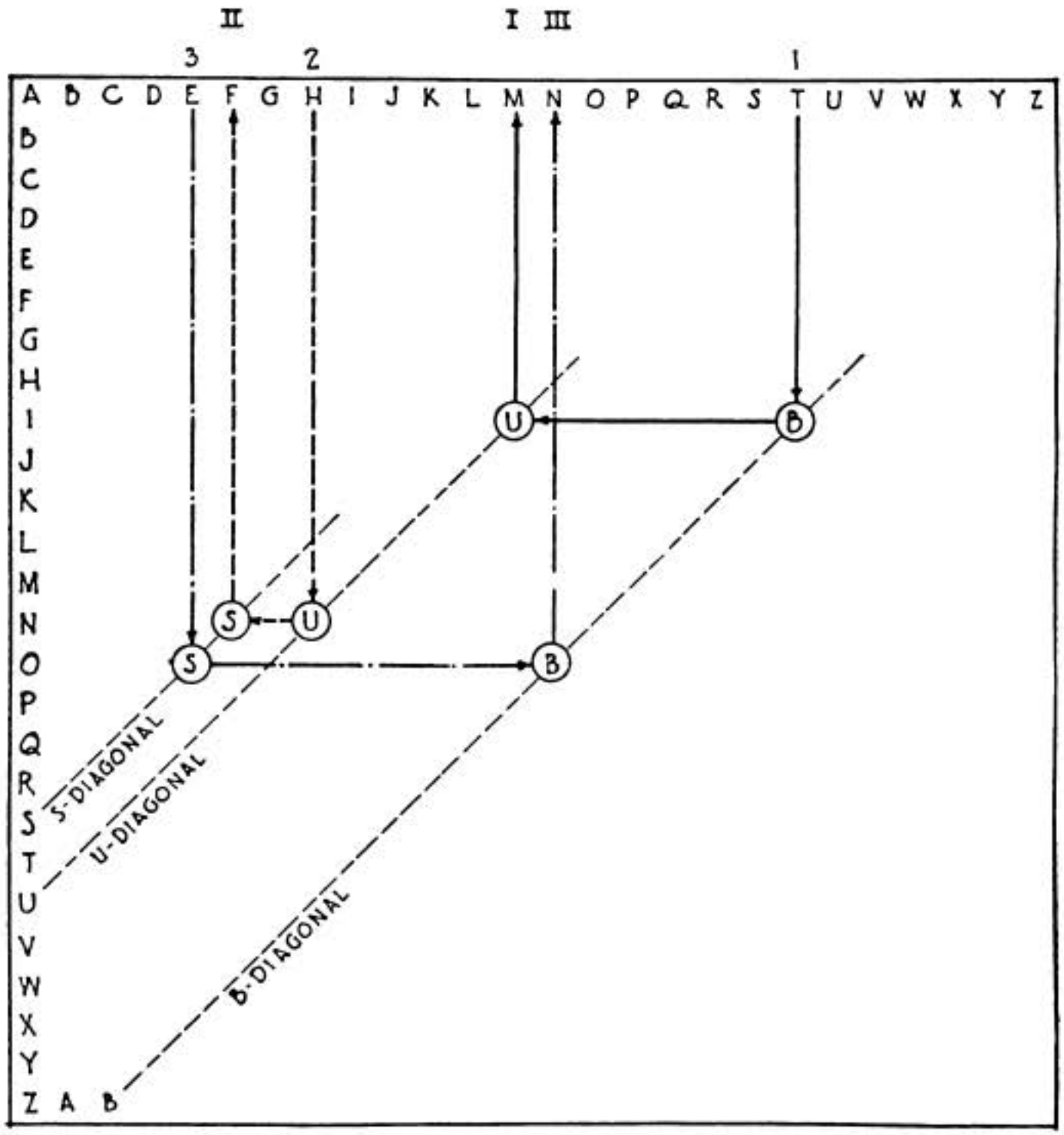


Fig. 9—*Rozier's System*

The resulting cryptogram is "MFN." It could have been more easily obtained with the Gronsfeld type of numerical key of −7, −2, +9.

The *complication* referred to by Givierge is nothing more than a long perambulation in the square resulting in distancing a crypto-element from its clear-element by a number of letters equal to the distance between its key-element and the next succeeding one. In fact:

T to M = B to U = +19 or −7

H to F = U to S = +24 or −2

E to N = S to B = +9

But it is childish to say that such systems are difficult or that particular studies were necessary to show that breaking them was possible. Why possible? Was there any doubt in his mind?

Perambulations in a square, no matter how long and devious, *do not at all* increase the difficulty of the systems based on such squares. These inventions—aberrations I should call them—can all be attacked and readily solved with the same devices used against a Vigenère, of which they are very close kin. The only difference between such systems and a Vigenère is merely in the key: the only effect resulting from a perambulation.

Thus:

	ROZIER	VIGENÈRE
clear:	T H E	T H E
crypto:	M F N	M F N
key:	B U S	T Y J

And, I think, we have had enough of this.

***

The heresies I am about to expose cannot be attributed to an expert. However, they appeared in a dignified scientific paper: the November 1916 issue of the *Engineers' Club of Philadelphia Proceedings*. The article is unsigned but an ominous WE in the preamble apparently directs the responsibility for its appearance towards its Committee on Publications.

Under the caption A NEW CIPHER CODE, the Vigenère table is given and its manipulations are duly explained. The readers are also regaled with

critical comparisons between the system and both Poe's *Gold Bug* story and Conan Doyle's *Dancing Men* adventures, which is as it should be.

But of the concluding evaluations of this new (?) cipher, some are exaggerated and others non-existent. It is needless to comment upon them except to say that as late as 1916 there still were, even in this country, believers in this overrated and now decrepit and valueless cipher. I have italicized the heresies.

> "The publication of this cipher code will no doubt bring to the mind of the readers other codes, *but it is doubted if any, heretofore invented, is as effective in every way as is this one.*
>
> "The method used for the preparation and reading of code messages is simple in the extreme and at the same time *impossible of translation unless the key-word is known.* The ease with which the key may be changed is another point in favor of the adoption of this code by those desiring to transmit important messages *without the slightest danger of their messages being read by political or business rivals, etc.*"

How disarmingly naive!!

***

Lastly, here is one of my own heresies which, of course, has never been published before.

I have said that the function of cryptanalysis (App. I, 3–20) is to attempt the restoration of ciphered texts to their intended meaning, without the knowledge of the cipher or key.

I wish to add here that the attempt at restoration is not always attended with positive results, in spite of the prevailing notion, often encouraged by the ebullience of self-styled experts, that there exists no cipher which cannot be unraveled.

Experts will undoubtedly object to the definition and particularly to the characterization that follows it. Among them, some will insist that the recent contributions to the knowledge of cryptanalysis have made of it

truly a science and that the intelligent application of its principles will always lead to a solution. Others, attracted by the beauty of the sentence or by its effusiveness, will blindly put their faith in Edgar Allan Poe's sweeping contention: "*. . . that human ingenuity cannot concoct a cipher which human ingenuity cannot resolve.*"

Do you really put much faith in these beliefs?

I do not.

Cryptanalysis is not a science even though it sometimes makes use of the *quasi-scientific data* of linguistics. Such data can only be used to a certain extent with the lower forms of ciphers. The more *concocted* the cipher, the less opportunity there is of applying toward its solution these so-called scientific principles. And no frequency tables, and percentages, and pilot letters, and fixed sequences, and the rest of these accepted notions, will ever by themselves solve well-constructed ciphers.

What has helped the spread of such fallacious notions is the fact that Governments have insisted, and unwisely continue to insist, on a type of simplicity in the making of field ciphers that inevitably renders them ineffectual.

We all grant that ciphers should be simple. A personnel operating in a war zone, beset with distracting difficulties, should not be subjected to the added mental strain resulting from handling complicated ciphers. But when it is decreed that a system must be such that the "*thickest leftenant*"[1] in the Army can use it, I wonder why it is that important issues affecting the life and security of a vast number of people—the fate of a nation, sometimes—should be entrusted to *thick lieutenants*.

After all, simplicity has, in common with other abstract qualities, a relative value. To the young boys who have learned the fundamental algebraic operations, the solving of a system of linear equations is a very simple thing, even though the operation is complex in character. It is, however, a mystery to myriads of people acquainted with arithmetic and a dreadful nightmare to hosts of educated grown-ups. All this, I am fully convinced, proves that there exists in the broad expanse of our world what is paradoxically known as *complex simplicity*.

---

[1] An expression attributed to a British officer, quoted by Col. Fabyan in *An Introduction to Methods for the Solution of Ciphers*, Riverbank Laboratories, Geneva, Illinois. Publication No. 17, Page 13.

Strong believer as I am in the omnipotence of the human intellect, ardent lover as I am of the art of decrypting, which I pursue with unbounded fascination, I am willing to assert that it is possible to construct systems of military ciphers that will resist decrypting, its arts and its guiles.

And I mean—simple systems.

10

On the Ranking of Cryptanalysts

In the early part of the 17th century, Duke Augustus of Braunschweig-Lüneburg[1] wrote an excellent treatise on ciphers.[2] In those days dukes were dukes and this particular one was the sovereign of his state. But perhaps he felt that the dignity of a monarch clashed with the more modest one of a book-writer and therefore he published his work under the nom-de-plume of Gustavus Selenus.[3]

Of course, changing one's name does not affect one's character except in stories of the Dr. Jekyll and Mr. Hyde variety, and our duke, as most rulers in this world, did not disdain the incense of his entourage. Frankly, I do not see how princes can escape it. Sycophants are natural appendages of royalty.

And so, with an apparent lack of modesty, Augustus *atque* Selenus prefaced his book with not less than seventeen small-folio pages of sundry, flamboyant and rather amusing tributes which his courtiers and scribes saw fit to pen for the occasion.

Today, of course, the publishing of private opinions on one's own work would be considered poor taste.

Now, what is this story leading to?

An opinion, not altogether laudatory, has been passed on this work and on myself. I can hardly be accused of bad taste in making it public, even though the opinion was privately given. I believe that I have the right to dispute it. The story is instructive because it pictures vividly the attitude of some experts toward newcomers.

---

[1] The line of Brunswick-Lüneburg is the branch of the house of Brunswick, from which the reigning house of Great Britain is descended.

[2] Gustavus Selenus: *Cryptomenytices et Cryptographiae Libri IX* (Lüneburg, 1624).

[3] Evidently he just veiled his name: Gustavus is a transposition of Augustus; Σελήνη (Selene) was the Greek goddess of the moon, which in Latin is *Luna*, whence Lüneburg, the name of one of his principalities.

The following verdict was rendered by one of six experts, named by me, to a publisher who had shown sufficient interest in my script:

> "the manuscript is the work of someone whose profession is not cryptanalysis."

Rather nice, don't you think? Let us see what it all means.
The expert asserts:

a) that there exists a profession of cryptanalysis;
b) that I am not a cryptanalyst by profession.

a) His positive assertion that there exists a profession of cryptanalysis I do not admit, and I am not quibbling about the significance of the word *profession*.

There exist in various departments of any civilized Government groups of men dealing in ciphers. Are they the ones our critic calls professionals? If so, why? Is it because they receive every fortnight a check from their Government for their daily efforts? Is it not a fact that only a mere handful of them are cryptanalysts, and the others just clerks? And is it not also a fact that from the average run of the cryptanalysts, only one or two occasionally emerge, worthy of being classed as such?

Now, what are the precise attributes that our expert associates with those whom he tags as "professional" cryptanalysts? Does he imply that they are better men, cryptanalytically speaking, than those whom he disdainfully excludes from his Olympus? Can he assert that, let us say, a man whose profession is the teaching of English is no better than one of those worthies whose interest in ciphers is awakened with clock-like precision at 10:00 a.m. and put to bed at 4:00 p.m.?

True cryptanalysts are the product of war; they emerge through and because of the stresses of a major conflict. It is very strange, but nevertheless a fact, that cryptanalysts who have been most useful to their countries are those whose peace-time occupations were far removed from the fields of cryptography and cryptanalysis. The last great war has furnished us with many shining examples of this simple truth.

b) The title page of my typescript showed that I am an architect;

it was not difficult, therefore, to deduce that I am not a *professional* cryptanalyst.

Then I must be an *amateur* cryptanalyst, for the opposite of professional is amateur in any language.

That being the case, where does the difference between professional and amateurish cipher-breaking precisely lie?

Does it lie in the result? Can one really assert that a mathematician's conclusion that $2 + 3 = 5$ is any different from that of a child who has just learned the process of counting? Obviously not.

Then it must lie in the method, and perhaps in the presentation.

As to the method, I maintain that the technique evolved is new, that it is the most direct technique and that—mathematically speaking—it is a thoroughly elegant technique.

As regards the presentation, I insist that each step of the solution is perfectly logical, *coldly* so, and that its development is rigorous, *mathematically* so.

These being the facts, was the criticism fair?

II. FAILURES

I shall now discuss the apparent failures of the ordinary approaches I applied in trying to break Bazeries' fourth cipher system. You must, however, remember that I put some limitations to this statement. It would be well to refer again to page 34, III: DIVERSE APPROACHES.

1

The Research for the "Nulls"

The interspersion of nulls in a secret text, if they are at all numerous, must be executed in accordance with a definite plan. A few nulls do not increase the difficulty of a cipher to any extent. On the other hand, when adopting a method of research, based on frequencies and adjacencies of elements, nulls are bothersome, as they ordinarily throw out of gear well known common bigrams, trigrams, etc. The sooner the presence of nulls is ascertained, the easier the rest of the work becomes.

Sometimes nulls are selected after the ciphering, from those elements that do not appear in the cryptogram. A short message such as ours does

not ordinarily include more than 18 to 21 elements out of the 25 or 26 letters that the alphabet contains. When so selected, the nulls are more susceptible to detection. But Bazeries, conscious of this fact, did not adopt this scheme: Fig. 7 discloses that only 22 elements found their way into the cryptogram.

Another possibility is the following: In a system where the deciphering operation must begin with a subdivision of the secret text into groups, the chances are that nulls have been inserted between some such periods. It follows that if a few letters have been used as nulls, they must be located at intervals that are multiples of the period.

I decided to make a search of this kind by preparing a schedule, a fragment of which is given hereunder, where the ordinal positions of all like-elements in the cryptogram were registered and the intervals between them computed. I was hopeful that some *persistent repetition* of possible factors would emerge from the schedule, with the excellent chance of the element showing it, being a null.

A	36		86		193					
		50		107						
B	6		17		26		49		85	
		11		9		23		36		19

B	104		130		165		179		207
		26		35		14		28	

No tangible results were obtained from this inquiry for the simple reason that very few nulls were scattered through the text. Had they been more numerous, it is doubtful whether I could have discovered them, due to my subconscious insistence in analyzing trigrams into which—I thought—the message had been divided, while in reality the division consisted of a succession of trigrams, tetragrams, and pentagrams.

2

Empiric Search for the Key-Word-Numeral

I have already discussed the wide selection of devices by means of which the indicatory elements could have been hidden in the cryptogram. I was cold to the idea of attempting to locate them. I even refused to assume that the initial elements, as was originally the case, might again be the ones. I argued that it would be the silliest thing to do to put them there—not subtle enough—and I was not willing to waste any time on this assumption.

Two groups, however,

1–2		69–70
LM	and	LM

attracted me almost magnetically. They looked suspicious. It is a common trick to insert indicatory elements before or after or on both sides of a repetition, itself a null, of an initial group.

While a lucky guess of this kind often yields quick results, it does not satisfy the searcher's *amour propre*. But in the scheme of cipher solving sentimentalities have no place and an immediate solution, especially in times of stress, is of paramount importance. So I decided to explore this possibility.

I prepared the following table giving ranking values from 1 to 25 to the elements of six alphabets: a normal one, an L-straight, an M-straight and their inverted ones.

→	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25		
I	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	X	Y	Z	A	IV
II	L	M	N	O	P	Q	R	S	T	U	V	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	V
III	M	N	O	P	Q	R	S	T	U	V	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	VI
	1	25	24	23	22	21	20	19	18	17	16	15	14	13	12	11	10	9	8	7	6	5	4	3	2	1	←

Fig. 10—*Various Ranking Values*

I tried without result all the possible combinations of the elements preceding and following the group 69–70,

				69	70			
Q	X	N	L	M	H	F	S	

and decided that appearances had deceived me. Frankly, I was glad to *have been thrown back for a loss*.

3

Spotting of the Vowels

The *spotting* of the vowels, that is, the determination of the crypto-elements that are most likely to represent the clear-vowels, is one of the analytical approaches generally favored by cryptanalysts. For this determination two well-known principles are applied:

I: In French, clear-E is so much more preponderant than any other element, that the crypto-element representing it in a mono-alphabetic substitution can correctly be selected at once.

II: In French, clear-E rarely associates with other vowels. Also, all vowels, with the exception of Y, are high-frequency elements. Therefore, if a tabulation of the appearances of the high-frequency crypto-elements that precede or follow the presumed equivalent of clear-E is made, it is possible to determine, with a certain degree of accuracy, which of them are vowels or consonants by noting the absence or presence of such adjacencies.

In this problem doubts existed as to the equivalent of clear-E: a study of the frequencies pointed to an actual dilution of its frequency but I made the same assumption I followed later[1], to the effect that crypto-K was one of the representations of clear-E.

Therefore, by preparing a tabulation of all the affixes of the crypto-elements with the highest frequencies—that is, the first eleven letters of Fig. 7—my expectations were, if luck was with me, not only to decide upon most of the vowels but to determine also the other E-equivalent by simply matching the K-column with the other columns and deciding upon the one most similar to it in general appearance.

The tabulation was easily derived from Fig. 6:

21 C	18 K	18 N	16 F	16 V	15 H	15 R	14 G	13 S	10 M	10 B
1 C 1	1 C	1 C 1	1 C 2	2 C	2 C 1	2 C	C 3	1 C	2 C 3	1 C 1
K 1	1 K 1	K	2 K	3 K 3	2 K 3	3 K 3	1 K	1 K	K	3 K 1
1 N 1	1 N	N	N	2 N 2	1 N 1	2 N 2	1 N 3	N 3	N 1	2 N 1
2 F 1	F 2	F	F	F 1	1 F 3	F 1	2 F 1	3 F	1 F	F 1
2 V 3	3 V 1	V 3	2 V 2	1 V 2	1 V	1 V 2	2 V 1	V 2	V	1 V 1
1 H 2	3 H 2	1 H 1	3 H 1	H	H 1	H	1 H 1	1 H 1	H 2	H 1
R 2	3 R 3	2 R 2	1 R	1 R 1	1 R	1 R 1	R	2 R 1	1 R	R 2
3 G	G 1	3 G 1	1 G 2	G	1 G 1	G	1 G 1	2 G 2	G	G
S 1	S 1	3 S	S 3	1 S 2	1 S 1	1 S 2	2 S 2	S	1 S 2	S
3 M 2	M	1 M	M 1	1 M	2 M	1 M	M	1 M 1	1 M 1	M 1
1 B 1	1 B 3	1 B 2	1 B	2 B	2 B	2 B	B	B	1 B	B

Fig. 11—*Affixes of the most Frequent Elements in the Cryptogram*

An examination of the K-column conclusively showed me that V, H, R, B

[1] See chapter V, II, 1, a.

are consonants, these letters having large prefixes and suffixes; C and N and probably F appeared to be vowels in spite of the fact that each presents one affix. It must not be forgotten that the transpositional scheme might have brought some vowels against clear-E that would not be possible in clear language.

My conclusions were confirmed when I examined the probable consonants, viz., the V-, H-, R-, and B-columns, where large affixes against C, K, N and some against F are present. Again, F has no affixes with itself (column F) and no affixes with N, but it has some with C which only means that F could be one of those vowels, not E, which usually combines with other vowels (. . . AUX, . . . OU, . . . AIT, etc.).

I was justified in deciding upon C, K, N and F as probable vowels.

On the other hand, the matching of the K-column with the other three, C-, N-, F-, in order to determine the second equivalent of clear-E, proved to be a more difficult task. The four columns, in fact, look very much alike and exhibit the same characteristics. However, one certainty emerges clearly and that is: either C or N or F must be the other equivalent of clear-E: for, their frequencies are the only ones that, if added to the one of K, would total approximately to the normal clear-E-frequency.

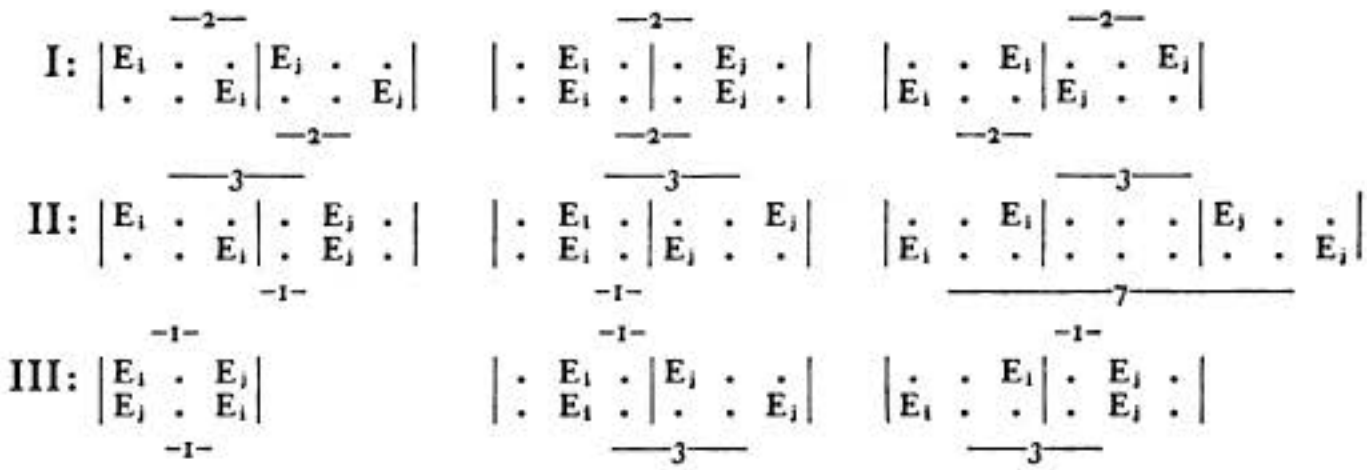
I devised a scheme to determine the other unknown equivalent of clear-E through a consideration of the high frequency of E.

The frequency range of clear-E oscillates between 15% and 20%. It means that, as a general average, every 5th or 6th element of a French text should be an E. But in reality the intervals between clear-E run sometimes as high as 15 or 20 letters. It follows that in many cases they are correspondingly nearer together.

It is possible to establish a frequency of intervals between clear-E. In looking through a number of French texts it can be noted that the most frequent intervals between clear-E are, in order of frequency, 2, 3, and 1, that is:

$$\text{I: } E_i \overset{-2-}{\ .\ .\ } E_j \qquad \text{II: } E_i \overset{-3-}{\ .\ .\ .\ } E_j \qquad \text{III: } E_i \overset{-1-}{\ .\ } E_j$$

Now, the possible results of the transposition by trigrams, operated upon the above combinations, showing the intervals after the transposition, are:



where the intervals, although at times interchanged, are still 1, 2 and 3. Consequently, by writing all the pentagrams beginning with crypto-K and tabulating the frequency of the elements on the 2nd, 3rd and 4th column following crypto-K—corresponding to intervals 1, 2, and 3—the most frequent element therein would very likely correspond to clear-E.

Accordingly, the following two tables were set up:

19	K	.	C	M	S
37	K	.	L	N	V
56	K	.	R	R	N
57	K	.	R	N	D
75	K	.	F	S	N
84	K	.	A	K	V
87	K	.	G	N	V
105	K	.	F	Q	U
121	K	.	K	R	O
123	K	.	O	D	N
133	K	.	G	G	N
141	K	.	V	H	N
152	K	.	N	V	K
156	K	.	D	Q	V
162	K	.	N	B	N
173	K	.	C	V	U
179	K	.	V	I	G
206	K	.	F	V	C

Fig. 12—*List of K-Pentagrams*

	C	L	R	F	A	G	K	O	V	N	D	M	S	Q	H	B	I	U	Totals
I:	II	I	II	III	I	II	I	I	II	II	I								18
II:			II			I	I		III	III	I	I	I	II	I	I	I		18
III:	I					I	I	I	IIII	IIIII	I		I					II	18
Totals	3	1	4	3	1	4	3	2	9	11	3	1	2	2	1	1	1	2	

Fig. 13—*Frequencies of Intervals of K-Pentagrams*

Fig. 13 unmistakably showed me that

crypto-N ≡ clear-E

and no doubt subsisted in my mind, as the next high-frequency element V, had already been established as a consonant.

A more exact computation should have taken in consideration the reverse K-pentagrams also. It would not have changed the result.

***

I had only *spotted* three of the possible five most frequent vowels—disregarding Y because of its rarity—but a search through the rare letters of the cryptogram would reveal others besides confirming previous findings. As we know, rare letters usually associate with vowels.

The rare letters with their affixes were separately tabulated:

	I	II	III	IV	V	VI	VII
A	S S B / K K M						
I		V V K N / C G C G					
L			N N F R / M G N S				
O				R K / D N			
P					U M H / M C B		
T						F Q V / K S K	
Z							C / F,

and the frequency of their affixes appearing more than once—S, B, K, M, V, N, C, G, F and R—were noted,

Element	I	II	III	IV	V	VI	VII	Total	
S	2	–	1	–	–	1	–	4	← possible vowels
B	1	–	–	–	1	–	–	2	
M	1	–	1	–	2	–	–	4	← possible vowels
K	2	1	–	1	–	2	–	6	← vowels decided upon
V	–	2	–	–	–	1	–	3	
N	–	1	3	1	–	–	–	5	← vowels decided upon
C	–	2	–	–	1	–	1	4	← vowels decided upon
G	–	2	1	–	–	–	–	3	
F	–	–	1	–	–	1	–	2	← vowels decided upon
R	–	–	1	1	–	–	–	2	

consonants already decided upon

Fig. 14—*Affixes of Rare Letters in Cryptogram*

revealing that the previous selections were well-founded, and, in addition, giving some indication as to the probabilities of "S" and "M" being vowels.

Reverting to Fig. 11 and studying the S-column, it was apparent that "S" is a vowel because it makes few contacts with the vowel group C, K, N, F and substantial ones with the consonant group V, H, R, G. Similarly, it was difficult to accept "M" as a vowel because, while it does not make *very* substantial contacts with the vowel group (if we add "S" to the vowel group, the contacts become substantial), it certainly is not any too friendly with the consonants V, H, R, G and B.

I reported these results on the cryptogram:

L M P C X B R L S Q H F M H H C B H K X C M S H Q B C U P M C C V F S

A K F L N V G S R X F C V B R S N X F T K K R R N D D Q G H Q X N L M

H F S V K R F S N I C R V K B A K V G N V C S G C N R S M M C H P B K

H F Q U C F U N X R V I G V T K H K R O D N R N B M R K F G G N C M C

K S V H N G S G C U R K G N V K D D Q V R K O N B N L G Q T S N K I C

V U K B V I G F G C Z F H U C H S A M N U C X F F V F C R H K B F V C

X N H G Q

Fig. 15—*Cryptogram with Four Principal Vowels*

Even though I had decided upon five elements representing principal vowels, totaling exactly 40% of the text, it was not possible to initiate a program of word-building in the cryptogram. The transpositional scheme, even assuming that it still consisted of reversed trigrams, would have led me into countless trials, especially considering that of the four vowels only "E" had been individualized.

The help of other factors was necessary. I decided to inquire into the most frequent bigrams and trigrams.

4

Frequent Polygrams

What is the effect of a group transposition upon bigrams and trigrams of a text? A short example will show it. All the possible bigrams and trigrams that can be derived from the word BINDER in the sentence THE BINDER WAS, are:

Bigrams		Trigrams	
1 —	EB	1 —	HEB
2 —	BI	2 —	EBI
3 —	IN	3 —	BIN
4 —	ND	4 —	IND
5 —	DE	5 —	NDE
6 —	ER	6 —	DER
7 —	RW	7 —	ERW
		8 —	RWS

Now, if the sentence is first divided into groups of three elements and the trigrams so obtained are then reversed, the bigrams and trigrams containing at least one element of the word BINDER are:

THE BIN DER WAS
EHT NIB RED SAW

Bigrams		Trigrams	
I	TN	I	HTN
II	NI	II	TNI
III	IB	III	NIB
IV	BR	IV	IBR
V	RE	V	BRE
VI	ED	VI	RED
VII	DS	VII	EDS
		VIII	DSA

If we compare the two lists of bigrams we will find that four of the seven bigrams are inverse to each other—2-III, 3-II, 5-VI and 6-V—that is 57%, while a comparison of the lists of trigrams will show that only two out of the eight will have the same quality—3-III and 6-VI—that is 25%.

The presence of nulls in the text would decrease these percentages still more.

The effect of a transposition by trigrams would, therefore, mask almost one-half of the bigrams and three-fourths of the trigrams. Bazeries certainly knew how to do things.

In the vain hope that a tabulation of the trigrams of the text (from which the bigrams, too, can be extracted) would yield some useful information, I prepared one with the help of Fig. 6 (see pages 32–33), but I was taken aback by the almost total absence of repetitions in the table: only two appearances each, in the groups of D, S and V emerged, viz.:

2—DDQ at 61 and 157
2—SGC at 93 and 147
2—VIG at 116 and 180.

Surely not much to speculate on.

With the hope that a list of the bigrams might prove more helpful, I decided to prepare it. Here is a tabulation of those appearing at least twice.

2—A K	3—H F	2—R S
2—B R	3—H K	2—R N
3—C X	2—H Q	2—R V
2—C M	2—I C	3—R K
2—C U	2—I G	2—S A
3—C V	2—K F	3—S N
2—C R	3—K R	2—S V
2—C H	3—K B	2—S G
2—D D	2—K H	2—T K
2—D Q	2—L M	3—U C
3—F S	2—M H	2—V F
2—F G	3—M C	3—V K
2—F V	3—N V	2—V C
2—G S	2—N X	2—V I
3—G N	2—N L	3—X F
3—G C	2—N V	2—X N
2—G Q	2—N R	
	2—N B	

Fig. 16—*Table of Repeated Bigrams in Cryptogram*

(3) C V	V C (2)
(2) C M	M C (3)
(2) C U	U C (3)
(2) F V	V F (2)
(2) G S	S G (2)
(2) H K	K H (2)
(2) H Q	Q H (1)

Fig. 17—*Table of Reversed Bigrams*

Remembering that at least one-half of the bigrams in the list are *false* as a result of the transposition, I felt that any research tending to establish a coincidence between the crypto-bigrams and the most common bigrams of the French language would prove futile. The elements for comparison were too meager to warrant a continuation of the work through analytic channels.

5

"*Probable Words*"[1]

In this category of researches, besides the essays on probable full words, are also included those which have as bases fixed sequences, such as QU and endings of words, such as ENT, EMENT, etc. I tried several of them.

A) THE FIXED SEQUENCE QU

We have already seen the effect of the transposition of bigrams with fixed sequence. (See page 57.)

From the table of frequencies, Fig. 7, it could be surmised that crypto-I might very well stand for clear-Q. There being only four crypto-I at 80, 117, 174 and 181, I tried them.

	80						80				
Group:	I C R	V K B	A K V	suggested	I C R	V K B	A K V	, which
	Q . .	. E .	. E .		Q A .	L E U	. E L	
	Q	E	E		. A Q	U E L	L E .	

looked possible in view of the frequencies of crypto-V and clear-L were 7% and 6.1% respectively.

Upon trying these values on the other three crypto-I

	117				174		181 [2]
U N X	R V I	G V T	and	I C V	U K B	V I G
	. L Q	. L .		Q A L	. E U	L Q .
	Q L .	. L .		L A Q	U E .	. Q L

[1] All the essays on probable words took place before I performed the analytical work previously described, so that no knowledge later acquired was used. I had, however, made the crypto-K = clear-E assumption at the time.

[2] I tried different group subdivisions. Those given here seemed the most likely.

I was stopped rather abruptly by the sequence QL, even though I had tried to make $\left|\begin{matrix}U&N&X\\N&I&C\\C&I&N\end{matrix}\right|\left|\begin{matrix}R&V&{}^{117}I\\&L&Q\\Q&L&\end{matrix}\right|$ or *cinq l*, before reading the next combination. Nothing could be made out of this.

***

With the same assumption, that is, crypto-I equals clear-Q, I then attempted:

$$\left|\begin{matrix}{}^{80}I&C&R\\Q&E&L\\\underline{L}&\underline{E}&\underline{Q}\end{matrix}\right|\left|\begin{matrix}V&K&B\\I&A&U\\\underline{U}&\underline{A}&\underline{I}\end{matrix}\right|,$$

which seemed perfectly acceptable (some fight might have taken place at one of the many *quais* in Paris). It gave up the possible trigram $\left|\begin{matrix}{}^{117}I&G&V\\Q&N&I\\I&N&Q\end{matrix}\right|$. But, upon transferring the values to $\left|\begin{matrix}{}^{174}I&C&V\\Q&E&I\\I&E&Q\end{matrix}\right|\left|\begin{matrix}U&K&B\\.&A&U\\U&A&.\end{matrix}\right|\left|\begin{matrix}V&I&G\\I&Q&N\\N&Q&I\end{matrix}\right|$, I again found myself facing an impasse.

The assumption crypto-I ≡ clear-Q was definitely abandoned.

***

Still the combination . . ELLE in A QUELLE at 80 (see: *supra*) looked promising and I would not give it up. By frequencies I concocted:

$$\left|\begin{matrix}{}^{80}I&C&R\\U&O&N\\\underline{N}&\underline{O}&\underline{U}\end{matrix}\right|\left|\begin{matrix}V&K&B\\L&E&V\\V&E&L\end{matrix}\right|\left|\begin{matrix}A&K&V\\.&E&L\\L&E&.\end{matrix}\right|,\text{ which yielded }\left|\begin{matrix}{}^{174}I&C&V\\U&O&L\\L&O&U\end{matrix}\right|\left|\begin{matrix}U&K&B\\\underline{R}&E&V\\V&E&\underline{R}\end{matrix}\right|\left|\begin{matrix}V&I&G\\L&U&\underline{T}\\\underline{T}&U&L\end{matrix}\right|,\text{ suggesting}$$

l ouvert ul, more or less passable—rather less.

On prosecuting the search, I again found myself in a blind alley.

***

I changed my route. The two bigrams SA–35 and SA–192 were assumed to stand for clear UQ. In fact:

35					192			
F	S	A			H	S	A	
(A	U	Q		and	(I	U	Q	
(I					(A			
Q	U	A)			Q	U	I)	
		I)					A)	

seemed probable.

The trials at crypto-A-86 determined the subdivisions in the places shown in the following figure, so that Q and U could be brought together:

86										
A	K	V	G		N	V	C	S	G	C	N
Q	E				.		.	U	.	.	.
.	E		Q		U		.	.	.	.	.

The presence of V in the first two tetragrams suggested the hypothesis of V being a null; in this case the two C would be in the center of the last two trigrams and by their frequency might be equal to clear-E. The two extreme N in the same trigrams, then, could easily be made to represent clear-L. The two G, if made to coincide with clear-D, would result in the perfectly acceptable subsequence:

86										
A	K	(V)	G		N	(V)	C	S	G	C	N
G	E		D		L		E	U	D	E	L
D	E		Q		U	E		L	L	E	D

I tried to exploit this possibility and divided the entire cryptogram into trigrams, cancelling all V and substituting the values thus assumed.

It was just a case of another seemingly good attempt *gone with the wind*.

Assuredly I was not in luck with the most tell-tale bigram of them all: the venerable QU.

B) VARIOUS WORDS

The technique used to ferret out probable words is the same as the one applied to trigrams. However, these words are generally selected for their pattern, that is, for the various like elements they contain. There is no need, therefore, to compare frequencies until a pattern, similar to the clear-pattern, has been discovered in the cryptogram. Hence, it is preferable to bring out in such words their *repetitive qualities*.

For instance, the word *magistrat* can take the following forms:

M A G	I S T	R A T	or	. M A	G I S	T R A	T . .	or	. . M	A G I	S T R	A T .
G A M	T S I	T A R		A M .	S I G	A R T	. . T		M . .	I G A	R T S	. T A

each of which is marked at the top of a square-ruled sheet or strip as given below and tried separately by sliding the strip along the entire cryptogram:

```
  ○ ●  ●○     ○       ○  ● ●          ○  ●  ●○
GAMTSITAR  AM.SIGART.T  M..IGARTS.TA
```

I tried the words:

MAGISTRAT	(magistrate)
CASSATION	(Court of Appeals)
COMMISSAIRE	(Police Commissioner)
COMMISSARIAT	(Police Station)
ARRONDISSEMENT	(A regional division of a city. It is invariably recorded in police reports and addresses.)
ASSISES LES ASSISES	(Assize-Court)

I will not give the various trials I made, except two: those on the words COMMISSARIAT and ASSISES. They gave me some genuine hopes.

C) THE WORD "COMMISSARIAT"

The usual transformation of commissariat produced the pattern

. . C	O M M	I S S	A R I	A T .
C . .	M M O	S S I	I R A	. T A

with three doubletons very close together. I had noted in the cryptogram a similar subsequence

```
   56
K  K  R  R  N  D  D,
```

but the doubletons were in reverse position. Was it possible that the cryptogram would have to be read in a reverse manner?

C . .	M M O	S S I	I R A	. T A
H G Q	D D N	R R K	K T F	X N S

The frequencies of the crypto-elements and the assumed values proved to be within acceptable ranges but the values F and S for the two clear-A could not be entertained. Further investigation led to a blank wall.

D) THE WORD "ASSISES"

In view of the dénouement in the preceding chapter, the trials on the word *assises* may be considered fairly dramatic. This word was the villain of the piece. I made it the especial object of my solicitude. I combined its elements in every possible way.

Nothing.

Still, I was convinced, more than ever, that this rascal of a word was hiding among these letters:

8
L S Q H F M H H C B H K X . .;

its general physiognomy could be plainly recognized but most of its component parts, for some mysterious reason, could not be brought together.

Yet it seemed that the beginning of a newspaper item dealing with judicial news might conceivably be:

Les assises de...
Aux assises de...
La cour d'assises de...

and I continued to hammer at the combination with all the perseverance I could muster.

The best of the three transposed combinations of *Les Assises* was:

L E S	A S S	I S E	S . .
S E L	S S A	E S I	. . S

which yielded

9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24
S	Q	H	F	M	H	H	C	B	H	K	X	C	M	S	H
		S	E	L	S	S	A	E	S	L	.	.	S		

The lack of coincidence of column 22 with columns 11, 14, 15 and 18 did not ruffle me, for it might have been the effect of a different transpositional grouping or of some nulls, there being another "H" at 24. The equivalences at columns 16, 19, 13 and 12 were all possible because of frequencies. But B ≡ E at 17 I could not very well accept and I was lukewarm to K ≡ L at 19, having assumed crypto-K to be equivalent to clear-E. Of course, the assumption could be wrong.

***

By sheer computations of frequencies I decided, at one time, on the following values:

11	12	13	14	15	16	17	18	19	20	21	22	23	24
H	F	M	H	H	C	B	H	K	X	C	M	S	H
S	I		S	S	A	D	S	E	T	A		O	S
S	I		S	D	A	S	T	E	S	S		O	A
		1			2			3					

which yielded by making M a null and reading the groups in the order 2, 1, 3.

(Cour) D'ASSISTES

↑Probable error(?)

but when I followed it up, I again found myself in a maze.

After innumerable other trials I finally gave up, reluctantly. "Assises" had proved a most elusive little rogue for my wits and I again conceded defeat. I was certainly fishing in troubled waters.

III. ENGLISH ADAPTATION

I feel that students will welcome an adaptation of the technique herein described to cryptograms obtained from English texts, ciphered by means of Bazeries' "paper and pencil" system.

It is very seldom that text books or papers on cryptanalysis include examples for practice. I do not know why it should be so, but I am inclined to think that it is a mistake. Compelling students to prepare their own exercises in order to put into practice the notions they have just acquired is not the proper way to test whether they have really absorbed them or not.

Of course, the journals of the various Cryptogram Associations are, in a sense, filling this want, but I find that they feed their readers a rather

monotonous fare. An addition to the usual diet of simple substitutions, simple transpositions and the various derivatives of the Vigenère type of multiple substitutions, should prove refreshing.

For these reasons, I have thought it desirable to append some graded exercises on this interesting type of combined substitution and transposition.

1

Basic Forms of English Numerals

The English words used to form cardinal numerals are few. To denote numbers containing from one to six digits, those given in the following list are combined in accordance with well-known rules:

—	ten	—	hundred
one	eleven	—	thousand
two	twelve	twenty	
three	thirteen	thirty	
four	fourteen	forty	
five	fifteen	fifty	
six	sixteen	sixty	
seven	seventeen	seventy	
eight	eighteen	eighty	
nine	nineteen	ninety	

Cardinal numerals as used in our cipher are adjectives. They, therefore, are invariable and no connective is necessary to link them when combined.

An analysis of the list discloses some peculiarities, analogous to those described for the French numerals. Similarly, they will be called "propositions." They are:

[1] This is only true for numerals smaller than (ONE) MILLION, which are large enough for the practical purpose of the cipher. Otherwise: MILLION contains M; BILLION contains B; QUADRILLION and QUINTILLION contain Q; SEPTILLION contains P; OCTILLION and DECILLION contain C. Propositions II, III, V, VI and VII are also so limited.

The element U appears only in FOUR, FOURTEEN, HUNDRED, THOUSAND..... Pp. VII

" " V " " " FIVE, SEVEN, ELEVEN, TWELVE, SEVENTEEN, SEVENTY..... Pp. VIII

" " F " " " FOUR, FIVE, FOURTEEN, FIFTEEN, FORTY, FIFTY..... Pp. IX

The elements S,O,F,T,E,N, are the only initials of English numerals. Pp. X

Initial pentagrams of all numbers from 11 to 999,999 are:

A: From 11 to 99

Form 1	ELVN-	for 11.	Form 12	FORTY	for 40–49.
2	TWELV	12.	13	FITY-	50.
3	THIRE	13.	14	O	51, 54.
4	FOURT	14.	15	W	52.
5	FITEN	15.	16	H	53.
6	SIXTE	16.	17	V	55.
7	SEVNT	17, 70–79.	18	S	56, 57.
8	EIGHT	18, 80–89.	19	E	58.
9	NIET-	19.	20	N	59.
10	TWENY	20–29.	21	SIXTY	60–69.
11	THIRY	30–39.	22	NIETY	90–99.

B: From 100 to 999:

Form 23	ONEHU	for 100–199.	Form 28	SIXHU	for 600–699.	
24	TWOHU	200–299.	29	SEVNH	700–799.	
25	THREU	300–399.			800–899.	Form (8)
26	FOURH	400–499.	20	NIEHU	900–999.	
27	FIVEH	500–599.				

C: From 1000 to 9999: Using THOUSAND as component:

Form 31	ONETH	for 1000–1999.	
		2000–2999:	Form (24)
32	THREO	3000–3999.	
		4000–4999:	" (4)
33	FIVET	5000–5999.	
34	SIXTH	6000–6999.	
		7000–7999:	" (7)
		8000–8999:	" (8)
35	NIETH	9000–9999.	

Or using HUNDRED as component:

Form 36	TENHU	for 1000–1099.			1500–1599:	"	(5)
37	ELVNH	1100–1199.			1600–1699:	"	(6)
		1200–1299:	Form	(2)	1700–1799:	"	(7)
		1300–1399:	"	(3)	1800–1899:	"	(8)
		1400–1499:	"	(4)	1900–1999:	"	(35)

for 2000–2999:	Form (10)	for 5500–5599:	Form (17)
3000–3999:	" (11)	5600–5799:	" (18)
4000–4999:	" (12)	5800–5899:	" (19)
5000–5099:	" (16)	5900–5999:	" (20)
5100–5199:	" (14)	6000–6999:	" (21)
5200–5299:	" (15)	7000–7999:	" (7)
5300–5399:	" (16)	8000–8999:	" (8)
5400–5499:	" (14)	9000–9999:	" (22)

D: From 10,000 to 99,999:

Form 38 TENHO	for 10,000–10,999.		for 19,000–19,999:	Form (35)
39 ELVNT	11,000–11,999.		20,000–29,999:	" (10)
	12,000–12,999:	Form (2)	30,000–39,999:	" (11)
	13,000–13,999:	" (3)	40,000–49,999:	" (12)
	14,000–14,999:	" (4)	50,000–59,999:	" (16)
	15,000–15,999:	" (5)	60,000–69,999:	" (21)
	16,000–16,999:	" (6)	70,000–79,999:	" (7)
	17,000–17,999:	" (7)	80,000–89,999:	" (8)
	18,000–18,999:	" (8)	90,000–99,999:	" (22)

Since the initials of English numerals are S,O,F,T,E,N, we will group the 39 basic forms just established in accordance with their initials, and divide them in classes:

TABLE IV: BASIC FORMS OF ENGLISH NUMERALS

I: EIGHT	(8)	VI: FORTY	(12)	XIII: SIXHU	(28)
II: ELVN-	(1)	VII: FOURH	(26)	XIV: SIXTE	(6)
ELVNH	(37)	FOURT	(4)	SIXTH	(34)
ELVNT	(39)			SIXTY	(21)
III: FITEN	(5)	VIII: NIEHU	(30)	XV: TENHO	(38)
				TENHU	(36)
IV: FITY-	(13)	IX: NIET-	(9)	XVI: THIRE	(3)
FITYE	(19)	NIETH	(35)	THIRY	(11)
FITYH	(16)	NIETY	(22)	XVII: THREO	(32)
FITYN	(20)			THREU	(25)
FITYO	(14)	X: ONEHU	(23)		
FITYS	(18)			XVIII: TWELV	(2)
FITYV	(17)	XI: ONETH	(31)		
FITYW	(15)			XIX: TWENY	(10)
V: FIVEH	(27)	XII: SEVNH	(29)	XX: TWOHU	(24)
FIVET	(33)	SEVNT	(7)		

2

Exercises

Note I:

In the following exercises:

a) The indicatory elements have been introduced at random. Had a uniform rule been followed, students would be tempted, after the first decrypting, merely to decipher the rest. The indicatory elements have been given to enable the students to check the crypto-alphabet after their reconstitution.

b) Crypto-alphabets have been set in the crypto-squares in accordance with Bazeries' scheme, that is: simple horizontal pattern.

Note II:

For exercises Nos. 1, 2, 3, 4 and 5:

a) The numerical values of the indicatory elements have been derived from *normal* alphabets.

b) The clear alphabets have been set in the clear square in accordance with Bazeries' scheme, that is: simple vertical pattern.

c) Nulls have been introduced.

Note III:

For exercises Nos. 6 and 7:

a) The numerical values of the indicatory elements have been derived from straight alphabets.

b) The clear alphabets have been set in the clear square in one of the two simple diagonal patterns.

c) Nulls have been introduced.

Note IV:

For exercise No. 8:

a) The numerical values of the indicatory elements have been derived from straight alphabets.
b) The clear alphabet has been set in the clear square in a vertical pattern and has been mildly diluted.
c) No nulls have been introduced.

Note V:

For exercises Nos. 9 and 10:

a) The numerical values of the indicatory elements have been derived from reverse straight alphabets.
b) The clear alphabets have been set in the clear squares in one of the two alternate diagonal patterns, and they have been appreciably diluted.
c) Nulls have been introduced.

Exercise No. 1:
50 Groups

MBVBP	HMVGN	THTNN	IPPCV	HMVGP	TSOTV	TAPAS	CTDVK	CLELB
LVGPC	VCBVM	VVHTL	KBOBG	PPCVY	SOOLV	IUUKV	PTLIV	MQAVB
QTSMV	GPPMV	GNFSP	YTUMQ	BPHVG	VAUVS	IDTUL	PDSVL	DLPBV
GLSLH	BYIDB	YMVPB	XVGMS	SONCC	VHMGP	TTDVX	ULTTB	OKBMD
KIYVN	VSMWD	VBTKY	PCBSB	LMXOB	LCPUV	PNMXT	SMQSX	SSYBT
UBVLP	GPBDV	YMHVC	SHMGP	TAVFS				

Exercise No. 2:
54 Groups

NDJGK OPIDL PJPIG YLNPD KVIGK VGORF GIHUD MLGKY CVVPY
LLFIP JKACE SYXKG NVDCV FAUGL UDGND AIPSD AWGLL FSLMP
SVUDP PPLYJ CAAPP GLVFP TUFVK WAQGU PGVGE PIFAE IXKWI
PGYDV GAJUP SUVFA CIKLW KCPPU FAUTO KSSYG TPIPD GPOVI
IKGLS LKKEP AFOXV FXLYJ INCPM PSLDE IPFLB VSVMP PJPUD
YCPLP VPHLI WKKCG HPJTA XGASL XGOOY VPGLF EAUIY UFBLO

⁂

Exercise No. 3:
44 Groups

DQSEC QOLSD LOBRV DWKQH EGBXD CUWGO ELLFC YMNVD NCNCH
FCSDR XKMSI ICGCX SKLVE OXYLL UOESY ROHHS FKNAV LWFVS
QKKRO FVSCD NCNCH FLFCO YLFOD OELVI KVYLK HOOEU FDFOK
HLOEU FDFOL VLDKD VOUOF CSBOS LVCLE SFKMD DKIKX QHFDO
BKCXS CDNON CMDXV SRXVM SFSLF EKVCC GRXSS OEFKQ

⁂

Exercise No. 4:
46 Groups

PFLRS PAPQF LPPRV KDSEQ PBCSK CLELR VFPGL EPUBS KDPNV
CUKVC SWOUP UCQLR CVLSP KPQEU SIEPI PFRSK ILCBK LYRRE
FLPBS IPPOF DVEPT KSVPU VSILK PFLUV KDLGW UPPLE QBPII
KCRVT IVCPV ESDBV EPSCK LVPDY BPFLU KCKLL VCFEL CPQEC
GVGVC RVYED OVCFS OEPKD LECNU VLEBP DELQF LVKYE PREEC
SLXRV

⁂

Exercise No. 5:

50 Groups

CFFSN MRCGP LXSKP EKLGT GDPEX IPPGO TEETE TOFTC IKKFT
LNPIC VGFAK ERLPG FTALK YPAOX CPQTL KITSK FLSYI FXXKA
LWLFS LGERK RKSFI XLTFF YDIAL RLFBP PGPWC PRFTE PSMOL
ETALI FLTLE VPAGP GKPEX KWXKO NEQST KYPCO XCVRK SXOPL
EDPAP PQPUK DXIER LLIPS KTKME ELXKP LEXRE GIPUP WFEXP
ALTGE OKMOY KITCF YIXOO FMODI

***

Exercise No. 6:

33 Groups

QOHCR QJDGV WFZDN VWVOD YGQWF SDWEK NLNJM DDUVN JLNSK
DLLQD SHLFM NPZON SFVYS PEINK LNFLD UWNOY CCFNE QQFOV
NLUJP ELDNI JFKLW CLNTD WDQNW GYCDY QFNEQ QJDSU NSWCN
YTHGS DYSNY SKQLN SFFHN LQXQN LHZAV

***

Exercise No. 7:

41 Groups

VFSZS WFGKV FEDAT OWSAR SWWKN OYDAW DWYOY OAXZN AFWAS
VFWOV FFZOB SDARW KZFEO ESUWZ DWKSR TEEAY AZSDY FOXSO
AZWSZ GSHEF NZOXD NYKYY DFARA AOYDZ KWGSZ SRYZA VPTWA
VNDYK AFWEA FURSA FCHSV ZSWSS ZFYOG BAFSG AXZOF AHCAW
DFYDA FEDWS VGSUG SQAAF YSZLW

***

Exercise No. 8:

54 Groups

GOEBY BVVQZ DMESC VQBDS OMUVY QNQMG BCEVA QFXHG ACEFN
ZGODR XSEDW GFCGL ECVEK BXSMO DXZML MTBQS VCLZC SEHYD
XCSXN FRFSO VCBKX SOYEW OMFGX SHMFX BYQCM YXXSQ OESMC
GDREK BVMOB AUQCG EQGRS VVVBS DYDZG EEQGO KOADS ASEQD
EVEYM OCEQM SXRGL MCDOE WVSGX XDAZG CMUBR QQMEB YVQMR
REZGO RLBED VGCMZ EQTVX DBKQB OCVDK XXHSE VGEEQ GEQBD

***

Exercise No. 9:

53 Groups

PEHFR	OKMIE	WCCFX	LOBIF	MXRAA	DOCSI	REXEU	ABWBF	MEAIS
HTPOC	XBEFD	LCZFI	UBYEU	ABFXS	RBRKM	TSFUB	VYOOR	XWAZH
SLVVD	YLRKM	EMFRO	BVPSR	RVXHI	ESUMZ	LDCBX	MIERR	STBAD
OASEV	OUEOR	MSAAE	MZNXV	DREBM	XULFR	EFROR	VISGB	IUBMF
MFSRT	LLCLE	SYVSX	IOUAV	NFCBU	WVSMM	CFSEF	IVIRY	HIEFU
WHEUU	NFREU	HBHEO	MFRDX	FUIFF	DMEEY	RIMXM	ISOMI	

***

Exercise No. 10:

35 Groups

QDBPL	BTFDI	LCYVG	DIWIF	SGIES	ISABI	AIIUD	QKOCV	BCYTZ
WDZYP	DNHDB	TQVFD	STACS	BCLDA	TEAUV	GAWWD	OOZIK	VFDAZ
ODTDU	MCDCM	ZLBIC	OFDVS	TBHPD	IEAOU	IAZRC	UHKWS	MCBZQ
STSDD	ACBLA	ITCBH	DTLVF	TCIFH	ADAFU	TBZCA	ASPWT	

Appendix I

A. ESSENTIALS OF CRYPTOGRAPHY[1]

1. The language we use in our everyday life is called *clear language*. Its graphic representation is called *clear writing*. The meaning of *clear-letter*, *clear-text* or *clear-message* is, therefore, obvious. Clear writing is characterized by the fact that as we read it, its meaning is *instantly* clear to us.
2. Writing, the reading of which is not instantly clear to us[2] but which has a hidden meaning is called *secret writing*.
3. There are many forms of secret writing. The most important one is *ciphered writing*.
4. Ciphered writing is nothing more than a transformation of clear writing which is accomplished by following certain specified conventions agreed upon beforehand by the correspondents. Obviously, a jumbled series of letters having no concealed meaning is not secret writing.
5. *Cryptography* (from the Greek κρυπτός, *hidden, secret*, + γραφία, γράφειν, *write* is therefore the science that teaches us how to transform clear writing into ciphered writing and vice versa.
6. The set of conventions used by correspondents in transforming writing from one type to the other is called *cipher* or *key*. Often the key is simply a word or a phrase performing some specified function. These are called *key-word* and *key-phrase*.
7. We shall call *element* any letter belonging to a text. When we wish to be more specific, a *clear-element* will denote one belonging to a clear

[1] We use the word *essentials* advisedly. The contents of this appendix are but a small fraction of the notions of even elementary cryptography. They are, however, sufficient for an intelligent reading of the text.

[2] Of course, we do not mean writing in a foreign language we do not know nor writing making use of characters different from those with which we are familiar, even though the writing, in these cases, is intrinsically secret. Moreover it has been used as such.

text; a *crypto-element*, one of a ciphered text. A ciphered text is often called a *cryptogram*. The transformation of a clear text is called *ciphering*; the transformation of a ciphered text is called *deciphering*.

8. In the process of transformation the normal subdivisions between words of a text are disregarded. A message about to be ciphered is written continuously. For this reason we sometimes call an entire message a *sequence*. Any part of a sequence is a *sub-sequence*. Subsequences of two, three, four, five, six and seven elements are generally called *bigrams*, *trigrams*, *tetragrams*, *pentagrams*, *hexagrams* and *heptagrams*. Cable regulations, on the other hand, direct that unpronounceable secret communications be divided in groups of five (5) letters. This is the reason cryptograms are usually written in series of pentagrams.

***

9. The alphabet of our language, in the order in which we learned it in our early school days, that is from A to Z, is called a *normal* alphabet. An alphabet beginning with any letter other than "A" but preserving the same order as the normal one is called a *straight* alphabet and is generally denoted by its initial letter. Thus the *straight*-D alphabet is DEF.....ZABC. An alphabet, the elements of which do not preserve their normal order, is called an *incoherent* alphabet.
10. Obviously, it is not possible to remember the order of the elements of *any* incoherent alphabet. There are, however, many devices, *easily* remembered, that teach us how to construct incoherent alphabets. Some devices are, of course, more effective than others in yielding alphabets with a greater degree of incoherency.
11. One such device consists in writing first a secret word, otherwise known as key-word, taking care to omit the repetition of similar letters it may contain, followed immediately by all the other letters of the alphabet not appearing in the key-word, in their alphabetical order. If the key-word were *general* the resulting incoherent alphabet would be:

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

It is evident that a short word does not yield much of an incoherent alphabet. Long words or phrases are ordinarily used to remedy this defect. For instance, the phrase *His Britannic Majesty's Ambassador* would give us:

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

which is sufficiently incoherent for any purpose.

***

12. There are two distinct classes of ciphers. Those in which the transformation is operated upon the single elements or, at the most, upon two or three elements of a text at a time, are called *alphabetic ciphers*. Those in which the transformation is operated upon syllables, whole words, phrases and full sentences are called *codes*.
13. Codes, even when not very bulky, are generally considered worthless for field use in military operations. They can easily get lost or fall into the hands of the enemy. Of the alphabetic ciphers, those requiring no written notes, or, at most, those that require conventional printed tables which can easily be constructed if lost, and, *at the same time*, do not disclose the secrecy of the cipher if seized by the enemy, are ordinarily used.

***

14. There are innumerable systems of alphabetic ciphers. Human ingenuity is boundless. Yet, they can all be reduced to just *two* general types:

    a. Those in which the elements of the sequence lose their identity and are substituted with other elements but preserve their position in the sequence, called *substitution ciphers*. For instance, if the table of equivalence

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

has been established, the sentence "HE HAD BEEN DEALING" will become

.... HEHAD BEEND EALIN G....
.... AOASN TOODN OSBPD R....

b. Those in which the elements preserve their identity but change their position in the sequence, called *transposition ciphers*. For instance, if it has been agreed to write a text horizontally in five columns and then cipher by reading the columns vertically, the same sentence will become

CLEAR
H	E	H	A	D
B	E	E	N	D
E	A	L	I	N
G				

CRYPTO: HBEGE EAHEL ANIDD N

***

15. There are a great many systems of substitution ciphers. Some make use of a single crypto-alphabet and are called *mono-alphabetic substitutions*; some make use of several crypto-alphabets and are called *poly-alphabetic substitutions*.
16. Of the mono-alphabetic systems, the simplest is the one first used by Julius Caesar[1] which consists of a straight crypto-alphabet against the clear-normal, such as:

TABLE I

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

The above table is called the ciphering alphabet. The deciphering alphabet would be written as follows:

TABLE II

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

You will notice that each vertical pair in Table I appears in Table II

[1] Julius Caesar actually used a straight-D alphabet.

in a reversed form. Of course, with simple alphabets of this kind there is no necessity for establishing the two tables of equivalence. The first one will suffice for both ciphering and deciphering.

17. A less simple substitution will naturally be obtained by using an incoherent crypto-alphabet instead of a straight one.

*
* *

18. There are a great many systems of transposition ciphers. The simplest one is the "*Hebrew*" transposition which consists in writing the full sequence in reversed order. Thus the sentence, "I WILL NOT COME," becomes:

E M O C T O N L L I W I

which can easily be read from right to left.

19. A less simple system is to divide the sequences into equal or unequal subsequences as might be agreed and then reversing the order of the elements in each subsequence.

The same sentence divided in trigrams, tetragrams or serially in groups of 4, 5, 3, will respectively yield the following secret texts:

CLEAR:	**I W I**	**L L N**	**O T C**	**O M E**	
CRYPTO:	I W I	N L L	C T O	E M O	, or IWINL LCTOE MO.
CLEAR:	**I W I L**	**L N O T**	**C O M E**		
CRYPTO:	L I W I	T O N L	E M O C		, or LIWIT ONLEM OC.
CLEAR:	**I W I L**	**L N O T C**	**O M E**		
CRYPTO:	L I W I	C T O N L	E M O		, or LIWIC TONLE MO.

*
* *

20. Very often, for the sake of greater security, the two systems are combined; i.e., the clear text is first subjected to a transformation of one type, and the resulting cryptogram is in turn subjected to a transformation of the other type. We have in this case an example of *superciphering*.

B. ESSENTIALS OF DECRYPTING

21. *Decrypting* or *Cryptanalysis* is that discipline which teaches us how to attempt the restoration of ciphered texts to their intended meaning without the knowledge or use of the cipher or key involved.
22. There are no fixed or, so to speak, mathematical rules of decrypting for all systems. Very few types—relics of former ages, held then in great esteem but hardly ever used today—are susceptible of an almost mechanical solution.
23. The bases upon which decrypting mainly rests are:

I: The use of the quasi-scientific statistical material derived from linguistics.
II: The determination of the degree of vulnerability of a given system obtained from a complete or partial knowledge of the system (its rules of composition).
III: The knowledge of all factual circumstances surrounding the issuance of the secret text under consideration.

The first two are analytical operations, the third is casual and depends on chance. We will briefly outline them.

A: LINGUISTICS

24. The elements of any alphabet are divided into vowels (sounds at rest) and consonants (sounds in suspension). Consonants readily associate with vowels and the reason is obvious. On the other hand, there are some consonants which readily associate with others (friendly), some rarely do or refuse altogether to do so (unfriendly). By uniting a vowel with a consonant or with a group of friendly consonants we obtain an articulate sound. Speech, or its graphic symbolism, is a succession of articulate sounds.
25. If articulated sounds were each composed of only one vowel and one consonant, it would follow that in any given text consonants and vowels would be in equal number, or if the language admitted also single vowel words (such as "A" and "I" in English) then the vowels would slightly outnumber the consonants. But, besides affecting friendly consonants,

languages emphasize some of them (double consonants) and as a consequence the number of consonants is slightly larger than the vowels.

26. Now, some languages have a lesser number of friendly consonants than others or they affect redoubling in a lesser degree. Therefore, they are richer in their proportion of vowels.

27. Some consonants are more or less predominant than others due to a variety of causes, the principal of which are the laws of inflections: formation of feminines, plurals, comparatives, superlatives and adverbs; the endings of verbal forms; etc.

28. Having established the concept that some letters are more or less frequent than others, we are now in a position to enunciate the *principle of frequency*.

    In any number of sufficiently long ordinary texts of the same language, containing the same number of letters, the frequency of each element, of bigrams, trigrams in each text is very nearly constant. That is to say, in each one of the texts under consideration we will find an almost equal number of "a," "e," "t," "s," etc.

29. Frequency is the *most powerful weapon* of cryptanalysis. Tabulations of the frequencies of each element and of the most common articulated sounds, friendly consonants, bigrams, trigrams, etc., have been prepared for all modern languages and are constantly used in decrypting.

30. Although we shall have no occasion to use this information, the frequencies of the alphabetic elements relating to the English language are here given for the sake of curiosity:

Elements:	A	B	C	D	E	F	G	H	I	J	K	L	M
%	8	1^7	3	4	13	2^7	2	5	7	1	6	4	2^8

	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
	7	7^8	2^1	0^1	6^4	6^3	8^6	2^6	1^1	2^1	0^1	1^9	0^1

or as is often necessary to use, in the form of a descending series:

High Frequency

E	T	A	O	N	I	R	S	H
13	8^6	8	7^8	7	7	6^4	6^3	5

Middle Frequency

D	L	C	F	U	M
4	4	3	2^7	2^6	2^8

Low Frequency

W	P	G	Y	B	V
2^1	2^1	2	1^9	1^7	1^7

Rare Letters

K	X	J	Q	Z
0^6	0^1	0^1	0^1	0^1

from which we derive that in English the vowels AEIOUY form 40% of the total elements of a text.

It must be borne in mind that these values are not absolute and that the frequencies of some special texts will not always approximate the ratios given above. Even ordinary texts will, at times, diverge considerably. Other facts of note are:

a) Most frequent bigrams: th, he, an, er, on, re, in, ed, nd, at, of, or, ha, en, nt, ea, to, ti, etc.
b) Most frequent trigrams: the, and, tha, hat, edt, ent, for, ion, nde, tio, has, men, nce, sth, etc.
*c) J and V are always followed by a vowel.
*d) Q is always followed by U.
*e) X, with few exceptions, is most invariably preceded by a vowel; it is very frequently followed by a vowel.

B: VULNERABILITY

31. The knowledge of the operative rules of a system determines the degree of its vulnerability. The most vulnerable factors of a system are the repetitions it yields. For instance, in a mono-alphabetic substitution the crypto-sequence *mirrors* ALL the linguistic peculiarities of its clear-sequence. It is its perfect image. We can easily pick out repetitions of elements, bigrams, and trigrams, etc. We can determine at times whole words by their individualistic pattern, words such as: philosopher, instinct, interpreter, ass assin, etc.
32. The images become fainter as the complications of the ciphering are increased, but generally there will be some left for a careful consideration. On the other hand, and this is more important, other types of tell-tale indices, peculiar to the particular ciphering system under scrutiny, emerge from the ciphered text, ready to give the system away.
33. In some systems, a close study of the elements with low or rare frequency proves sometimes very profitable. These elements behave peculiarly. They are the aristocrats of the alphabet. They have a marked predilection for the company of the Misses A.E.I.O.U. Through them, these

* General Luigi Sacco (*Manuale di Crittografia, Roma, 1936—XIV*) calls these elements *pilot letters*. It is an appropriate characterization that should be followed. We are very partial to this excellent manual, in our opinion the most thorough, the most logically presented and the most scientific modern work on elementary cryptography and decrypting. And the least verbose.

ladies are easily recognized, and their twin sisters, parading in the message, easily spotted.

34. Cryptologists have invented—it is a very logical corollary—several devices to side-track cryptanalysts. In mono-alphabetic substitutions for instance, they sometimes omit from the clear alphabet one or more of the rare letters such as, W or X or Q or J which, if required, can easily be represented in the clear-text by VV, KS, K and I, respectively. We would have no difficulty in recognizing *where*, *own*, *exist*, *fix*, *conquest*, *adjacent* if spelled *vvhere*, *ovvn*, *eksist*, *fiks*, *conkuest*, *adiacent:* It is a matter of. . . . visual habit. This device enables them to apply two or more crypto-values to the most frequent elements, especially the vowels with the result that their frequencies become *diluted*.

35. The multiple representation of some elements naturally increases the difficulty of correctly interpreting the clear-equivalents. A ciphering alphabet of this kind may look somewhat as follows:

Ciphering table: Key: The love of the three Kings.
in the clear: W = VV
X = KS
J = I

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

where clear-A can be represented either by crypto-T or crypto-Q and similarly, the three crypto-values O, J, W, may be given to clear-E and the two crypto-values M, X, to clear-T.

36. Another device to confuse the analyst is the introduction of *nulls*, or elements without value in secret text. A prearranged number of them are appended at the beginning and the ending of a cryptogram to hide the true location of these two very vulnerable points. When inserted in the body of a message they follow a preconcerted plan, often arithmetical. Their aim is twofold: firstly, to mask pattern words or easily recognizable frequent *adjacencies*; secondly, to exaggerate the frequencies of the letters being used as nulls.

37. The suppression of double letters in clear messages is often resorted to when dealing with mono-alphabetic substitutions. Their images in cryptograms are a valuable help to the cryptanalyst in determining

the elements preceding and following doubled crypto-elements. When the doubled element is a vowel, the preceding and next following elements are consonants, such as *soon*, *troops*, *seen*; when the doubled element is a consonant the others are vowels, such as in *attack*, *allies*, *successes*, unless the doubled element is at the end of a word, such as in *the success to be gained will depend upon three or four factors* . . . , in which case the rule is generally partially true.

C: EXTERNAL CIRCUMSTANCES

38. The most important factors that will facilitate decrypting outside of the statistical tables of linguistics and the study of vulnerabilities inherent to each ciphering system can be briefly summarized as follows:

For any system:

1. The knowledge of the language of the clear text.
2. The knowledge of the ciphering system or its general physiognomy. (This knowledge has been implied in our discussion B: Vulnerability.)
3. The general knowledge of the subject matter of the ciphered text.

For transposition ciphers:

4. The shorter the cryptogram, the easier it is to decrypt it. A long transposed text, if not of an easy type, is a laborious operation. The decrypting is generally possible.
5. *However*, no matter how difficult a system has been adopted, the possession of a series of cryptograms of the same length, even two of them, or almost of the same length, makes the decrypting easy and almost mechanical.

For substitution ciphers:

6. The shorter the cryptogram, the harder it is to decrypt it. In simple systems, the decrypting of a single cryptogram, even a relatively short one, is possible.
7. The possession of several cryptograms in the same system and the same key, even if short ones, facilitates the decrypting and in simple types makes it mechanical.
8. The knowledge of one or more words of the clear text either at the beginning (stereotype introductory phrases) or in the body (probable words) or at the end (signatures) will help the solution greatly.

Sometimes a simple word, correctly guessed, completely unfolds the secret text.

39. There are various types of statistical tables that must be prepared before beginning the work of decrypting. The most important is the tabulation of the elements of the cryptogram and the computation of their frequencies.

40. A simple tabulation of the elements is obtained by stroking at the side of a normal alphabet the appearance of each letter of the message. Thus the cryptogram of 69 letters:

P L T W S T E C G T D P K Z P L T X D C P T G E P
J P T E K Z J I T S C B J C E P L T B L C T Z I J
O C E P S J P T K Z P L T D J P C K D

which is a simple substitution meaning "*The President of the United States of America is the Chief Magistrate of the Nation*," will be tabulated as follows:

Elements	Appearances	Total	Frequency %
A		0	
B	II	2	2.8
C	IIIII II	7	10.
D	IIII	4	5.8
E	IIIII	5	7.2
F		0	
G	II	2	2.8
H		0	
I	II	2	2.8
J	IIIII I	6	8.7
K	IIII	4	5.8
L	IIIII	5	7.2
M		0	
N		0	
O	I	1	1.4
P	IIIII IIIII I	11	15.9
Q		0	
R		0	
S	III	3	4.3
T	IIIII IIIII I	11	15.9
U		0	
V		0	
W	I	1	1.4
X	I	1	1.4
Y		0	
Z	IIII	4	5.8
Totals.....		69	99.2

41. Sometimes a suffix table is prepared instead of the above. It is obtained by setting down against each element of the alphabet the letter that follows the one we are considering. For instance, in our example the first letter is P: on line P write down L, the element after P; the second letter is L: on line L write down T which follows L, etc. The presence of the last letter of the message, having no suffix, is shown by a dash.
Thus:

Elements	Suffixes	Total	Frequency %	Number of Different Suffixes
A		0	—	—
B	JL	2	2.6	2
C	GPBETEK	7	10.	6
D	PCJ—	4	5.8	3
E	CPKPP	5	7.2	3
F		0	—	—
G	TE	2	2.8	2
H		0	—	—
I	TJ	2	2.8	2
J	PICOPP	6	8.7	4
K	ZZZD	4	5.8	2
L	TTTCT	5	7.2	2
M		0	—	—
N		0	—	—
O	C	1	1.4	—
P	LKLTJTLSTLC	11	15.9	6
Q		0	—	—
R		0	—	—
S	TCJ	3	4.3	3
T	WEDXGESBZKD	11	15.9	9
U		0	—	—
V		0	—	—
W	S	1	1.4	—
X	D	1	1.4	—
Y		0	—	—
Z	PJIP	4	5.8	3
Totals.....		69	99.2	

From a table of this kind, an exercised adept will draw a great deal of useful information. For instance, he will not hesitate to select the proper value for clear-E, between T and P, both appearing 11 times; he will immediately make clear-E = crypto-T because T combines with 9 different elements against 6 of P. The persistence of the suffixes of K and L will tell him that either of them stands for clear-H. He will select L without a second thought because with T, already individual-

ized, it forms LT = clear-HE, a very common English bigram. This brings him back to consider P = clear-T, because in line P, he sees 4 L, yielding PLT = clear-THE, and so on. These three values alone, when interlined with the cryptogram, will lead to its solution.

42. A more informative tabulation of the elements of a cryptogram is obtained from a *Trigraphic Frequency Table*, one of which is illustrated on pages 32–33. The upper element of each pair of affixes is the prefix and the lower one is the suffix of the crypto-element on the outside column. The absence of a prefix to the first element and of a suffix to the last element are indicated by dashes. (See L and Q).

Appendix II

THE PROBLEM IN THE ORIGINAL FRENCH VERSION

CRYPTOGRAPHIE MILITAIRE

—

COMMANDANT BAZERIES

PROPOSITION d'un système cryptographique militaire, n'exigeant qu'un crayon et du papier, facile à retenir de mémoire.

(Copie)

En 1891, j'ai présenté à la Guerre un appareil cryptographique de mon invention, donnant un chiffre facile à établir, facile à traduire, n'exigeant aucun secret de l'appareil, ni aucune étude préalable.

Tous les officiers supérieurs et généraux qui ont eu entre les mains mon cryptographe ont été surpris de sa facilité d'emploi et m'en ont fait des éloges.

Ce cryptographe n'a pas été adopté.

∴

Il résulte de plusieurs conversations que j'ai eues avec des officiers généraux au sujet de la cryptographie et de la cryptographie militaire en particulier, que l'idée bien arrêtée de l'État-Major général est de trouver un système n'exigeant qu'un crayon et du papier, et pouvant se retenir facilement de mémoire sans le secours d'aucune note écrite.

J'ai fait des recherches et des essais dans cet ordre d'idées. Je n'ose me flatter d'avoir trouvé

un système indéchiffrable. Cependant, si les trois cryptogrammes que je donne plus loin résistent aux essais des déchiffreurs auxquels ils seront soumis, j'aurai peut-être trouvé la solution du problème, cherchée en vain jusqu'ici.

∴

Tout système cryptographique trahit sa méthode par l'analyse et la décomposition du cryptogramme. Une fois la méthode trouvée, le reste du déchiffrement n'est qu'un jeu pour un spécialiste un peu habile.

Le système auquel je me suis arrêté a l'avantage de laisser le doute sur la méthode employée ; je dirai plus, il trompe le déchiffreur. Les recherches, portant à faux, ne peuvent aboutir.

Les combinaisons compliquées ne valent rien. Je me suis attaché, comme toujours, à la plus grande simplicité possible. J'ai employé quelques ruses cryptographiques pour déguiser le système. Ces ruses triompheront-elles des déchiffreurs? Je le pense. Il me semble que, personnellement, j'y aurais été trompé et, par conséquent, dépisté et impuissant.

Reste à savoir si de plus habiles s'y tromperont aussi. Si oui, le système est bon.

Je ne puis, pour le moment, indiquer la méthode

employée; elle est tellement simple que le secret de cette méthode me paraît s'imposer absolument. Cependant je n'ai pas dit mon dernier mot; car, en modifiant un peu cette méthode, tout en lui conservant sa conception originale, on pourrait peut-être arriver à ne pas craindre sa divulgation.

∴

J'ai toujours considéré comme un danger réel de baser la sécurité d'un système cryptographique sur le secret de la méthode employée. Trop de négligences peuvent être commises pour que ce secret, objet des convoitises de l'ennemi et forcément en la possession d'un très grand nombre de personnes, reste longtemps *secret*. A mon avis, la sécurité doit résider dans l'excellence du système et dans le seul secret de la clef.

Tout ce que je puis dire, pour l'instant, c'est que, comme rapidité du chiffrement et du déchiffrement, le système ne laisse rien à désirer. Il est aussi rapide, sinon plus, que les systèmes connus ou employés. En plus, chaque cryptogramme est fait avec une clef différente, clef choisie à volonté par le chiffreur sans qu'il soit tenu de l'indiquer au préalable au destinataire. En un mot, le cryptogramme indique et porte sa clef.

*
* *

On remarquera que je ne suis pas aussi affirmatif pour l'indéchiffrabilité que je l'ai été lorsque j'ai présenté mon cryptographe cylindrique, n'étant pas aussi sûr de ce système que je l'étais et le suis toujours de mon cryptographe.

Je donnerai la méthode dès qu'elle me sera demandée.

Cryptogrammes chiffrés d'après la méthode Bazeries et n'exigeant pour leur traduction qu'un crayon et du papier.

N° 1. — 85 Groupes

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

N° 2. — 40 Groupes

D E G S C	L M L H Y	O S K S A	U Q O L Q
U A O S H	H Y S A E	M Q S H S	H Q O N D
S B Q C X	O L L U U	S L D S K	C C Q C S
B S N K S	X C T I O	N D D S K	Q T N A O
S C G X D	M N G Q D	L X L Y R	O M C H Q
Q D S S C	T M X O S	H Y T Q Y	S L C S K
O G X M S	H T B J N	E O L Q Q	S O A O J
N H R S Q	R S M S H	Q K Y C O	M R O S A
Y H X S K	O R Q C L	M S N O M	Q S C H X
R H S Y A	O S K B L	B A O S H	N D Q T T./.

N° 3. — 48 Groupes

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

Signé : Com[t] Bazeries.

Le 14 septembre 1898, on nous avisait que notre mémoire était soumis à l'examen de la Commission de cryptographie militaire.

Quelque temps après, nous avons été invité par M. le général Niox à faire connaître notre méthode, tenue secrète jusqu'alors.

Voici copie de cette méthode.

CRYPTOGRAPHIE MILITAIRE

COMMANDANT BAZERIES

(Copie)

MÉTHODE n'exigeant qu'un crayon et du papier

POUR CHIFFRER. — Écrire le texte clair de préférence sur du papier quadrillé, une lettre dans chaque case en écriture courante et en laissant une ligne en blanc entre chaque ligne du texte clair. Cette ligne en blanc est destinée à recevoir le chiffrement.

Soit à chiffrer : Envoyez un bataillon d'infanterie au Creuzot, ce soir, par voie ferrée.

Exemple .

c n v o y e z u n b a t a i l l o n d i n f a n t e r i e
a u c r e u z o t c e s o i r p a r v o i e f e r r é e

∴

CLEF. — Choisir une clef de substitution. Cette clef consiste en deux lettres quelconques. En attribuant à chacune d'elles leur numéro d'ordre dans l'alphabet normal, on transforme ces deux lettres en un nombre entier.

Exemple :

A B = 1 2
D Z = 4 2 5
B A = 2 1
Z F = 2 5 6
etc. etc.

Une fois la clef choisie, ZF, par exemple; soit : « *Deux cent cinquante-six* », établir un alphabet conventionnel où toutes les lettres existant dans la clef sont en tête, soit : DEUXCNTIQAS et celles non existant dans la clef prennent place à leur suite dans leur ordre d'alphabet, soit : BFGHTKLMOPRVYZ.

Écrire horizontalement cet alphabet conventionnel, du commencement à la fin, dans les cases d'un carré de 5.

Exemple :

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

Écrire à côté dans un carré semblable, mais verticalement, l'alphabet normal du commencement à la fin.

Exemple :

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

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

Nota. — Ne pas se préoccuper des lettres qui se trouveraient être les mêmes dans les cases correspondantes des deux carrés de cinq. C'est un effet du hasard.

* * *

CHIFFREMENT PAR SUBSTITUTION. — Une fois la clef établie, substituer à chaque lettre du texte clair, sur la ligne laissée en blanc, la lettre donnée par la clef de substitution et écrire cette lettre en majuscule.

Nota. — Pour ne pas perdre de temps, transformer en suivant, toutes les mêmes lettres, avant de passer à la lettre suivante. En opérant ainsi, l'opération du chiffrement est vite faite.

Exemple :

e n v o y e z u n b a t a i l l o n d i n f a n t e r i e
P L A V O P Z C L N D Y D K I I V L J K L E D L Y P G K P

a u c r e u z o t c e s o i r p a r v o i e f e r r é e
D C S G P C Z V Y S P M V K G X D G A V K P E P G G P P

Une fois la substitution opérée, partager le chiffrement en tranches de trois lettres par une ligne noire, rouge ou au crayon.

Exemple :

e n v	o y e	z u n	b a t	a i l	l o n	d i n	f a n	t e r	i e
P L A	V O P	Z C L	N D Y	D K I	I V L	J K L	E D L	Y P G	K P

a	u c r	e u z	o t c	e s o	i r p	a r v	o i e	f e r	r e e
D	C S G	P C Z	V Y S	P M V	K G X	D G A	V K P	E P G	G P P

∴

CRYPTOGRAMME PAR TRANSPOSITION. — Former le cryptogramme en renversant les tranches de trois lettres.

∴

CONVENTIONS. — Il est convenu que les deux premières lettres du cryptogramme indiquent la clef de substitution et que, chaque fois que la première lettre d'un groupe de trois est une voyelle : A.E.I.O.U.Y., cette voyelle est nulle. On fait ainsi des nulles quand on le veut, et autant qu'on le veut. Forcément une nulle doit être employée lorsque la première lettre de la tranche renversée est une voyelle. Lorsque cette première lettre est une consonne, la nulle est facultative.

∴

OBSERVATIONS. — On s'arrange pour terminer le cryptogramme en un dernier groupe de 5 lettres, sans fractions, clef comprise, ce qui est facile par la liberté que l'on a de faire des nulles à volonté.

Il est bon d'indiquer le nombre de groupes de 5 lettres en tête de la dépêche, de manière que, si le télégraphe en omet un, on puisse essayer de déchiffrer quand même, sans être obligé de redemander la transmission de la dépêche.

∴

Exemple de cryptogramme pour la dépêche chiffrée plus haut :

Général Commandant 8e Corps à
Général Commandant d'Armes à Dijon.

13 groupes. Z F I A L P P O V L C Z A Y D N E I K D
L V I A L K J L D E G P Y D P K G S C A Z C P S Y
V V M P X G K A A G D P K V G P E P P G

∴

Pour déchiffrer. -- Commencer par éliminer les lettres nulles en faisant les tranches de trois lettres.

Exemple :

13 groupes. (Z) (F) (I) A L P | P O V | L C Z | (A) Y D N | (E) I K D
L V I | (A) L K J | L D E | G P Y | D P K | G S C | (A) Z C P | S Y
V | V M P | X G K | (A) A G D | P K V | G P E | P P G

Cette opération faite, copier en interligne en retournant les tranches.

Exemple :

P L A V O P Z C L N D Y D K I I V L J K L E D L
Y P G K P D C S G P C Z V Y S P M V K G X D G A
V K P E P G G P P.

Il ne reste plus qu'à substituer à chaque lettre du cryptogramme la lettre vraie, d'après la clef indi-

quée et que l'on a eu, au préalable, le soin d'établir, et on lit : Envoyez un bataillon, etc... etc...

Comme on le voit, c'est assez vite fait.

∴

Les cryptogrammes soumis au déchiffrement, dans mon étude cryptographique du 28 août dernier, sont établis comme il vient d'être exposé dans cette méthode.

Il deviendra aisé de les traduire.

C'est la méthode dans sa plus grande simplicité.

∴

Comme je l'ai dit dans mon étude précitée et comme on peut maintenant s'en rendre compte, le secret de cette méthode s'impose absolument. Il est déjà imprudent de l'avoir écrite. C'est de vive voix qu'elle aurait dû être communiquée.

Cependant, avec une petite modification, j'espère arriver à ne pas craindre la divulgation du procédé.

Cette modification, je la ferai connaître de vive voix. Avant, il serait utile que des déchiffreurs, connaissant ma méthode, essayent de faire la traduction du nouveau cryptogramme ci-après.

S'il résiste au déchiffrement, c'est que le système est réellement indéchiffrable pour quiconque n'en possède pas la clef.

CRYPTOGRAMME

Fait divers pris, dans un journal, aux nouvelles judiciaires

43 groupes. L M P C X B R L S Q H F M H H C B H K X
C M S H Q B C U P M C C V F S A K F L N V G S R X
F C V B R S N X F T K K R R N D D Q G H Q X N L M
H F S V K R F S N I C R V K B A K V G N V C S G C
N R S M M C H P B K H F Q U C F U N X R V I G V T
K H K R O D N R N B M R K F G G N C M C K S V H N
G S G C U R K G N V K D D Q V R K O N B N L G Q T
S N K I C V U K B V I G F G C Z F H U C H S A M N
U C X F F V F C R H K B F V C X N H G Q.

Ce cryptogramme, comme ceux précédemment établis, porte sa clef.

Signé :

Com[t] BAZERIES.

Le lecteur connait la réponse; elle est du 19 avril 1899, et elle figure au chapitre III de la troisième partie.

Reproduisons-la, quand même :

« Il a été reconnu que la méthode ne présentait « pas les garanties de sécurité suffisantes pour être « adoptée. »

∴

Comment concilier cette réponse, bien affirmative, avec le non-déchiffrement du cryptogramme de 43 groupes qui termine l'exposé de notre méthode ?

Mystère !

Appendix III

THE TRANSLATION OF THE THREE CRYPTOGRAMS CONTAINED IN THE PROBLEM

CRYPTOGRAM NO. 1—85 GROUPS

DATA:

a) Numerical values of alphabetic elements according to their rank:

A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	X	Y	Z
1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25

b) Initial Bigram: E J or 5 1 0, viz.: C I N Q (C) E (N) T D (I) X

c)

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

Crypto-alphabet — Clear-alphabet

CRYPTOGRAM:

(E) (J) A D S X S O S X C J A D E C E Y P E L C M X F S
G E L E N E L A R G U A T S U D A I L C E

L E G É N É R A L A U G U S T I A D É C L-

S J C S E A H C X E C J M S L X S B B I B C R I
E R A E U Q M A L A R I E D L E V V V A Y

A R É Q U E L' A M I R A L D E V V E Y A V-

```
Y M C  H S L  L O C  C X S  Q C F  I  E Y M  O  Y C X  O
T I A  M E D  D N A  A L E  P A C     U T I     T A L
A I T  D E M  A N D  É L A  C A P     I T U     L A T-
```

```
O V M  H S L  M O C  U  S X X  U  O C L  S X P  X S L  L M C  S O E
N O I  M E D  I N A     E L L     N A D  E L S  L E D  D I A  E N U
I O N  D E M  A N I     L L E     D A N  S L E  D É L  A I D' U N E
```

```
U  E S G  X S J  S P S  C Q P  V O D  C P X  Y  O C R  S J Y  P E I
   U E H  L E R  E S E  A P S  O N G  A S L     N A Y  E R T  S U F
   H E U  R E L  E S E  S P A  G N O  L S A     Y A N  T R E  F U S-
```

```
S L S  J S P  L O S  X S J  M H C  X C J  S H C  F M J  Y  O M C
E D E  R E S  D N E  L E R  I M A  L A R  E M A  C I R     N I A
É D E  S E R  E N D  R E L' A M I  R A L  A M É  R I C     A I N
```

```
J V C  A  O V L  L S O  V T S  C T H  S L J  C X J  X M B  X S X
R O A     N O D  D E N  O B E  A B M  E D R  A L R  L I V  L E L
A O R     D O N  N É D  E B O  M B A  R D E  R L A  V I L  L E. L-
```

```
S P S  C Q P  V O D  V P X  C Y O  J V X  J C P  J V T  S X S
E S E  A P S  O N G  O S L  A T N  R O L  R A S  R O B  E L E
E S E  S P A  G N O  L S O  N T A  L O R  S A R  B O R  É L E
```

```
C J L  C S Q  U  X T E  F O C  D S X  S O S  A  X C J
A R D  A E P     L B U  C N A  G E L  E N E     L A R
D R A  P E A     U B L  A N C.  L E G  É N É     R A L
```

```
      (1)
D E C  Y P E  B C M  A  Y M C  A  E C P  M S Y  S H H  C M L
G U A  T S U  V A I     T I A     U A S  I E T  E M M  A I D
A U G  U S T  I A V     A I T     S A U  T É I  M M É  D I A-
```

```
          (2)
H S Y  E  Y O S  I  O C L  I  E O P  G F S  V X C  S Q E  X X C
M E T     T N E     N A D     U N S  H C E  O L A  E P U  L L A
T E M     E N T     D A N     S U N  E C H  A L O  U P E  A L L-
```

APPENDIX III

C H S S L O M E A Y Y C X O O S Y M C L U Y S Y A Y S (3) O
A M E E D N I U Q T A L N E T I A D T E T T E N
E M A N D E Q U I L' A T T E N D A I T E T N, É T (S)

A Y M C A O S J C E L (4) H V T A E L L M C N J S P C O M
T I A N E R A U D M O B U D D I A K R E S A N I
A I T R E N D U À B O M D D U K A I S E R I N A- (R)

O E D E C Y P E O S X M B C L S J O E D S J J S X C S
U G U A T S N E L I V A D E R U G E R R E L A E
U G U S T A. L E N A V I R E D E G U E R R E A L-

H S X L O C A Y P S J C Q L M Y C H S X M O C S X A
M E L D N A T S E R A P D I T A M E L I N A E L
L E M A N D E S T P A R T I D E M A N I L L E A-

(5)
O C B C X Y A O M I T E L T H V L H C A S H S A Y O
N A V A L T N I F B U D B M O D M A E M E T N
V A N T L A F I N D U B O M B A M D E M E N T
(R)

1. Bazeries forgot to follow his rule and insert a null-vowel in front of Y.
2. This group, EOP, should have been OEP, equivalent to NUS, which transposed becomes SUN, the correct letters required to make sense.
3. This letter should be P. Its clear-equivalent is S, which is required for a correct reading instead of N.
4. and 5. This letter should be J. Its clear-equivalent is R, which is required for a correct reading instead of H.

CRYPTOGRAM NO. 2—40 GROUPS

DATA:

a) Numerical values of alphabetic elements according to their rank.

A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	X	Y	Z
1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25

b) Initial Bigram: D E or 4 5, viz.: Q U A R (A) N T E C I (N) (Q)

c)

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

CRYPTOGRAM:

(D) (E)

G S C L M L H Y O S K S A U Q O L Q U A O S H
M E L I N I R T S E D E F A S I A F S E R

L E M I N I S T R E D E S A F F A I R E S

H Y S A E M Q S H S H Q O N D S B Q C X O L
R T E G N A E R E R A S U C E V A L O S I

É T R A N G É R E S A R E Ç U L' A V I S O-

L U U S L D S K C C Q C S B S N K S X C T I
I F F E I C E D L L A L E V E U D E O L B

F F I C I E L D E L A L E V É E D U B L O-

O N D D S K Q T N A O S C G X D M N G Q D L X L Y
S U C C E D A B U S E L M O C N U M A C I O I T

C U S D E C U B A. L E S C O M M U N I C A T I O-

APPENDIX III

R O M C H Q Q D S S C T M X O S H Y T Q Y S L C
P S N L R A A C E E L B N O S E R T B A T E I L

N S P A R L E C Â B L E S O N T R É T A B L I E-

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

S. D E N O M B R E U X V A I S S E A U X S E P R-

Q R S M S H Q K Y C O M R O S A Y H X S K O R Q C
A P E N E R A D T L S N P S E T R O E D S P A L

É P A R E N T D A N S L E S P O R T S D E L A P-

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

É N I N S U L E A P O R T E R D E S V I V R E S

N D Q (1) T T
U C A

A C U B B
(A)

1. This letter should be Q. Its clear-equivalent is A, required for a correct reading instead of T.

CRYPTOGRAM NO. 3—48 GROUPS

DATA:

a) Numerical values of alphabetic elements according to their rank:

A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	X	Y	Z
1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	21	23	24	25

b) Initial Bigram: I A or 9 1 viz.: Q U A T R E V I N G (T) O (N) Z (E)

c)

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

CRYPTOGRAM:

(I) (A)

VM I M JM A IQC CMB XHC LQX XJQ
GE L E NE LAR REM TIR YAT TNA

LE G ÉNÉ RAL MER RIT TAY ANT

BMF FJQ HKM JQB A IIH MFM QCG MXH
MED DNA ISE NAM LLI EDE ARV ETI

DEM AND É S I MAN ILL E DE VRA IT É-

MCX I OOS MTR SOM SPJ XJH MBM TXJ A
ERT CCO EPU OCE OJN TNI EME PTN

TRE OCC UPÉ E CO NJO INT EME NT P-

ICQ QKM CMB QOH KJH A IXM HKM RKJ
LRA ASE REM ACI SNI LTE ISE USN

AR L E S A MÉR ICA INS ET L E S I NSU-

APPENDIX III

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

R G É S L E P R É S I D E N T M A C K I N L E Y

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

A R É P O N D U Q U E L A V I L L E, L A B A I E

O I X M (1) J T M F X C Q G M J M H X M X S M C R O O
L T E N P E D T R A V E N E I T E T O E R U C C

E T L E P N R T D E V A I E N T Ê T R E O C C U-
(O)

K M T C Q T K M I C S U K M O K M F Q X M R K X
S E P R A P S E L R O F S E C S E D A T E U S T

P É S P A R L E S F O R C E S D E S É T A T S U-

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

N I S M A I S Q U' I L N' Y A U R A I T P A S D' O-

R O O X Q T A J S H A D H B M X
U C C T A P N O I X I M E T

C C U P A T I O N M I X T E

1. This letter should be S. Its clear-equivalent is O, which is required for the correct reading instead of J.