

MILITARY CRYPTOGRAPHY

La cryptographie militaire

Auguste Kerckhoffs, January 1883

Journal des sciences militaires, January 1883, Volume IX, pp. 5-38. Translation of the first instalment of this article. A period-conscious English working translation of the scanned original, with some diagrams reproduced from the original pages. Where an example depends upon French plaintext, the French has been retained and an English gloss is given in brackets. I have kept nineteenth-century military terms such as cipher, key, despatch, cryptogram, and decipherer, plus some archaic English terms like interverted, to keep the feel of the piece. The font is Baskerville Old Face, the closest match I could find to the original although slightly out of fashion by 1883.

Sophie Baskerville, June 2026

“Cryptography is a powerful auxiliary of military tactics.”

(Général Lewal, Études de guerre.)

I. Cryptography in the Army

A. Historical notions

Cryptography, or the art of ciphering, is a science as old as the world. Confounded in its origin with military telegraphy, it was cultivated from remotest antiquity by the Chinese, Persians, and Carthaginians; it was taught in the tactical schools of Greece, and held in high esteem by the most illustrious Roman generals.¹

From the modest scytale of the Lacedaemonians and the devices invented or reported by Aeneas the Tactician, down to the famous drum of Kessler, men of war have imagined many contrivances for transmitting secret orders afar, or for shielding their instructions from the investigations and surprises of the enemy.²

We possess, nevertheless, only very incomplete information concerning the cryptographic procedures, properly so called, used among the ancients. Apart from the Commentaries of Aeneas, one meets on the subject here before us only isolated passages in Polybius, Plutarch, Dion Cassius, Suetonius, Aulus Gellius, Isidore, and Julius Africanus.³

During the Middle Ages, cryptography was scarcely cultivated except by monks and cabalists; and even where it served some practical end, its inventors sought rather to throw the reader off the scent as to the meaning of the communications transmitted than to imagine methods of correspondence more or less indecipherable. In those shadowed times of ignorance it was almost as dangerous to correspond in a mysterious or indecipherable language as to write the most compromising secrets in clear.

Even in the seventeenth century the mere fact of having corresponded in secret characters was still considered by English courts as an aggravating circumstance. Thus, in the famous trial of the Earl of Somerset for poisoning, Chancellor Bacon noted, as a grave charge against the noble accused, his habit of writing to his friends in cipher.

It was therefore steganography that our fathers practised, artificium sine secreti latentis suspicione scribendi, rather than cryptography in the sense now attached to that word. In the works of the Jesuit Schott and in an old treatise on cryptography by the Duke of Brunswick may be read the thousand artifices successively invented for that purpose.⁴ Only from the Renaissance onward did cryptography become a true art, ars occulte scribendi, as it was then called, and acquire a certain importance in the correspondence of princes with their ambassadors, and in the relations of great lords with their adherents.

The letters addressed by Henry IV to the Landgrave of Hesse, published some years ago by de Rommel, show that the king liked to use a cipher for his intimate correspondence. It is likewise known that Henry IV, having caused certain ciphered letters sent by members of the League to the Spanish government to be intercepted, charged the mathematician Viète with discovering the key. Viète succeeded, and the king was thus able, for nearly two years, to watch the intrigues of his enemies.

Under Richelieu, the art of deciphering secret writings rose almost to the height of a state science; according to Marshal de Camp Beausobre, the minister for foreign affairs even maintained an academy in which it was taught.⁵ Supported by the largesse of governments, and encouraged by the lack of political probity that marks the following reigns, the art of deciphering continued, until the July Revolution, to be cultivated with equal success by spies of the court and by the men of the black chamber.

I have not, however, been able to find very clear traces of the employment of cryptographic correspondence in the army during the sixteenth century. But it is known positively that, from the seventeenth century onward, orders were transmitted to generals commanding on the frontiers or in enemy country only by cipher.⁶

In the narratives of the wars of the First Empire, cryptographic communications are often mentioned. Generals had two keys for corresponding with one another and with general headquarters: the great cipher and the small, or ordinary, cipher. Baron Fain, secretary to Napoleon I, reports that during the Russian campaign the Emperor maintained ciphered correspondence.⁷ It is also known that, during the Peninsular War, a Spaniard found means to steal Suchet's cipher and used it to facilitate for his countrymen the recapture of Mequinenza and Lerida.

Today, correspondence by secret ciphers is adopted in all the armies of Europe; but it is still applied in systematic fashion only in the bureaus of the chancelleries.

B. State of the question

The Germans lay down as a principle that cryptographic correspondence should be employed in the most extensive manner. The programmes of their military schools prescribe not only that officers be exercised in the composition and reading of secret despatches, but also that they be initiated into all the theoretical principles of the art of deciphering.

Article 32 of the regulation of 19 January 1874 likewise provides that military despatches should, so far as possible, be ciphered.

One might therefore be astonished at first sight that, with rare exceptions, the use of ciphered correspondence should still be limited today in the French army to commanders-in-chief. But a system of cryptography "easy and safe in use" is, says General Lewal, "a desideratum that has always existed in our army".⁸ The former commandant of the Ecole supérieure de guerre adds, it is true, that procedures for this purpose do exist, and that it would suffice to adopt one "that was at once portable and of a use within the reach of all". Yet certain disappointments suffered by the staff in our recent Tunisian campaign, as well as the methods taught and recommended in our higher military schools, might lead one to suppose that there is a singular analogy between this easy and safe system and the philosopher's stone of the old alchemists.

Our best generals are well of the opinion today that the several commanders of an army must have at their disposal a system of secret communications by which to correspond freely, not only among themselves and with their commander-in-chief, but also with their lieutenants. Thus the tactician whom I have just cited thinks that in peace as in war generals, heads of regiments or services, and all commanders of columns and posts should be provided with a cipher. He adds, and rightly, that during peace our officers should be trained in the handling of this correspondence.

"This is a matter to be foreseen and settled before the war," he says; "once operations have begun, it is too late to think of it. Besides, even in peace one needs, at every instant, to correspond secretly."

In General Bardin's historical researches on the military art, one reads that the use of ciphers had died out amid the conflagration of 1814, and that, when Napoleon wished to rally round the nucleus of the army all his foreign garrisons and several large French garrisons, Feltre and Berthier sent their orders in plain French. Few despatches therefore reached their destinations, and the enemy seized most of them. "Perhaps," says Bardin, "the fate of France and the face of Europe depended upon the desuetude of cryptography."⁹

But it is not enough to have a cipher for secret correspondence; it must also present serious guarantees of indecipherability. This is the weak side of most systems hitherto imagined, and where this capital defect has been avoided one finds practical inconveniences just as grave.

Even at the Ministry of War, choice or combination of cipher has not hitherto been very happy. It is no secret that during the Russo-Turkish War there was received, one Sunday, from one of the military attaches following the operations of the armies in conflict, a ciphered despatch which, owing to the absence of the head of the bureau charged with cryptographic correspondence, could not be deciphered. The Minister, ignorant of the key, believed he could do no better than ask an officer of the staff to try deciphering it without a key. After a few hours the cryptogram was translated. Happily for the secrecy of the correspondence, the skilful decipherer was the Minister's own son.¹⁰

The obituary articles published in the German newspapers in 1879, on the death of Captain Max Hering, chief of the telegraph service who discovered the cable of the Seine in 1870, showed what services were rendered to the besiegers by the absence of a safe system of secret correspondence between the army of Paris and the generals of the provinces.

I do not know what one should think of the assertions of journalists across the Rhine; but when I see authorised judges declare that cryptography is a "powerful auxiliary of military tactics", and when I reflect that the destinies of a country, the fate of a city or of an army, may at times depend upon the greater or lesser indecipherability of a cryptogram, I am stupefied to see our savants and professors teaching and recommending for war systems whose key a decipherer of but little experience would certainly find in less than an hour.

This excess of confidence in certain ciphers is hardly explicable except by the abandonment into which cryptographic studies have fallen since the suppression of the black chambers and the security of postal relations. It is also permissible to think that the unmeasured assertions of certain authors, no less than the complete absence of serious work on the art of deciphering secret writings, have largely contributed to circulating the most erroneous ideas upon the value of our systems of cryptography.

Thus General Lewal affirms categorically in his *Etudes de guerre* that ciphers with a variable basis are illegible, or at least that they can be deciphered only with unheard-of difficulties. And did not Voltaire himself say, in an article on ciphered writings, and at the very time when the art of deciphering was in full flower, that “those who boast of deciphering a letter without being acquainted with the affairs treated in it, and without preliminary aids, are greater charlatans than those who should boast of understanding a language they have never learned”?¹¹

In the preface to the *Contre-espion*, in which “citizen” Dlandol made known, in 1793, the keys of certain ciphers used by the royalists in their correspondence with the emigres, it is said that “it was not one of the least services to render the fatherland, in the circumstances of the time, to annihilate by publicity the most dangerous weapon of the secret enemies of the Republic”. I believe in my turn that I am not acting as a bad citizen by bringing into full daylight a state of things which, though belonging to a different order of ideas, is identical at bottom, and from which our enemies abroad might one day derive only too great and too easy an advantage.

In the pages that follow I shall first examine the desiderata of every system of military cryptography; then I shall say a few words on the different ciphers; next I shall indicate a new process of decipherment applicable to the most-used systems of cryptography with variable basis; and I shall end with some considerations upon cipher dictionaries and cryptographs.¹²

II. Desiderata of Military Cryptography

A clear distinction must be drawn between a system of ciphered writing devised for a momentary exchange of letters among a few isolated persons, and a method of cryptography intended to regulate, for an unlimited time, the correspondence of the several chiefs of an army among themselves. The latter cannot, at their pleasure and at a given moment, modify their conventions. Moreover, they must never carry upon them any object or writing of such a nature as to enlighten the enemy upon the sense of secret despatches that may fall into his hands.

A great number of ingenious combinations can answer the purpose in the first case. In the second, a system is needed that fulfils certain exceptional conditions, which I summarise under the six following heads:

1. The system must be materially, if not mathematically, indecipherable.
2. It must not require secrecy, and it must be able without inconvenience to fall into the hands of the enemy.
3. The key must be capable of communication and retention without the aid of written notes, and must be capable of being changed or modified at the will of the correspondents.
4. It must be applicable to telegraphic correspondence.
5. It must be portable, and its handling or operation must not require the assistance of several persons.
6. Finally, in view of the circumstances governing its application, the system must be easy to use, requiring neither strain of mind nor the knowledge of a long series of rules to be observed.

Everyone agrees in admitting the reason for the last three desiderata; there is less agreement when the first three are in question.

Thus authorised persons maintain that absolute indecipherability of the cipher could not be regarded as a *sine qua non* condition of its admission into army service; that ciphered instructions transmitted in time of war have only a momentary importance and scarcely require secrecy beyond the three or four hours following the moment at which they are given; that it matters little, therefore, whether the sense of a secret despatch be known to the enemy some hours after its interception; that, in short, it suffices for the system to be so contrived that the translation of a cryptogram requires at least three or four hours of work. It is added that the possibility of changing the key at will removes from the defect of non-indecipherability all its importance.

This argument may at first sight appear fairly just; at bottom I believe it false.

It forgets, in my opinion, that the secrecy of communications sent to a distance very often preserves its importance beyond the day on which they are transmitted. Without enumerating all possible cases, it will suffice to cite that in which the commander of a besieged town sends information to the army that is to relieve him. Moreover, once an intercepted cryptogram has been deciphered, every new despatch written with the same key and meeting the same fate can be read instantly. It will consequently happen that, for a longer or shorter time, despatches will be sent in all directions whose decipherment will, as it were, have been performed in advance, unless one supposes that in an army corps all ciphered

instructions emanate from a single person, or at least pass through the hands of a single person, which would reduce secret correspondence to a singularly modest role.

The power to change the key at will is certainly an essential condition of every cryptographic system, but it is a deceptive advantage, and one would be wrong to count upon its practical realisation through the thousand vicissitudes of a long campaign.

As to the necessity of secrecy, which in my eyes constitutes the principal defect of all our cryptographic systems, I observe that it in some sort restricts the employment of ciphered correspondence to commanders-in-chief alone. By secrecy I mean here, not the key properly so called, but that which forms the material part of the system: tables, dictionaries, or mechanical apparatus of whatever kind that permit its application. Indeed, one need not create imaginary spectres, nor suspect the incorruptibility of subordinate employees or agents, to understand that if a system requiring secrecy were in the hands of too great a number of individuals it might be compromised at every engagement in which one or another of them took part. From this point of view alone there would be reason to condemn the use of the cipher dictionary now employed in the army.

It may perhaps be objected that, while admitting the second desideratum, it is scarcely possible to establish a completely indecipherable system. We must understand one another. I know very well that under these conditions the search for a mathematically indecipherable system is mathematically impossible; but I affirm, and not without good reasons, that while satisfying the different desiderata enumerated above, one may perfectly combine systems which, if not mathematically, are at least materially indecipherable.

It appears that serious consideration is being given at the Ministry of War to replacing the cipher dictionary by some other, more practical, system. Well then: if the Administration wishes to profit from all the services that a well-combined system of cryptographic correspondence can render, it must absolutely renounce secret methods, and lay it down as a principle that it will accept only a process capable of being taught in full daylight in our military schools, which our pupils shall be free to communicate to whomever they please, and which our neighbours may even copy and adopt, if that suits them. I will say more: only when our officers have studied the principles of cryptography and learned the art of deciphering will they be in a position to avoid the numerous blunders that compromise the key of the best ciphers, and to which all laymen are necessarily exposed. Only then will the article of the regulation of 19 November 1874, mentioned above, receive a practical and truly satisfactory application.

III. The Different Methods of Cryptography

The different systems of secret writing may be referred to three principal methods:

1. The method limited to a simple transposition of the letters of the clear text.
2. The method that bases the combination of the cipher upon an interversion of the alphabetical order of the letters.
3. The method that represents syllables, words, or even whole sentences by numbers or groups of letters.

A. Method by transposition

Systems resting upon a transposition of letters are very ancient. They permit numerous variations and have served as the basis of certain mechanical apparatus, such as grilles, which still enjoy the favour of the public.¹³

Here is an example of elementary transposition. The letters of the despatch are first written in their natural order upon a certain number of lines of a determined number of characters; they are then copied in an agreed order. The number representing this second disposition constitutes the key of the cipher.¹⁴

Une attaque simulee aura lieu demain matin a quatre heures.

[A sham attack will take place tomorrow morning at four o'clock.]

Cryptogram: nsuqtteeuatamlrueuaiaeleaneiumiamdihrtqnetaufdcreebae

Une attaque simulée aura lieu demain matin à quatre heures.

A	1	2	3	4	5	6	7	8	9	10	11
1	u	n	e	a	t	t	a	q	u	e	s
2	i	m	u	l	e	e	a	u	r	a	l
3	i	e	u	d	e	m	a	i	n	m	a
4	t	i	n	a	q	u	a	t	r	e	h
5	e	u	r	e	s	a	b	e	d	e	f
B	2	11	9	8	5	3	10	1	7	6	4
1	n	s	u	q	t	e	e	u	a	t	a
2	m	l	r	u	e	u	a	i	a	e	l
3	e	a	n	i	e	u	m	i	a	m	d
4	i	h	r	t	q	n	e	t	a	u	a
5	u	f	d	e	s	r	e	e	b	a	e

= u s u q t e e u a t a
m l r u e u a i a e l
e a n i e u m i a m d
i h r t q n e t a u a
u f d e s r e e b a e

Une fois que le déchiffreur se doute du procédé qui a été adopté, et c'est ce qu'il voit tout de suite à la lettre E, qui en ce

Figure 1. Transposition example from the original page 16.

Once the decipherer suspects the procedure adopted, and he sees at once the letter e, which in this case recurs most often, the decipherment is nothing more than trial. It suffices first to count the letters of the cryptogram and to decompose that number into two factors, here $55 = 5 \times 11$. One factor gives the number of horizontal lines, the other that of vertical columns. The mere presence of a q or an x, the former always followed and the latter generally preceded by a u, betrays the secret of the key.

On the occasion of the recent trials of the nihilists, the Russian newspapers made known the secret cipher adopted by the accused. It is a system of double transposition. The letters, after having been transposed a first time by vertical columns, are transposed a second time in the direction of the horizontal columns. The same word serves as key for the two transpositions; to this end it is transformed into a numerical formula by replacing each letter by an Arabic numeral in such a manner that the value of the numerals corresponds to the rank of the letters in alphabetical order.¹⁵

The original applies this procedure to the word Schuvalow, and then to the sentence: "Vous êtes invité à vous trouver ce soir, à onze heures précises, au local habituel de nos réunions."

schuvalow -> 623781459

Final cryptogram begins:

sciaueselavivonteytrrsoucabioltneulosuder...

horizontales. Le même mot sert de clef pour les deux transpositions¹; à cet effet, on le transforme en formule numérique, en mettant à la place de chaque lettre un chiffre arabe, et en s'y prenant de telle façon que la valeur des chiffres corresponde au rang des lettres dans le classement alphabétique².

Voici le procédé appliqué au mot *Schuvalow* :

$$\begin{array}{cccccccc} a & c & h & l & o & s & u & v & w \\ \hline 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 \end{array} = \begin{array}{cccccccc} s & c & h & u & v & a & l & o & w \\ \hline 6 & 2 & 3 & 7 & 8 & 1 & 4 & 5 & 9 \end{array}$$

S'il s'agissait maintenant de transposer une phrase, comme celle-ci : Vous êtes invité à vous trouver ce soir, à onze heures précises, au local habituel de nos réunions, on procéderait d'abord comme dans le cas précédent, puis on reprendrait la même opération pour les lignes horizontales.

A	1	2	3	4	5	6	7	8	9
1	v	o	u	s	e	t	e	s	i
2	n	v	i	t	e	a	v	o	u
3	s	t	r	o	u	v	e	r	c
4	e	s	o	i	r	a	o	n	z
5	c	h	e	u	r	e	s	p	r
6	e	c	i	s	e	s	a	u	l
7	o	e	a	l	h	a	b	i	t
8	u	e	l	d	e	n	o	s	r
9	e	u	n	i	o	n	s	x	x

¹ C'est une faute très grave de la part de celui qui n'a imaginé le système.

Figure 2. First table for the Schuvalow double transposition example.

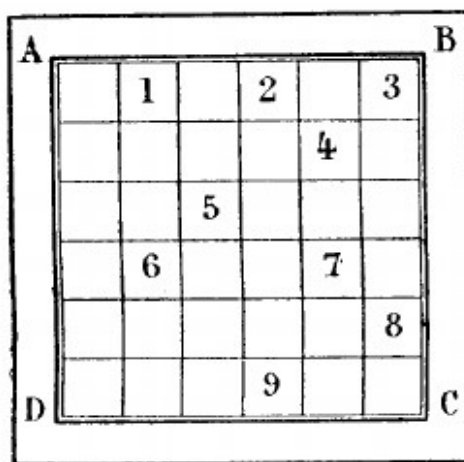
B	6	2	3	7	8	1	4	5	9
6	s	e	i	a	u	e	s	e	l
2	a	v	i	v	o	n	t	e	u
3	v	t	r	e	r	s	o	u	e
7	a	e	a	b	i	o	l	h	t
8	n	e	l	o	s	u	d	e	r
1	t	o	u	e	s	v	s	e	i
4	a	s	o	o	n	e	i	r	z

Figure 3. Second table for the Schuvalow example.

However complicated this transposition may appear, the deciphering of a cryptogram written according to this system could never present insurmountable difficulties in languages where certain letters can appear only in determined combinations, such as the French *q* or *x*. It would seem that the Russian decipherers brought their labour to a successful end in a comparatively short time.

If a more complicated system be adopted, it ceases to be practical without thereby becoming much more difficult to decipher.

I have said that the grille rests upon the principle of transposition. It is an ingenious process, much used in the last century, and one which the recent improvements introduced by the Austrian Colonel Fleissner seem to have rendered indecipherable.¹⁶ The old model shown in the original is a square metal plate divided into thirty-six squares, of which the nine numbered spaces are cut through. To write a phrase, one lays the plate on a sheet of paper on which a square of the same size has been traced, writes the first nine letters in the open spaces, turns the instrument from right to left, and continues until the thirty-sixth letter. The example given produces a compact cryptogram; capitals in the figure mark the initials of the words only for clarity.



nières lettres de la dépêche ; on fait tourner ensuite l'instrument
e droite à gauche, de manière que le côté BC prenne la place
u côté AB ; on inscrit les 9 lettres qui suivent, et l'on retourne
e nouveau la plaque pour continuer la même opération jusqu'à
l 36^e lettre. On aura le cryptogramme suivant, où, pour plus de
larté, j'ai indiqué par des majuscules les initiales des mots :

[Cryptogramme]

Figure 4. Rotating grille, with resulting cryptogram grid.

Colonel Fleissner's grille, his neue Patronen-Geheimschrift, is the fruit of long and patient research and may be varied without limit. But besides certain practical inconveniences, it cannot, in my opinion, suit the uses of war, for the very reason that it imperiously requires secrecy.

B. Method by substitution

In systems that belong to the substitution method, one must distinguish those with an invariable basis, that is to say those in which each letter of the alphabet is represented throughout the same cryptogram by the same character or sign, from those with a variable basis, where the alphabet is changed at every word or at every letter. The former are commonly called single-key systems, and the latter double-key systems.

Single-key systems offer no security; only double-key systems admit combinations more or less indecipherable.

1. Single-key systems

In respect of form, single-key systems may be varied to infinity. One may not only combine the ordinary alphabet in a number of different ways that is in some sort incalculable, but may replace alphabetic characters by numbers, algebraic signs, astronomical signs, fanciful signs, or by groups of letters or figures, and even by whole words or phrases. In substance, however, and for the decipherer, all these combinations constitute only one and the same system, falling under the application of the same process of decipherment.

The simplest and most practical system consists in changing the value of the letters of the alphabet according to an agreed key.

We have seen above how one transforms a key word into a key number. The same procedure may be adopted to establish the order of succession of the letters of the new alphabet. Suppose Champigny is the key; the corresponding numerical formula is 241685379. If we wished to order the cryptographic alphabet according to that number, we should obtain a particular substituted alphabet. "Tournez les positions de l'ennemi" would then give the cryptogram printed in the original.

This system is two thousand years old. The Emperor Augustus already used it to write to his children; and, according to Suetonius and Aulus Gellius, Caesar himself had contrived nothing better for corresponding secretly with his friends than an alphabet in which every letter was moved forward four places.¹⁷ The generic term "Julius Caesar method" is therefore often used for any system resting upon a simple interversion of the letters of the alphabet.

It matters little whether the cryptographic characters are numbers, arbitrary signs, or the ordinary letters of the alphabet.

The Bibliothèque nationale possesses two volumes of ciphered letters found by Moreau at Offenburg in the baggage-wagons of the Austrian General Klinglin, who was charged with the service of secret correspondence. In these letters, very compromising for the royalist party of the time, each character of the clear text is represented by a fixed number composed of two Arabic figures, while word separation is indicated by zero. The general was probably stronger in military tactics than in cryptography, for he plainly ignored the elementary principle just recalled; he believed it enough to cut certain words arbitrarily in order to throw the decipherers off the scent.

Rien de nouveau, si ce n'est la certitude de la suspension d'armes demandée.

[Nothing new, except the certainty of the requested suspension of arms.]

899952450 44520 455625365211250 si ce n'est la 3152891499
14 255452 44520 2311094259467524594995645 44118934
5294 445234114544520.

89 99 52 45 0 44 52 0 45 56 25 36 52 11 25 0 si ce n'est la
r i e n d e n o u v e a u

31 52 89 14 99 14 25 44 52 44 52 0 23 11 0 94 25 94 67
c e r t i t u d e d e l a s u s p
52 45 94 99 56 45 44 11 89 34 52 94 44 52 34 11 45 44 52 0
e n s i o n d a r m e s d e m a n d e
= Rien de nouveau, si ce n'est la certitude de la suspension
d'armes demandée.

Figure 5. Numerical cipher letter from 31 December 1795, with deciphered plaintext beneath (source p. 18).

I cannot enumerate here all single-key systems. I must confine myself to citing, among older authors, the names of Trithemius, Porta, Blaise de Vigenere, Bacon, Hermann, and Mirabeau, who imagined alphabets more or less ingenious, described in the special treatises.¹⁸ For us these inventions can possess only a purely archaeological interest. They are not practical, and all, with the exception of Hermann's, are deciphered with equal ease.

2. Decipherment of single-key systems

Whatever the adopted system, whether with an invariable or a variable basis, the decipherment of a cryptogram whose key is not known comprises two quite distinct operations: a calculation of probability and a labour of trial.

The calculation of probability rests upon a peculiarity common to all languages, namely that certain letters recur more frequently than others, and that the ratio of these repetitions is expressed by a fairly constant average for the nine to twelve principal letters of the alphabet. Thus, in French, English, and German, it is the letter e that occurs most often; in Spanish it is o, in Russian a, and in Italian e and i. In French there is on average one e in five letters.

Thus, if one had to cipher a despatch with an alphabet built on the key Orleans, one would know in advance that the cipher A should recur most often. "Votre depeche a ete dechiffree" would in fact yield a cryptogram in which, of twenty-six characters, A occurs nine times.

ZSRPABATACLAEARABACLMDDPNAA

A calculation that I made upon certain circulars of the Minister of War gave me an average of 560 consonants and 440 vowels per thousand letters, distributed as shown in the original table.

24

JOURNAL DES SCIENCES MILITAIRES.

Un calcul que j'ai fait sur quelques circulaires du Ministre de la guerre m'a donné une moyenne de 560 consonnes et 440 voyelles sur 1,000 lettres, soit :

E = 185	N = 71	D = 42	F = 14	B = 5
S = 88	T = 65	M = 36	Q = 10	H = 4
R = 78	O = 57	C = 34	G = 8	Z = 3
I = 74	U = 52	P = 24	X = 7	Y = 1
A = 72	L = 46	V = 16	J = 6	K et W = 0

Lorsqu'on opère sur des dépêches d'une ou de deux lignes, on ne peut guère compter que sur l'E, et encore arrive-t-il quel-

Figure 6. Kerckhoffs's frequency table for French letters, calculated from War Ministry circulars (source p. 20).

When working upon despatches of one or two lines, one can hardly count on anything but e; and even then it sometimes happens that the letter recurring most often is an s, an r, or an i.¹⁹ Besides the repetitions of isolated letters, there must be noted their binary and ternary combinations, and a host of other peculiarities too long to enumerate here. Thus among binary combinations of e one most often finds es and en; then, in order of importance, se, te, et, de, me, el, em, le.

I do not speak of the very composition of words, for a system that preserved in the ciphered text the outward disposition of the words of the clear text would not present even the shadow of security.

In general, it suffices, in the decipherment of a cryptogram, to know the character representing the letter e in order to be assured of finding, whether by calculation or by trial, the meaning of all the others. One could even lay down as a principle that the value of a cipher is measured by the guarantees it offers against discovery of the sign corresponding to that letter.²⁰

Since my purpose is not so much to teach the reader to decipher as to indicate the course followed by decipherers, I shall content myself with a very elementary example of the manner of proceeding when one does not possess the key.

SP Z BOB CSRRSQSPB CB PSXB JBJ PBOOXB

The character most often met is B; I say that it corresponds to e, and reason thus. BOB, being a trigram beginning and ending with e, can only be ete. Z, a one-letter word, can only be a or y; ete cannot be preceded by y, therefore Z = a. JBJ can only be ses. PBOOXB, of which five letters are already known, must be lettres. SP, in the context "a ete", can only be il, on, or ca; since P is l, SP = il. PSXB becomes lire. The longer group CSRRSQSPB must be difficile. CB is de. We therefore obtain:

Il a été difficile de lire ses lettres.

[It has been difficult to read his letters.]

The longer a cryptogram is, the easier it is to decipher. As a general rule, one line is sufficient.

General Lewal says in his *Etudes de guerre* that a single-key cipher sufficiently guarantees secrecy for ordinary needs and “for matters of no major importance”. I do not know what is to be understood by matters of no major importance; but the reader has been able to assure himself from the cryptogram just analysed that a despatch written under such conditions, when it is two or three lines long and no other artifice has been used, may in some sort be deciphered at sight.

A single-key cipher presents a few slight guarantees only under the following three conditions: first, that the separation of words is not indicated in the cipher text; secondly, that double letters are suppressed; and thirdly, that capitals, accent marks, and punctuation are not used. To avoid transcription errors it is even indispensable to divide the cryptograms into groups of four or five characters.²¹ Our last despatch should therefore have been ciphered thus:

SPZBO BCSRS QSPBC BPSXB JBJPB OXBJ

3. Double-key systems

We have seen that double-key ciphers are those in which the alphabet changes at every letter.

Many combinations with a variable basis have been imagined, but there are scarcely three or four that are genuinely practical and still in honour today. However different in form, they are identical in substance and return to the system expounded at the end of the sixteenth century by Blaise de Vigenère. For nearly three centuries they served as secret cipher to most of the small courts of Germany and Italy; even today they pass as indecipherable in the eyes of persons unacquainted with deciphering methods.

Since every method of cryptographic writing intended for the needs of the army must be capable of application to telegraphy, we need concern ourselves only with systems based solely on the employment of letters or of Arabic numerals, excluding any combination requiring the simultaneous use of both.²²

a. Porta's system

The invention of the first literal double-key system goes back, as I have said, to the physicist Porta. Although he was himself far from perceiving all the importance of introducing a key properly so called into the method of ciphered writing, we must nevertheless regard him as the founder of cryptography.²³

Porta employs eleven different alphabets, which he designates, as seen in the original table, by the letters AB, CD, and so forth, or quite simply by A, C, or B, D. To write with one or another of these alphabets, one chooses, to represent the letters of the clear text, those that face them in the table. Thus if one ciphers with alphabet D or C, a is represented by z, and conversely z by a; b by n and n by b; and so on.

JOURNAL DES SCIENCES MILITAIRES.

on écrire avec l'un ou l'autre de ces alphabets, on
représenter les lettres du texte en clair, celles qui, dar

AB	a	b	c	d	e	f	g	h	i	l	m
	n	o	p	q	r	s	t	v	x	y	z
CD	a	b	c	d	e	f	g	h	i	l	m
	z	n	o	p	q	r	s	t	v	x	y
EF	a	b	c	d	e	f	g	h	i	l	m
	y	z	n	o	p	q	r	s	t	v	x
GH	a	b	c	d	e	f	g	h	i	l	m
	x	y	z	n	o	p	q	r	s	t	v
IL	a	b	c	d	e	f	g	h	i	l	m
	v	x	y	z	n	o	p	q	r	s	t
MN	a	b	c	d	e	f	g	h	i	l	m
	t	v	x	y	z	n	o	p	q	r	s
OP	a	b	c	d	e	f	g	h	i	l	m
	s	t	v	x	y	z	n	o	p	q	r
QR	a	b	c	d	e	f	g	h	i	l	m
	r	s	t	v	x	y	z	n	o	p	q
ST	a	b	c	d	e	f	g	h	i	l	m
	q	r	s	t	v	x	y	z	n	o	p
VX	a	b	c	d	e	f	g	h	i	l	m
	p	q	r	s	t	v	x	y	z	n	o
YZ	a	b	c	d	e	f	g	h	i	l	m
	o	p	q	r	s	t	v	x	y	z	n

au, leur font face. Ainsi. Si l'on cryptographie avec

Figure 7. Porta's paired alphabet table.

But to disconcert the calculations of investigators, Porta, as a man who knew how to decipher, recommends writing each letter with a different alphabet. Moreover, in order not to oblige correspondents to take the eleven alphabets in succession, which would soon betray the secret, he proposes that only four, five, or six be adopted, and that a word be agreed whose different letters shall indicate the alphabets to be chosen successively. This word constitutes the key of the cryptogram; it is written below the text to be ciphered and repeated as often as necessary.

Porta's invention, as we have seen, opens in some sort a new era in the history of cryptography; but it presents two serious inconveniences, which long ago caused it to be abandoned: first the small number of its alphabets, and secondly the need to represent the same alphabet by two different letters. Owing to this latter circumstance, a four-letter word such as poli gives in reality a key containing only two alphabets.

b. Square cipher, or Vigenère table

The square cipher, also called the indecipherable cipher or the cipher par excellence, is nothing other than Porta's system simplified by Blaise de Vigenère, who expounded it in his *Traite des chiffres* in the form still used today. The square cipher enjoyed extraordinary credit among the chancelleries of the eighteenth century, and what might suggest that nothing better has since been found is that it was still used, after 1870, at the Ministry of War.

Dlandol made it known to the public at the time of the Revolution in an opusculé already cited. In chapter VI he says that "this cipher has been named the cipher par excellence because it unites the greatest number of advantages that can be desired for secret correspondence". It would unite them all without exception, he adds, "were it not somewhat slow in execution; but

it fully redeems this inconvenience by the incredible safety of which it is capable. This safety is such that, if the whole universe knew it, provided the key word agreed between the correspondents were not known, one might show one's letter to everybody, and nobody could read it." Certainly citizen Dlandol was a better patriot than skillful decipherer.

The arrangement of Vigenère's table differs from Porta's in that the alphabet is set out as a square of letters, thus yielding as many different alphabets as there are letters in the alphabet.²⁴

La disposition du tableau de Vigenère diffère de celle du tableau de Porta, en ce que l'alphabet y est mis en *nombre carré*, et qu'on obtient ainsi autant d'alphabets différents qu'il y a de lettres dans l'alphabet ¹.

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

Quant au mariage de ce tableau, on procède comme pour le

Figure 8. Vigenere square from the original article (source p. 26).

As to the handling of this table, the procedure is the same as for Porta's system. It is only necessary to note that the upper horizontal alphabet represents the normal alphabet, and that the twenty-six others beneath it are the cryptographic alphabets.

If the despatch "Detruisez le tunnel" is to be ciphered with the three alphabets corresponding to the word BAC, the original gives the resulting rows and cryptogram. Nothing is easier, when one knows the key, than to read a cryptogram written under these conditions. One transcribes the cipher text in equal sections according to the number of alphabets chosen, writes the key beneath, and performs the inverse of the first operation. Thus a cryptogram such as "eyfdaorrakhhgpkqcfmm", the key being Tunis, is at once read by the same procedure.

As we shall see further on, despatches written with Vigenère's table are very easily deciphered. Only in exceptional cases can the system present some security.

c. Saint-Cyr system

This system, long in use, is only a disguised form of Vigenère's table. For want of a proper denomination I have designated it by the name of the school where it is taught and recommended today.

Here is its description, taken from the Cours d'Art militaire of the year 1880-1881, as autographed for the pupils of the first division. "The instrument," it says, "consists of a fixed alphabet beneath which slides a double movable alphabet; two strips of squared paper suffice." A word of three to five letters is taken to form the key. Let the word BAC be adopted and the despatch be "Détruisez le tunnel". Since the key has three letters, the phrase is divided equally into groups of three letters: det-rui-sez-let-unn-el. One ciphers first the first letters of each group, then the second, and finally the third.

To cipher the first letters, one places the first letter of the key, B, taken on the movable alphabet, beneath the letter A of the fixed alphabet; then, taking the first letter of each group on the upper alphabet, one writes the letter corresponding to it on the lower alphabet. One then passes to the second letters of the groups. To cipher them one places the second letter of the key, A, beneath A of the fixed alphabet, and operates as before. The same is done for the third letters. The despatch is then written as shown in the original.

“Assuming,” adds the text, “that the instrument is lost or taken, it reveals nothing; the key must be known.” It is easy to assure oneself that this procedure is merely an abbreviation of the preceding one, by comparing in the two systems the three alphabets corresponding to the key BAC.

Chiffre carré.

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

Système de Saint-Cyr.

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

The only advantage this procedure offers over the preceding is that, in case of loss, the instrument can be remade in two or three minutes. From the cryptographic point of view, it acquires real value only on condition that the order of the letters in the movable alphabet be interverted.

The Cours d'Art militaire says that the instrument might be made more portable by forming it of two concentric circles, one of which would be movable and would turn about its axis. The movable circle would correspond to the double alphabet. This arrangement, represented in the original figure, was imagined by Porta as early as 1563 and has since received numerous applications, such as Wheatstone's cryptograph and the boxes with movable dials sold at the time of the Italian war. All these apparatus, however, some of which are presented in recent works on telegraphy as marvellous inventions, are in reality nothing but a simple Vigenère table.

d. Beaufort system

A rather ingenious modification was made to the square cipher by the English admiral Francis Beaufort in 1857. Though at first sight it seems to affect only the handling of the table, it alters the cryptographic text quite appreciably and gives it, to the eyes of the uninitiated, a true appearance of indecipherability. The Beaufort table is shown in the original.

Une modification assez ingénieuse a été apportée au chiffre carré par l'amiral anglais Francis Beaufort (1857). Quoiqu'elle paraisse au premier abord n'affecter que le maniement du tableau, elle altère assez sensiblement le texte cryptographique pour lui donner aux yeux des non-initiés un véritable air d'indéchiffrabilité. Voici d'abord le tableau de Beaufort :

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

¹ Cf COLORNI. *Scotoaraphia. ovvero Scienza di scrivere oscuro* : Prague. 1593.

Figure 10. Beaufort table.

The phrase "Emparez-vous des hauteurs", ciphered with the key BAC, gives the cryptogram reproduced in the original. The procedure is this: point to the letter e in the first horizontal alphabet, descend in a straight line until the b is reached; then make a half-turn, either to the left or to the right, go to the extremity of the column, and the letter x encountered there is the cryptographic sign sought. The same is done for the other letters.

Emparez-vous des hauteurs, chiffré avec la clef BAC, donnera le cryptogramme suivant :

e m p	a r e	z v o	u s d	e s h	a u t	e u r	s
B A C	B A C	B A C	B A C	B A C	B A C	B A C	B
x o n	b j y	c f o	h i z	x i v	b g j	x g l	j

Voyons maintenant comment on procède. Pointez la lettre *e* dans le premier alphabet horizontal, descendez en ligne droite jusqu'à la rencontre de *b* ; là, faites un demi-tour, soit à gauche, soit à droite ; avancez jusqu'à l'extrémité de la colonne, et la lettre *x*, que vous y rencontrez, est le signe cryptographique cherché ; et ainsi de suite avec les autres lettres.

Les déchiffreurs anglais, que le système de Beaufort a tant émerveillés, ne se doutaient certainement pas qu'on pût obtenir le même résultat avec les systèmes de Vigenère ou de Saint-Cyr en retournant tout simplement l'alphabet normal ¹.

Il est facile de s'en assurer par l'inspection des deux figures qui suivent :

Chiffre carré.

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

Système de Saint-Cyr.

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

¹ Il est probable que l'amiral anglais lui-même n'a jamais cru à la possibi-

Figure 11. Beaufort example and comparison with square cipher and Saint-Cyr arrangement.

The English decipherers, whom Beaufort's system so greatly astonished, certainly did not suspect that the same result could be obtained with the systems of Vigenère or Saint-Cyr by simply reversing the normal alphabet.²⁶ It is easy to confirm this by inspecting the two figures that follow in the source.

The result would again be the same if, instead of interverting the order of the letters in the normal alphabet, one placed in the square cipher the alphabet azyxwvutsrqponmlkjihgfedcb according to the principle shown in the original.

e. Gronsfeld system

This system differs from the two preceding only in that the work may be done mentally, instead of requiring the assistance of a table or any apparatus. M. Bontemps, inspector of telegraph lines, expresses himself on it as follows: "Suppose that any number whatever has been chosen as a key; under the phrase to be transmitted one writes it as many times as may be necessary, establishing a correspondence between successive letters and figures. For the letter to be sent, one takes the letter that is placed in the alphabet at a distance from the true letter equal to the figure written beneath it, and one thus composes a grimoire of which it is impossible to discover the key, were one endowed with the perspicacity Edgar Poe attributes to his hero in *The Gold-Bug*, or the intelligence of the agents employed to decipher the correspondence of the Duchess de Berry in 1832, according to the narrative in the memoirs of M. Gisquet."²⁷

	A	B	C	D	E	F	G	H	I	J etc.
A	a	z	y	x	w	v	u	t	s	r
B	b	a	z	y	x	w	v	u	t	s
C	c	b	a	z	y	x	w	v	u	t
D	d	c	b	a	z	y	x	w	v	u

e. Système de Gronsfeld.

stème ne diffère des deux précédents qu'en ce que le
it être fait de tête, au lieu d'exiger le concours d'un

Figure 12. Schematic of the reversed alphabet arrangement preceding the Gronsfeld discussion.

With all respect to the author just cited, Count Gronsfeld's system is not much more difficult to decipher than a modest single-key cipher; indeed it is only a disguised form of Vigenère's table.³⁸ The correspondence between figures and alphabets is immediate: zero leaves the alphabet unchanged; one advances the alphabet by one place, two by two places, and so on. The numerical key therefore serves only to name a succession of ordinary shifted alphabets.

If the key be 123 and the clear phrase be "Nous partons demain", the letters are displaced successively by one, two, and three places. The ease of execution explains the favour the method has enjoyed; but this very ease must not be confounded with cryptographic strength. A short numerical key, repeated, gives the decipherer repeated coincidences, and once the length of the key is suspected the separate columns may be attacked by the familiar calculation of frequencies.

For this reason the Gronsfeld system, however convenient for the hand and memory, does not solve the military problem as I have stated it. It does not remove the necessity of secrecy; it merely conceals the old Vigenère mechanism beneath arithmetic of the simplest kind.

The author next discusses a refinement: the use of a letter of arrest, inserted in the cryptographic text, to indicate interruptions in the repeated key. For example, in writing a key word such as Epaminondas beneath the phrase "Nous partons demain", the key may be broken arbitrarily. The point of interruption is then indicated by one of the letters of the key, inserted at the desired places in the cipher text.

To avoid all confusion in the meaning attributed to this letter of arrest, it is replaced in the cryptographic text by an Arabic numeral corresponding to its place in the key word. In the example printed by Kerckhoffs, where P is the second letter of the key, it is replaced by 2 wherever it must not play the role of a letter of arrest.

With the square cipher the cryptogram would then be:

rduePt2rfwagPhtPa2az.

To prevent the decipherer from making guesses upon the first letters of the despatch, it is preceded by a few nulls, taking care to indicate, by the letter of arrest, the point where the true text begins. The cryptogram could finally be written thus:

Xmoprduet2rfwagphtpq2az.

AUG. KERCKHOFFS, Doctor of Letters, Professor at the Ecole des hautes études commerciales and at the Ecole Arago.

(To be continued.)

Endnotes and bibliographical notes

1. Kerckhoffs notes that encyclopaedic dictionaries commonly file such material under steganography, cipher, or secret writing. Ancient and early modern terms include *ars notarum*, *ars zipherarum*, *polygraphia*, *scotographia*, *cryptologia*, *steganologia*, *cryptomenyitics*, and others; the Germans say *Geheimschrift* or *Chiffreschrift*, and the English *cryptography*.

2. Among the devices mentioned are letters concealed in the soles of a messenger's shoes, communications hidden in ulcers or in women's earrings, disks pierced with twenty-four holes through which a thread passed, and carrier pigeons. Aeneas, fourth century BC, is the earliest military author whose writings were known to Kerckhoffs.
3. The ancient references named by Kerckhoffs include Polybius, Plutarch, Dion Cassius, Suetonius, Aulus Gellius, Isidore, and Julius Africanus. He adds that Philo of Byzantium had written a treatise on sending secret letters, now lost.
4. Gaspar Schott, *Schola steganographica*, 1665; Gustavus Selenus, *Cryptomenytices et cryptographiae libri IX*, 1624.
5. Beausobre's note is in the *Commentaires sur la defense des places*. Kerckhoffs also cites Mazarin's *Breviarium Politicorum*: write secret matters with your own hand, and entrust them to no engraving unless you write in cipher.
6. Kerckhoffs cites Bardin's *Dictionnaire de l'Armee de terre*, 1843.
7. Baron Fain, *Manuscrit de 1812, 1827*. Kerckhoffs notes that Colonel Fleissner wrongly attributed to Napoleon the invention of a new cipher.
8. General Lewal, *Tactique de marche*, 1876.
9. Bardin, article on steganographic ciphers.
10. The officer was Captain Henri Berthaut, whom Kerckhoffs describes as certainly one of the ablest decipherers on the staff.
11. Voltaire, *Dictionnaire philosophique*, article "Poste". Kerckhoffs also cites a similar judgement by the Earl of Clarendon upon self-proclaimed decipherers.
12. Kerckhoffs says that the bibliographical information is included for readers wishing to pursue the matter further, since almost all the books cited could then be found at the *Bibliothèque nationale*.
13. Kerckhoffs cites Kluber, *Kryptographik*, chapter XIII, and Du Moncel, *Exposé des applications de l'électricité*, III, p. 530.
14. He adds that null letters must be inserted as needed so that the total number of letters fits the table; in the first example five nulls are needed.
15. Kerckhoffs remarks that using the same word for both transpositions is a very serious fault, and that repeated letters in a key word must be counted in alphabetical order as successive letters.
16. He attributes the grille to Cardano in the sixteenth century, citing *De subtilitate*, and also de Prasse, *De reticulis cryptographicis*, Leipzig, 1799. Colonel Fleissner's *Handbuch der Kryptographie* appeared at Vienna in 1881.
17. Suetonius, *Octavian*, chap. 88; Isidore, *Origines*, I, 24; Suetonius, *Caesar*, chap. 56; Aulus Gellius, *Attic Nights*, XVII, 9. Kerckhoffs also notes Biblical substitutions in *Jeremiah*.
18. Among the special works cited are Hanedi, Selenus, Frederici, Rees's *Encyclopaedia*, the *Encyclopaedia Britannica*, Lacroix, and others.
19. Kerckhoffs gives the most frequent German letters as E, N, I, R, S, T, U, D, A, H; and the English as E, T, A, O, N, I, R, I, H, D, L, preserving his printed order.
20. Porta's *De furtivis litterarum notis* is named as the first cryptographic treatise to discuss principles of decipherment. Kerckhoffs then lists later works by Nicéron, Gravesande, Breithaupt, Davys, Conrad, Thicknesse, Kluber, Vesin de Romanini, Kasiski, Fleissner, and others.
21. Because the telegraph administration counted secret despatches in groups of five, Kerckhoffs considered pentagram division preferable.
22. Kerckhoffs observes that international telegraph conventions were moving toward excluding the simultaneous use of letters and numerals in secret language; he also notes the difficulty of avoiding errors in telegraphic transmission unless ciphered despatches are cut into short fixed groups.
23. Porta, *De furtivis litterarum notis*, book II, chapter 16. Kerckhoffs also insists that Porta, not Trithemius, deserves to be called the father of modern cryptography.
24. Father Kircher later replaced the letters of the Vigenère table by numbers, whence the name *Abacus numeralis*; Schott commented on Kircher's system.
25. Kerckhoffs notes that when the alphabet is "interverted" the Saint-Cyr system gives a different text.
26. Kerckhoffs suspects that Admiral Beaufort himself did not realise the system could be reduced to an ordinary square cipher.
27. Bontemps, *Les systèmes télégraphiques aériens, électriques, pneumatiques*, Paris, 1876, p. 261.

28. A note reports that in an 1873 lecture at the Society of Military Sciences in Vienna, Dr Orges maintained that this cipher had been invented by General Trochu.