

Military Cryptography

Second instalment, February 1883

Auguste Kerckhoffs

Military Cryptography

Journal des Sciences Militaires, February 1883, Volume IX, pp 161-191. Translation of the second instalment of this article. A period-conscious English working translation of the scanned original, with 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 archæic 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

4. Decipherment of double-key systems

Except for a small work written in 1863 by the German Major Kasiski,¹ no essay has, to my knowledge, been published on the decipherment of secret writings with a double key. Everything to be found in Porta, Cospi, Breithaupt, 's Gravezande, Thickenesse, Klüber, Lacroix, Vesin, Joliet, and others applies only to single-key systems; and even these authors have scarcely thought of deciphering cryptograms in which the separation of words is not ostentatiously indicated.²

A passage in the *Interprétation des Chiffres* by Cospi, secretary to the Grand Duke of Tuscany, might lead one to believe that decipherers have at all times avoided revealing their methods of decipherment to the profane. On page 3 one reads: "There are two sorts of ciphers, some simple and the others compound; leaving aside the latter as almost impossible to decipher, we shall speak only of the former, which are the simple ones."³ Yet it is scarcely probable that a man of Cospi's talent did not know how to decipher the systems which Porta and Vigenère had published half a century earlier.

Major Kasiski based his system of decipherment almost exclusively upon the determination of the letters of the keyword. While paying due homage to the author's skill, I cannot help finding this a strangely complicated method, and one which in many cases must give a negative result. I shall indicate a procedure which seems to me not only surer, but also simpler and more methodical. Without wishing to give a complete work, for which I do not really see the

¹ *Die Geheimschriften und die Dechiffirkunst.*

² Colonel Fleissner, in his *Handbuch der Kryptographie*, adopted Major Kasiski's method of decipherment without any modification.

³ I quote from Father Nicéron's translation.

necessity, I shall nevertheless try to develop the question sufficiently so that the reader who wishes to practise the “art of deciphering” may find for himself, and without difficulty, all the small details whose complete exposition would require at least fifty pages. *Fabricando fit faber*: one becomes a decipherer by deciphering.

I said above that, in every system by interversion, the decipherment of a cryptogram for which one has not the key involves two quite distinct operations: a calculation of probability and a work of trial. In single-key systems, where only one alphabet is used, calculation and trial are necessarily limited to determining the arrangement of that alphabet. In double-key systems two unknowns must be found: first, the number of alphabets; second, their respective arrangement.

a. Number of alphabets

At first sight it might seem that the elements of investigation must be lacking for establishing the number of letters or alphabets in the key; yet nothing is easier.

Suppose one has to encipher a phrase such as:

Vous ne pouvez vous défendre sans vous exposer, etc.
[You cannot defend yourself without exposing yourself, etc.]

Since between the first two instances of *vous* there is a distance of 8 letters, and between the second and the third a distance of 12 letters, it will happen, if I take a key of 4 letters, that the three instances of *vous* will be enciphered with the same alphabets, and will give three similar tetragrams. If there were a fourth *vous* later in the text, it would again give a similar tetragram, provided that it were separated from the last by a number of letters forming a multiple of 4.

Take another example: *la présence de soldats ennemis nous a de nouveau été annoncée ce matin de différents côtés* [the presence of enemy soldiers has again been reported to us this morning from different quarters], and suppress the intervals:

lapresencedesoldatsennemisnousadenouveaueeteannoncee
matindedifferentscotes

In these 75 letters there occur 18 repetitions, of which 3 are trigrams, *nou*, *sen*, *nce*, and 15 are bigrams, *en*, *es*, *de*, *ce*, *no*, *te*, *ts*, etc.

One may take a key of 5, 6, 7, 8, 9, or 10 different alphabets; it will always happen that one or another of these repetitions is enciphered with the same alphabets, and that one will thus have a cipher text presenting, at the corresponding places, similar groups of letters.⁴ I now generalise the case, and lay down the two following principles: first, in any cipher text, two similar polygrams are the product of two similar groups of letters enciphered with the same alphabets; second, the number of cipher-signs comprised in the interval between the two polygrams is a multiple of the number of letters in the key.⁵

⁴ In enciphering this phrase with a key of 3 alphabets, one would have 9 repetitions; with 4, 5, 6, and 12 alphabets, one would have 8; one would have only 3 with 13 alphabets, and none with a key of 11, 14, or 18 alphabets.

⁵ I hardly need point out that it may very well happen that two similar bigrams, for a trigram it is already very rare, are the product of two different groups of letters.

To obtain the exact number of alphabets in the key, therefore, it is only necessary to seek the common factor contained in the numbers which represent the letters of the respective intervals.

Let us apply this reasoning to the following cryptogram:

R MU U W Q P M Q GXH W B GG K K K N I TM U X W W TMG GXH E P H

We have here four repetitions: one trigram, GXH, and three bigrams, MU, GG, TM.

MU to MU'	21 cipher-signs	= 7 x 3
GG to GG'	15	= 5 x 3
TM to TM'	6	= 2 x 3
GXH to GXH'	21	= 7 x 3

The common factor is 3; and, in fact, the cryptogram has been enciphered with a key of 3 letters.

It is easy to understand that the chances of meeting combinations of letters produced by the encounter of the same alphabets are in inverse ratio to the length of the key and in direct ratio to the length of the cryptogram.

When the relation of the letters of the key to those of the cipher-signs in the cryptogram is such that no repetition can have occurred, the decipherment presents difficulties, and one is obliged to have recourse to trial. This is a point to which I shall return later.

b. Ordering of the alphabets

Let us first observe that the number of different alphabets can scarcely go beyond the number of letters in the alphabet itself. With a lower or higher number it becomes impossible to represent the key by a word, or at least there are certain difficulties in the handling of the key. Besides, what gives value to a system is not the possibility of using a great number of different alphabets, but rather the greater or lesser difficulty of determining the number of alphabets employed.⁶

These 26 alphabets may be ordered in three different ways:

1. The letters may follow one another in the order of the normal alphabet, as in the table of Vigenère.
2. Or that order may be interverted in some fashion, but the 26 alphabets are nonetheless disposed in a square.
3. Or, again, the 26 letters may be placed in a different order in each of the 26 alphabets.

The decipherer generally has no trouble establishing which of these three arrangements has been adopted.

a. Alphabets not interverted

Let us take up the preceding cryptogram again and divide it into slices of three cipher-signs:

⁶ A German author, Krohn, *Buchstaben- und Zahlensysteme für die Chiffri- rung von Telegrammen* (Berlin, 1873), failed to grasp this principle, and composed, for use in cryptographic correspondence, a dictionary containing 3,200 alphabets. It is at once too much and too little.

1 2 3 1 2 3 1 2 3 1 2 3 1 2 3 1 2 3 1 2 3 1 2 3 1 2 3 1 2 3
 R M U U W Q P M Q G X H W B G G K K K N I T M U X W W T M G G X H
 E P H

We know that it is the letter E which must recur most frequently. If, therefore, I collect the letters which, in the several slices, belong to the same alphabet, it will be easy for me to establish which are the three cipher-signs representing the letter E. Moreover, since each of the 26 alphabets is characterised by the cipher-sign corresponding to E, the knowledge of this single cipher-sign will necessarily entail knowledge of all the others of the same alphabet, whether the cryptogram has been enciphered with the table of Vigenère or with the systems of Saint-Cyr and Gronsfeld. We shall therefore have:

I	II	III		
R	M	U		
U	W	Q		
P	M	Q	1st column:	G = E
G	X	H	2nd column:	M = E
W	B	G	3rd column:	H = E
G	K	K		
K	N	I		
T	M	U		
X	W	W		
T	M	G		
G	X	H		
E	P	H		

If one now seeks in our table on page 30 which alphabets have the letter E represented by the cipher-signs G, M, H, one finds that these are the third, ninth, and fourth, that is to say those corresponding to the key *cid*, or to the number 283 in Gronsfeld's system.⁷ The rest follows of itself.⁸ Here, moreover, are the three alphabets:

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

= Personne ne peut déchiffrer votre dépêche.

⁷ Since in Gronsfeld's system the first alphabet is represented by a zero, the order number of each alphabet must be diminished by one.

⁸ When the decipherer knows that a text in a foreign language has been enciphered under these conditions, he need not concern himself, for the success of his work, with whether he understands the language or not. It is enough for him to be informed of the letter which occurs most often in that language.

Thus the cryptogram reads:

Personne ne peut déchiffrer votre dépêche.
[No one can decipher your despatch.]

When the despatch is short, it sometimes happens that the coefficient of repetitions in one series or another leaves us in doubt as to the cipher-sign corresponding to E. This disadvantage is not very great, especially if the key has only five or six letters, for the context immediately sets us on the track.

It may even happen that, in a cryptogram of several lines, none of the most frequently repeated cipher-signs corresponds to the letter E. There is a very simple way of determining the different alphabets of the key in spite of this anomaly.

To grasp this procedure well it must be remembered that, in alphabets which are not interverted, the relative position of the letters is always the same. In the alphabet where *l* corresponds to E, the following letter, or *m*, necessarily corresponds to F, and *r* will correspond to K and *d* to W. Likewise, in the alphabet where the letter E is represented by *p*, the letters K and W will be represented by the cipher-signs *v* and *h*. Now, since K and W occur only exceptionally in French, the decipherer will reject any alphabet in which the cipher-signs corresponding to those letters have a rather high coefficient.

Suppose now that, in the count of the letters of such and such a column, I find, as the highest frequencies, 12 *l*, 9 *r*, 8 *d*, 6 *v*, 5 *h*, 5 *u*, 4 *x*, 3 *o*, 3 *q*. I shall see at once, on inspection of the table, that the alphabet sought must be that in which E is represented by the cipher-sign *h*, for in the eight other alphabets the cipher-signs *l*, *r*, *d*, *h*, *u*, etc. correspond now to a K, now to a W, an H, a Y, or a Z, which, given the very small importance of those letters, is an inadmissible case.

From the point of view of the decipherability of despatches, systems with non-interverted alphabets offer no more guarantees than a single-key interversion in which word separation is not indicated.⁹

b. Irregularly interverted alphabets

When, in deciphering a cryptogram, it is impossible to construct a meaning with the alphabets that the returns of the letter E seemed to indicate, one must suppose oneself in the presence of a system with interverted alphabets, and must in some sense take by storm, one after another, the first cipher-signs of the despatch. If the cryptogram is fairly long, the solution of the problem rarely presents insurmountable difficulties. It requires only a little patience and a certain spirit of induction. It is then that, beyond the calculation of isolated repetitions, one must mark the returns of certain binary and ternary combinations of which I spoke on page 24; one must also know how to profit from the information supplied concerning the probable nature of the correspondence, and take account of the style which the circumstances or the respective situation of the correspondents require. Thus, to cite an example, the binary combination *ez* is extremely rare in correspondence between persons who address one another

⁹ M. d'Auriol, *Manuel de la correspondance secrète, postale ou télégraphique* (Paris, 1867), published a table which allows the letters of the plaintext to be enciphered two by two. Apart from the fact that one can establish on letter combinations the same calculation as on letters taken singly, the system offers too much purchase to trial, and moreover requires absolute secrecy.

as *tu*, while, on the other hand, most of the instructions delivered, in the field, to subordinates begin with *vous* or *le*.

We shall decipher a despatch sent from London to the Havas Agency concerning the military affairs of Egypt.

London, 2 September.

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

Let us first try to determine the number of alphabets in the key:

RB to R'B'	= 55	= 11 x 5
RB to R"B"	= 105	= 21 x 5
BJ to BJ'	= 50	= 10 x 5
BJ to BJ''	= 225	= 45 x 5
BG to B'G'	= 5	= 5
BG to B"G"	= 40	= 8 x 5 or 4 x 10
RE to R'E'	= 115	= 23 x 5
MW to M'W'	= 94	= 47 x 2
MJ to MJ'	= 105	= 21 x 5
PQ to P'Q'	= 305	= 61 x 5

I have noted here only half the repetitions, but that is enough to show us that the key must be composed of five letters.

If we next divide the cryptogram into slices of five cipher-signs and make the count of repetitions by column, we find:

1st column: 19 j, 8 r, 7 d, 7 n, 7 s, 7 c, 6 i, 5 l, 4 g, 3 p, 3 u, 2 h, 2 k, 2 q, 2 e, 2 a, 2 z, 1 m
 2nd column: 14 b, 10 e, 7 w, 7 j, 6 a, 5 p, 5 t, 5 v, 5 d, 5 k, 4 f, 3 u, 3 h, 3 q, 2 m, 1 l, 1 i, 1 z, 1 g, 1 x
 3rd column: 12 m, 9 g, 9 a, 7 x, 6 j, 6 u, 6 b, 6 c, 5 z, 4 s, 4 p, 4 y, 2 k, 2 n, 2 l, 1 q, 1 o, 1 i, 1 t
 4th column: 15 b, 8 w, 7 e, 7 h, 7 k, 6 u, 6 a, 6 m, 5 v, 5 d, 5 j, 3 t, 2 p, 2 i, 1 s, 1 c, 1 f, 1 q
 5th column: 16 z, 12 j, 9 x, 8 g, 7 w, 6 o, 4 l, 4 k, 4 r, 3 c, 3 h, 3 m, 3 n, 3 e, 1 a, 1 v, 1 s

Since we are working upon a cryptogram of some extent, we are authorised to believe that the cipher-sign most often repeated in each column corresponds to the letter *e*. We also admit, as a necessary consequence, that the second and fourth columns (*B* = *e*) represent the same alphabet.

As to the probable contents of the cryptogram, we should expect to find in it words such as: *Arabi, Wolseley, Suez, Ismaïlia, canal, général, soldats.*

Let us also remark that, among the first ten cipher-signs, we already know three which represent *e*, namely:

1	2	3	4	5	1	2	3	4	5
R	B	N	B	J	J	H	G	T	S
.	e	.	e	.	e	.	.	.	.

That said, I ask myself by what part of speech a telegram addressed to newspapers may well begin, and I proceed, as must always be done, by exclusion.

It is scarcely probable that the first phrase is interrogative or imperative. If, therefore, the first word is a verb, it must be in the infinitive or present participle. The very simple style of this kind of communication does not allow one to suppose that it is an infinitive. Nor is it a present participle, for it would have to belong to a verb of four syllables with an *e* in each syllable, and *régénérer*, *régénérant*, which alone is in this case, does not suit the situation.

As for substantives, one must eliminate common nouns, which are always preceded by some determinative. The same must be done for the adjectives *divers*, *différent*, *maint*, and *certain*, which alone could begin the sentence without being preceded by *de*, but which do not have the *e* in the required place.

Among proper names, those that are in play of course, numerals, adverbs, prepositions, and conjunctions, there is not a single word which has its two *es* in the third and fourth places.

The cryptogram can therefore begin only with the article *le*, *les*; the pronouns *je*, *me*, *ce*, *cet*, *ces*, *mes*, *ses*; the negative *ne*; or the preposition *de*.

If it is the negative *ne*, a verb in the present participle must follow, such as *recevant*, *revenant*, and GTS represents the ending *ant*. Now that is inadmissible, *t* being a very common letter and the cipher-sign S occurring only once in the fifth column.

We must also reject *les*, *cet*, *ces*, *mes*, *ses*, since the third cipher-sign N can scarcely be the letter *s* or *t*, for the reason that it occurs in all only twice in its column. Since the first cipher-sign R occurs eight times, it is likewise impossible that we are dealing with a *j* (*je*). It is therefore *le* or *ce*, but rather *le* than *ce*, because of the frequency of the cipher-sign R.

Le or *ce* must be followed by a substantive, an adjective, or a numeral; and, let us note it well, the word must have an *e* in the first two syllables. No numeral is in this case. The adjectives *récent*, *décent*, and *téméraire*, which have the two *es*, must be rejected, the coefficient 1 of the cipher-sign N being, as has already been said, too weak for a *t*. *Détestable* will not do either, since the twelfth cipher-sign T is not an *e*. The substantives *désert* and *télégraphe* are, because of their *t*, in the same case as *décent* and *téméraire*. One finds only *général* which fulfils the required conditions. We consequently decide for *le* instead of *ce*. I write these two words down and continue.

S P T A B G J X

Le général e . e .

It is to be presumed that the despatch says which general is meant. It is therefore a proper name that follows. The cipher-sign S must be a very little-used letter, such as *k*, *w*, *y*, or *z*, for, as we have said, it occurs only once in its column. We have besides an *e* in the fifth and seventh positions, and this latter *e* is followed by a cipher-sign with coefficient 1. That answers exactly to *Wolseley*.

Z B G J I C E M Q A M

Le général Wolseley . e l e e

It is still probable that the verb follows its subject. We already know the value of the second, third, and fourth cipher-signs, and we know that Z has a fairly high coefficient. If Z is the auxiliary verb *a*, the following participle is *élevé* or *électrisé*, but these do not have the final *e* in the required place. Therefore the verb is in a simple tense. Of the only possible verbs, *dépend*, *dément*, *mène*, *retenu*, and *télégraphie*, one must prefer the last because of the final *e*.

U W I V G A G N E

télégraphie a i l . . a

There is every reason to suppose that *télégraphie* is followed by *que* or *qu'il*, or else by a place-name. It is not *que*, since I is not an *e*. It is not *qu'il*, for we know the *l* (=T) of the second column. It is therefore probably a place-name.

The place-name must be preceded by the preposition *de*. Here, however, it must be a simple *d'*, for the *e* of the third column is represented by a B. Among place-names beginning with a vowel, having an *a* in the fourth position and an *l* in the sixth, one can cite only *Ismaïlia*.

I M W R E Z K Z S U A B R R B P B J C

d'Ismaïlia . . i l a t . e . d s e . l e . e n .

The turn of the sentence, as well as the presence of *il*, immediately indicates that IM signifies *qu*; the verb must follow, and from the letters we already know one easily divines that this verb is *attend*. As for the final group, the dictionary gives only the words *selle* and *seulement*, which square with the whole. It is obviously the latter that we have here.

GYBGJJMHENPM

qu'il attend seulement . . e l e . e r . i . e

The adverb *seulement* is rarely followed by *que*; but as G occurs only once in its column, which applies very well to *q*, and as we have in the third position an *e*, we must admit *que*. The last group is a word beginning with a consonant, since it is preceded by *le*, and that consonant recurs fairly often. There is, moreover, an *i* in the fifth position. *Service* alone answers to these data.

UZCHGWOU DCKOJ KKB C P V P M J N P G K W P W A

d e t r a r t . e t . e . o m m u n i c a t i o n s

This passage presents no difficulty, and we read: *de transports et de communications* [of transport and communications]. The end of the sentence is still easier: *soit complètement o.ga.ise .our .a.re.ne n.u.elle marche en ..ant*, that is, *soit complètement organisé pour faire une nouvelle marche en avant* [is completely organised for making a fresh forward movement].

I stop here. It will be easy for the reader to decipher the rest himself.

Apart from the number, it is possible for the decipherer to determine the value of the letters composing the key only when the despatch has been enciphered with the Saint-Cyr system. Unless one admits that the key must necessarily be a French word, or have some meaning, every despatch written with alphabets arranged in a square admits 26 different keys, according to the initial alphabet of the table. Nothing shows better than this consideration how wrong Major Kasiski was to found his method of decipherment upon the actual value of the letters of the key.

In the present case the key is *degel* with the Saint-Cyr system, and *puluy* with the table which follows.

Once one has been able to determine the number of letters in the key, assuming that the despatch has a certain length and that one has been able to collect some information about the correspondents or the probable nature of the contents, it is very rare that a cryptogram cannot be deciphered. In somewhat difficult cases it is generally the first two or three words which play the part of traitors. Now, nothing is easier for the decipherer than to draw up a list of the words which, in wartime, may begin a despatch and then to classify them according to the place of the E within them. Those which contain no E will thereby be all the more pointedly brought to his attention.

c. Regularly interverted alphabets. Symmetry of position

I have deciphered the preceding despatch without seeking to know whether it had been enciphered according to a system which orders its alphabets in a square, or whether the correspondents had merely chosen five different alphabets at random. Yet this is a very important point and one which the decipherer must never neglect. From the moment, indeed, that the alphabets are arranged in a square, and that the meaning of a common cipher-sign has been found in two or more alphabets, one may, by means of a simple addition, determine the

place which any new cipher-sign, whose value may be established in a single alphabet, must occupy in the different alphabets.

To understand this peculiarity, which has not yet been noticed in any work on cryptography, let us consider for a moment the table which served to encipher our cryptogram.

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

The arrangement of this table differs from that of Vigenère only in that the normal order of the letters has been interverted. The same letters, while never occupying the same place twice in relation to the ordinal number of the vertical columns, nevertheless always follow one another in the same order in the horizontal columns.¹⁰ Thus, in each of the latter, R is always followed by E, and E is always at an interval of one rank from P and at an interval of four ranks from L. Once, therefore, that one knows the place of R in two alphabets, the place of the cipher-signs

¹⁰ It matters little, and this is an essential point to note, whether the order of succession of the letters in the vertical columns is the same as in the horizontal columns. That order is generally observed only to enable the correspondents to establish their table more easily from memory.

E, P, and L will be determined in the second alphabet as soon as one has been able to establish it in the first.

Take an example. I suppose that, in trying to decipher a despatch enciphered with a key of three alphabets, one has already found the value of the 19 cipher-signs indicated below, namely EPBLAFN for the first alphabet, UAT for the second, and TDFHKMRSIC for the third. Since the cipher-signs of the three alphabets, taken two by two, have a common letter, A and T, I can carry the letters of one alphabet into the other on the simple condition of placing them, in the three alphabets, at respectively equal distances from the common letter.

	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	
1	.	e	.	p	.	b	l	.	.	a	.	.	.	.	.	f	.	.	.	.	.	.	.	.	n	.	
2	.	.	.	.	.	.	.	.	.	.	.	.	.	u	.	.	.	.	a	.	.	t	.	.	.	.	
3	.	.	t	.	.	d	f	.	.	h	.	.	km	.	.	.	.	r	.	s	.	.	.	.	.	i	e
1	r	e	s	p	u	b	l	i	c	a	.	.	t	.	.	d	f	.	.	h	.	.	km	.	.	n	.
2	.	.	h	.	.	km	.	.	.	.	.	.	.	.	.	r	e	s	p	u	b	l	i	c	a	.	
3	.	.	.	.	t	.	.	d	f	.	.	h	.	.	km	.	.	.	.	.	.	.	.	.	.	.	.

If I had taken account of this peculiarity in deciphering our despatch, I could have stopped at the fifth word, the number of letters already deciphered, increased by the number of letters known by symmetry of position, being more than sufficient to decipher the rest of the cryptogram, so to speak, as fast as the pen could move.

This may easily be seen by inspecting the table below, in which the letters known through the decipherment of the first five words are represented by capitals, while those whose value is revealed by the principle of symmetry of position are shown by lower-case letters:

	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
1			g	h	J		m	Q	N		x	R	e	s	P	u	b		l	c	a	z		t	v	w
2.4	E	s	p	U	B		l	c	A	z		T	V	w			g	H	J		m	q	n		X	r
3	G	h	j		M	q	N		x	r	e	s	p	u	b		i	C	A	Z		t	v	w		
5		i	c	a	z		t	v	W			G	h	J		M	q	n		x	r	e	S	p	u	b

It is all the more important not to neglect this peculiarity of alphabets arranged in a square because one can scarcely have occasion to decipher a cryptogram whose 26 alphabets are ordered at random. Such a system would be little practical and, by that very fact, inapplicable in wartime. For, if the obligation of committing to memory the arrangement of a single alphabet may sometimes present certain difficulties, what embarrassment would there not be when it was a matter of retaining 26 different alphabets, each ordered according to a plan that excludes all regularity? One would be obliged to have recourse to written notes, and the value or security of the system would depend only upon the prudence of the agent called upon to apply it. Thus all combinations of some value which have been devised in recent years, such as, for example, Wheatstone's cryptograph, rest upon a regular interversion of the alphabet, and the principle I have just set out is perfectly applicable to them.

d. Undetermined alphabets

If, in deciphering a cryptogram with interverted alphabets, it is impossible to determine the number of alphabets in the key, either because the despatch is too short or because the key is too long, the solution of the problem presents difficulties which, if not insurmountable, are at least capable of exhausting the patience of the most skilful decipherer.

The situation changes if one has in one's possession several cryptograms written with the same key, however short they may be. By arranging them one below another one can perform, on the repetition of letters, a calculation analogous to that which we made above on cipher-signs grouped by slices or columns.

Here are a dozen very short cryptograms which have been enciphered according to the preceding table, and with a whole phrase: *je me mets sur la défensive* [I place myself on the defensive]. We shall see that their decipherment is fairly easy.

- No. 1. UHYBRJIMBCFAMMTJTDMRIQ
- No. 2. UHWPRBQLKIBEWREJRBKLGIXBQEXHM
- No. 3. IEWHCHQKQMTMVGJJEDZVA
- No. 4. UWVRRHIKMCWWEGHDCXSRQH
- No. 5. UHSHAHKSVCJWZVXJYNDMQQN
- No. 6. YHVHMAGQKCWXPVIHHWLZVLTHV
- No. 7. LHVHAAGRLPFMSOHIPWZZJELQRBW
- No. 8. SWUIRXICJUFSGWRSZBAAL
- No. 9. UHWHVAYULCJWOUKDEBKQ
- No. 10. YWXHYHBALGBVPSWIWWJRRH
- No. 11. WQREXBIENHVMVYMHSIYM
- No. 12. SWUHDHPJJCKXGMHL
- No. 13. GQVQRVOTQQSPWR

Let us note in passing that, among the 22 letters of which the key is composed, 3 are repeated and thus we have in reality only 14 different alphabets. This is a case which it is scarcely possible to avoid and which the decipherer must know how to turn to account.

In order not to extend the demonstration excessively, I shall attach myself only to the first two words of Nos. IV, V, VI, and VII; moreover, so that the reader may more easily follow my reasoning, I shall put in advance the letters of the key above the corresponding columns.

	1 J	2 E	3 M	4 E	5 M	6 E	7 T	8 S	9 S	10 U	etc.
I	u	h	y	b	r	j	i	m	b	c	fammtjt d m r i q
II	u	h	w	p	r	b	q	l	k	i	blwre j r b, etc.
III	i	e	w	h	c	h	q	k	q	m	tmvgjjedzva
IV	u	w	v	r	r	h	i	k	m	c	ww e g h d e x s r q h
V	u	h	s	h	a	h	k	s	v	c	jwz etc.
VI	y	h	v	h	m	a	g	q	k	c	wxpvi etc.
VII	l	h	v	h	a	a	g	r	l	p	fms o h i etc.
VIII	s	w	u	i	r	x	i	e	j	u	fshg w r s z b a a l
IX	u	h	w	h	v	a	g	u	l	c	jwoukdeb k q
X	y	w	x	h	y	h	b	a	l	g	bvp s w i w w j r r h
XI	w	q	r	e	x	b	i	e	n	h	m v y m h s i y m
XII	s	w	u	h	d	h	p	j	j	c	k x g m h l
XIII	g	q	y	q	r	v	o	t	q	q	spwr

Applying the calculation of repetitions, we admit the presence of *e* in columns 2 (=H), 4 (=H), 5 (=R), 6 (=H), 7 (=I), 9 (=L), and 10 (=C). We see, moreover, that the cipher-sign representing the letter *e* is the same for columns 2, 4, and 6, which permits us to conclude that these correspond to one and the same alphabet. Columns 3 and 5, as well as columns 8 and 9, likewise belong to the same respective alphabet; but since we are supposed to be ignorant of the key, it is only later that we shall be able to establish this. We therefore count provisionally, over the 10 columns, 8 different alphabets. Let us begin with No. IV:

1 2 3 4 5 6 7
 N° IV. U W V R R H I
 e e e

We have admitted that the cipher-signs RHI all three represent the letter *e*. No word in French can begin with two *es*; we therefore have here a word ending in *ée*. The number of cipher-signs preceding this ending immediately indicates that we are dealing with the word *armée*, preceded

by *I'*. Let us therefore enter six cipher-signs, of which two are given by the symmetry of position.¹¹

	1	2	3	4	5	6	7	8	9
Nº V.	U	H	S	H	A	H	K	S	V
	l	e	.	e	.	e	.	.	.

We have just seen that U = l. The word following *le* has an *e* in the second and fourth places. This is the case of the despatch we deciphered on page 169. It is therefore useless to recommence our reasoning, and we say at once that it is *général*.

The decipherment of this last word gives us 10 new cipher-signs, namely the five of the word *général*, S A K S V, plus five others supplied by the symmetry of position. The meeting of S in alphabets 8 and 9 shows at the same time that the two columns have been enciphered with the same alphabet.

	1	2	3	4	5	6	7	8	9
Nº VI.	Y	H	V	H	M	A	G	G	K
	.	e	r	e	.	v	.	.	.

Since M does not correspond to an *n* (=A), the first word can scarcely be anything but *ferez* or *serez*. It is impossible for the moment to decide between *f* and *s*, but whatever the verb, it must be followed by *vous*. Let us enter 15 new cipher-signs, of which four are obtained by decipherment and 11 by symmetry of position.

	1	2	3	4	5	6	7	8	9	10
Nº VII.	L	H	V	H	A	A	G	R	L	P
	.	e	r	e	n	v	o	.	e	.

We have here *le renvoi*, *je renvoie*, or *ne renvoyez*. Now the symmetry of position prevents the R in the eighth column from being an *i*, for we should then have in the third alphabet an R placed at an interval of one rank from S, and another R placed at an interval of 17 ranks from S in the eighth alphabet. It is therefore a *y*, and we translate: *ne renvoyez* [do not send back].

The decipherment has given us here only the meaning of three new cipher-signs; but the symmetry of position makes known to us 46 in the different alphabets taken together. Merely by entering L in the alphabet of the first column, where we still knew only U = l, we can determine there the place of 11 new cipher-signs. We establish at the same time that columns 3 and 5 are enciphered with the same alphabet.

The reader will experience no difficulty in deciphering the rest himself, especially if he continues with Nos. XI and XIII.

¹¹ The reader will not properly grasp what is said here about the application of the principle of symmetry of position unless he draws up on a sheet of paper a table with the normal alphabet at the head, leaving blank spaces for eight alphabets, (1, 2, 4, 6), 3, 5, 7, 8, 9, 10, spaces which he will fill in as we advance.

Let us conclude from what precedes that, whatever arrangement of the alphabets is adopted, correspondents are always bound to write each of their despatches with a different key.

e. System with variable key

On page 37 there was mention of systems with a variable key. A despatch written according to the indicated system is scarcely decipherable unless the decipherer can recover the stopping letter. This is not easy with a very short despatch; but when it has four or five lines, one immediately detects a certain regularity in the very irregularity of the returns of the letter. It is the only cipher-sign, for example, which is never met twice in succession. Now, once the stopping letter is found, decipherment is assured. It is enough to set in columns the different groups formed by the intervals from one stopping letter to the next, and to make the calculation which we know. Precious information is, moreover, supplied by the Arabic digit which indicates the place occupied by the stopping letter in the key.¹²

The decipherment can present some difficulties only when the alphabetical order of the letters has been irregularly interverted. Thus I was able to decipher, in less than two hours, the cryptograms composed according to this system which were given to me by the Commission of Military Telegraphy.

5. A triple-key cipher

It results from our attempts at decipherment that, of all the variable-basis cryptographic systems in use today, none presents serious guarantees of indecipherability. Certainly, it may happen that such and such a despatch, four or five lines long, enciphered with non-interverted alphabets and with a key having only five or six letters, resists the efforts of the best decipherer. Nothing is even easier for one who knows how to decipher than to compose indecipherable cryptograms with the most vulgar of systems. But if cryptography is ever to become, as one of our best generals has said, a powerful auxiliary of military tactics, the adopted system must be able to defy the most laborious investigations of decipherers even when it is handled by inexperienced hands.

If one were allowed for a moment to neglect the essentially practical side which every system of cryptography intended for the needs of the army must present, and to value only the desideratum which demands the exclusion of secrecy, one might adopt a triple-key system, and combine a transposition procedure with a variable-basis system of interversion. The Saint-Cyr system, combined with the method of transposition indicated on page 17, would allow the minimum of written notes, and would give a cryptogram, if not mathematically indecipherable, then at least one not admitting any calculation of probability.

The two keys would have to be represented by different words, such as an adjective and a substantive. The first word, composed of a small number of letters, would serve as the key for the work of interversion, and the second, of a larger number of letters, would give the formula of the transposition; for example: *chose problématique, affaire exceptionnelle* [problematic thing, exceptional affair].¹³

¹² In case of unforeseen difficulties one tries the 26 letters of the alphabet.

¹³ The simultaneous use of the two cryptographic procedures could not relieve correspondents of the need to change key for each despatch.

Let us encipher a despatch according to this system: *Vous ferez ce soir une attaque simulée* [You will make a simulated attack this evening], taking *sénat romain* as the key and using the table of Vigenère.

v o u s f e r e z c e s o i r u n e a t t a q u e s i m u l é e
Š E N A T S E N A T S E N A T S E N A T S E N A T S E N A T S E
n s h s y w v r z v w w b i k m r r a m l e d u x k m z u e w i

Romain gives the numerical formula 653124; thus we have:

A	1 2 3 4 5 6						B	6 5 3 1 2 4					
	1	2	3	4	5	6		6	5	3	1	2	4
1	n	s	h	s	y	w	6	d	c	a	w	i	b
2	v	r	z	v	w	w	5	e	u	m	x	k	z
3	b	i	k	m	r	r	3	r	r	k	b	i	m
4	a	m	l	e	d	u	1	w	y	h	n	s	s
5	x	k	m	z	u	e	2	w	w	z	v	r	v
6	w	i	a	b	c	d	4	u	d	l	a	m	e

= dcawibeumxkzrrkbimwyhnswwzvrvudlame.

But, I repeat, this procedure, however much it dispenses with the necessity of secrecy and guarantees almost complete indecipherability, leaves too much to be desired from the practical point of view for one to think of applying it to the service of war. It is therefore only as a curiosity that I have wished to indicate a system which dispenses with the necessity of secrecy and thus realises the principal desideratum of military cryptography.

C. Cipher dictionaries

It is difficult to obtain precise information about the different systems of cryptography which, since the last century, have been in use in the French army. It is known positively, however, that even before the Revolution the general staff had had tables drawn up for secret correspondence similar to those still used today by the Ministry of Foreign Affairs. These tables contained, alongside ready-made phrases, a certain number of common words; opposite them were one or two numbers to represent them. General Lewal has cited in the *Journal des Sciences Militaires* a fragment of a letter addressed, under the date 2 May 1815, by the Minister of War Davout to his colleague at Foreign Affairs, asking him for two ciphers of this kind for military correspondence. These ciphers, or ciphering tables, as they were formerly called, have become the cipher dictionary now used in the army.

As early as 1850, Brachet¹⁴ had thought of composing for the public an analogous dictionary, in which each word is invariably represented by a number of five figures. M. Sittler¹⁵ has since

¹⁴ *Dictionnaire chiffré. Nouveau système de correspondance occulte* (Paris, 1850).

¹⁵ *Dictionnaire abrégatif chiffré* (Paris, 1868).

devised a small vocabulary of about fifty sheets, each page containing 100 words represented by numbers from 00 to 99. The word one wishes to write is determined by adding to that number the page number. The pagination, which is left blank and must be entered by hand according to a conventional system, constitutes the secret of the method. The plan of the work is rather well conceived; it is all the more to be regretted that the author forgot to indicate the precautions to be taken to assure the secrecy of despatches in the event that the dictionary should fall into the enemy's hands.

MM. Brunswick¹⁶ and Gallian¹⁷ sought to fill this gap: the first by composing a dictionary in which the letters, with their various binary combinations, and several thousand words with their grammatical inflections, are represented by groups of figures from 0000 to 9999; the second by drawing up an analogous dictionary in which the groups of four figures are replaced by combinations of three letters.¹⁸

The method adopted by the two authors to thwart the calculations of decipherers is very ingenious. Here, in a few words, is M. Brunswick's procedure. First the order of the figures of each group or number is interverted, and this according to an agreed formula; then this interverted number is increased or diminished by another number. This latter number, together with the formula of interversion, constitutes the key of the combination. Let us take an example. Suppose that one wishes to write *avancez* [advance], and that the corresponding number given by the dictionary is 2143. This number may be interverted in 12 different ways: 2134, 4321, etc. Let us adopt 2134. If the conventional number to be added is 214, the final cipher will be $2134 + 214 = 2348$.

Since there is great latitude in the choice of the number to be added or subtracted, it is impossible, so long as one has not the dictionary, to establish the least calculation on the groups thus obtained. But once in possession of the dictionary, it is enough to know any two groups of a despatch to recover at once the key of the whole. Now, the circumstances in which a despatch was written being known, it is very easy to recognise, from the repetitions of certain groups, the presence of such and such a word. Thus the four following groups, 4213, 6555, 6555, 2140, placed at the beginning of a cryptogram, would probably contain the repeated pronoun *nous*, *vous*, or *ce*. It would indeed be difficult in French to compose the beginning of a sentence in

¹⁶ *Dictionnaire pour la correspondance télégraphique secrète*, by a secretary of legation (Paris, 1868).

¹⁷ *Dictionnaire télégraphique économique et secret*, by Mamert-Gallian (Paris, 1874).

¹⁸ The German dictionaries of Niethe (Berlin, 1877) and Walter (Winterthur, 1877), as well as Bolton's dictionary for English correspondence, rest upon the same principle. M. Louis, director of the *Journal des Postes*, has also published a *Dictionnaire pour la correspondance secrète* containing more than 20,000 words. The category of cipher dictionaries includes the system consisting in replacing the most important words of the correspondence by other words diverted from their usual meaning. This procedure has often been applied, but it can have a practical side only in exceptional circumstances. In the correspondence relating to the conspiracy organised in 1831 by the Bonapartist party, a document was found in Prince Louis-Napoléon's hand containing a list of the conventional words adopted by the conspirators to designate the persons and things whose names had to recur most often: Queen Hortense was designated by *M. Antoine*, Prince Louis-Napoléon by *Mme Charles*, England by *Mme Lirson*, the Bonapartists by *Mme Gock*, the army by *Mlle Amélie*, the police by *M. Pamberg*, etc. See the *Mémoires* of Gisquet, former Prefect of Police (1840), p. 351.

which a word other than *nous*, *vous*, or *ce* could be repeated in the second and third positions; for example: *Pouvez-vous vous défendre?* [Can you defend yourself?] *Devons-nous nous retirer?* [Must we withdraw?] *Est-ce ce soir?* [Is it this evening?]

It would take too long to enter into all the details which the decipherment of a despatch enciphered with a cipher dictionary may involve. I shall limit myself to a single example.

I suppose that certain indications authorise me to believe that, in an intercepted despatch, the group 9645 means *colonel*, and the group 7457 *régiment*. Here is how I should proceed to recover the transposition formula as well as the key number.

Let us admit that the dictionary gives for *colonel* and *régiment* the numbers 4913 and 2734. If I compare these two groups with the numbers 9645 and 7457 of the cipher text, I see, from the presence of the 9 and the 7, which have remained intact and are placed in the first rank, that the key is composed of only three figures, and that, in the permutation of the primitive number, the second figure has been carried to the first rank. Moreover, the figure 6 of the first number clearly indicates that the key involves an addition and not a subtraction.

The numbers 645 and 457 therefore represent the sum of the key number increased by the number produced by the permutation of 413 and 234. Now, if I successively subtract from the first two numbers the six permutations obtained, I shall have for the two operations a common difference, which will represent the conventional number, at the same time as it will make known what formula of permutation was adopted.

$645 - 413 = 232$	$457 - 234 = 223$
$645 - 431 = 214$	$457 - 243 = 214$
$645 - 143 = 502$	$457 - 423 = 034$
$645 - 134 = 511$	$457 - 432 = 025$
$645 - 341 = 304$	$457 - 324 = 133$
$645 - 314 = 331$	$457 - 342 = 115$

I say that 214 is the key number, and *badc* the formula of permutation.

The operation can give a common difference only in so far as the groups of the cipher text really correspond to the supposed words.

Of all known methods of cryptography, it is assuredly the cipher dictionaries, at least those based on a double principle of combination, like those of Brunswick, Gallian, and Niethe, which best guarantee the secrecy of correspondence. But beside this real advantage, they present such great inconveniences in their application to correspondence in wartime that one can only be astonished at the favour they have so far enjoyed among certain chiefs of the army.

The greatest reproach one can make against cipher dictionaries is that they require secrecy, and that by the very fact of their adoption they constitute an obstacle to the generalisation of cryptographic correspondence. This condition of secrecy may, moreover, cause the gravest embarrassments.

It is related that, on 8 January 1871, a cryptogram from the headquarters of the King of Prussia was handed to General von Werder, who could not decipher it immediately, since the dictionary containing the key to the secret correspondence was locked up in a valise placed on a distant carriage.

During the Russo-Turkish War, Selim Pasha, political under-chief of Mehemet Ali, absented himself for a few days in September 1877 and inadvertently took away the deciphering book.

During that time the commander-in-chief received a large number of enciphered despatches which it was impossible for him to read.

But, besides the fact that a printed vocabulary can be bought by the enemy, and that the adoption of a dictionary must necessarily restrict secret correspondence, there are the greatest inconveniences in making the meaning of a word or of an entire phrase depend upon the correct transcription of a number. Let a single figure in a group be faulty, let the telegraph or the copyist put, for example, a 3 where there should be a 5, and the meaning will be completely changed. Usually there is only a simple misreading, or an incomprehensible sentence; but the error may have more unfortunate consequences, and it has happened more than once that a badly transmitted or badly read figure has completely distorted the meaning of an order or an item of intelligence. If it is not rare to see the persons most accustomed to handling figures make, in a moment of excitement, errors in a simple addition, nothing is more common than to see telegraph clerks make mistakes in the transmission of cipher groups. This inconvenience, which was keenly felt during the war of 1870, when half the despatches sent by the military authority to the prefects contained illegible parts, was again experienced several times during our campaign in Tunisia. More than once it was impossible, at the Ministry of War, to decipher the despatches of the Army of Africa.

Not very long ago, the Italian ministry was singularly puzzled by the news transmitted to it by its ambassador at Saint Petersburg that Count Andr  ssy was expected in the Russian capital. It was simply an error of cipher which had caused the name of an embassy attach   to be taken for that of the celebrated statesman.

Cipher dictionaries are truly practical and safe only for chanceries, whose personnel, with their papers and their baggage, is inviolable in all civilised countries, and which have their despatches enciphered and deciphered by clerks trained in this kind of work and having every means of verifying at leisure the faithful transmission of correspondence.

IV. Cryptographs

If the few attempts at decipherment which precede have brought out the weak side of our principal systems of secret correspondence, they also allow us to appreciate all the difficulties presented by the elaboration of a cryptographic procedure realising the desideratum which I have indicated as the basis of every method of military cryptography, namely the non-necessity of secrecy.

We have seen that it is impossible to replace phrases and words by groups of letters or figures without thereby creating a dictionary which requires secrecy. We also know that transposition procedures guarantee indecipherability only on condition that they are based on some secret apparatus. It follows, and I insist on this point, that no method both safe and practical can be established except upon a conventional interversion of letters. It is true that, if the system is simple and rests upon some regular procedure or some systematic combination, it necessarily exposes itself to the calculations of decipherers. If, on the other hand, it is at all complicated and comprises many combinations, it requires secrecy, or else it ceases to be practical.

But I believe that the solution of the problem must be sought in the application of some mechanical apparatus based upon the principle of interversion, that is to say in the use of a cryptograph.

This idea, moreover, is not new.

The Lacedæmonian scytale; the tablet of Æneas, pierced with twenty-four holes representing the letters of the alphabet, through which one passed a string to indicate the order of succession of the letters of the secret missive; and Kessler's barrel were true cryptographs.

The first model of a cryptograph worthy of the name is found in Porta's *Traité des Chiffres*. It is the dial system of which I have already had occasion to speak.

Father Kircher had also devised a mechanical apparatus which he called the *Arca glottotactica*.¹⁹ It was a kind of movable catalogue in which words were arranged in a certain order corresponding to the several letters of the alphabet. Chappe's aerial telegraph, like the Morse telegraph, are also true cryptographs.

In recent times cryptographic apparatuses have been devised by MM. Moulleron, Vinay and Gaussin, Rondepierre, Wheatstone, Silas, and others.

M. Moulleron's system, of which a description is found in Du Moncel's *Exposé des applications de l'électricité*,²⁰ is a mechanism mounted on a desk, rather complicated and offering no practical advantage. The author does not appear to have made a very thorough study of double-key ciphers, for his bulky mechanism results only in giving us a cryptogram enciphered according to the table of Vigenère. It is easy to assure oneself of the perfect accuracy of what I advance by enciphering the example which the author gives, *La victoire est à nous* [Victory is ours], with our table on page 30. With the key *kzîrh*, one will obtain the same cryptogram as that given by M. Moulleron's apparatus with the key *paris*,²¹ namely:

l a v i c t o i r e e s t a n o u s
<u>k z î r h k z î r h k z î r h k z î</u>
v z d z j d n q i l o r b r n y t a
= v z d z j d n q i l o r b r n y t a

The cryptograph of MM. Vinay and Gaussin is a printing mechanism by means of which despatches are at once printed and enciphered. While more portable than the preceding one, it is still too bulky for its application to be possible in wartime. From the strictly cryptographic point of view, moreover, it has no value.²²

M. Rondepierre's cryptograph or phyrograph is based on the system of transposition set out on page 17. The vertical columns are represented by ivory rods on which are traced divisions intended to receive a letter. They are first transposed according to a numerical formula; then the despatch is written in pencil on the rods themselves. These are next restored to their original place, and the letters are copied in the new order in which they present themselves. The system is, from one point of view, rather practical, but it offers only relative security.²³

¹⁹ See Schott, *Schola steganographica*, p. 27.

²⁰ Third edition, vol. III, p. 529.

²¹ *Kzîrh* is simply *Paris* written with the reversed alphabet.

²² See Du Moncel, *loc. cit.*

²³ For particular reasons, the apparatus could not be put on sale, but specimens may be seen at M. Luard's, case-maker, 16 rue Dauphine.

I shall say nothing of the cryptograph of M. Silas, formerly attached to the French embassy in Vienna. Although it is a serious and very well-combined piece of work, it is, in my opinion, too complicated for the uses of war.

Of all the cryptographs invented in recent years, Wheatstone's seems to me to be, if not the safest, then at least the simplest. Since I have not been able to procure a specimen of the apparatus, I borrow its description from the Report of the Military Commission on the Universal Exposition of 1867.²⁴

"The very simple instrument proposed by M. Wheatstone for writing despatches in cipher is easy to use," says the rapporteur, "and *assures the most absolute secrecy* (?) for all those who do not possess the key of the system".

"Here is the principle according to which the fictitious alphabet is formed. One chooses any word as a key: *France, exposition, projectile*, etc. Let us suppose that one adopts the word *projectile*; one writes this word spacing the letters composing it, and below writes those letters of the alphabet which it does not contain, in a regular order, as follows:

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

"Taking up the letters in the order in which they occur in successive vertical columns, one obtains the following conventional alphabet:

pasrbuodvjfxegychztkwimlnq



"The letters of the conventional alphabet are written on a cardboard circle. This circle is applied concentrically upon a metal dial, which bears on its circumference an ordinary alphabet completed by the stopping sign +, to which one returns at the end of each word, but which does not exist in the cipher. Two hands, 1 and 2, move simultaneously on this double dial, but with different speeds and according to a law such that, in bringing the first back to the letter B, the second does not return to the same letter, such as V, indicated in the figure, but to another letter of the inner dial."

²⁴ Cf. Bontemps, *Les systèmes télégraphiques*, p. 257; Du Moncel, *Exposé des applications de l'électricité*, vol. III, p. 532. Wheatstone deciphered, in 1858, several very interesting letters of Charles I, written entirely in Arabic figures. See *Report of the Royal Commission on Historical Manuscripts*, 1870.

When one wishes to translate any letter into cipher language, one advances the large hand to the place occupied by that letter in the normal alphabet, and marks the letter on which the small hand has stopped in the conventional alphabet. The system thus involves two keys: the arrangement of the cryptographic alphabet and the point of departure.

Whatever Colonel Laussedat, author of the report I have just cited, may think, despatches written with Wheatstone's cryptograph are perfectly decipherable.

The system gives only a very limited number of different alphabets. The same alphabetical arrangement therefore returns after a determined number of stops. Suppose that this is after the 26th or 30th letter. I then have only to consider the cryptogram to be deciphered as written with a key of 26 or 30 alphabets, and to set it in columns by series of 26 or 30 cipher-signs, as we did for the despatch on page 168. But the greatest inconvenience presented by the apparatus is that it requires absolute secrecy; for once fallen into enemy hands, a few trials on the first letters of the despatch are enough to recover the initial point.

When several despatches written with the same key have been intercepted, it is no longer necessary to possess the apparatus to decipher them. One applies the procedure I indicated on page 177.

A new system of cryptograph has just been presented to the Commission of Military Telegraphy, and it appears to me to realise all the desiderata I set out at the beginning: complete indecipherability, simplicity, and non-necessity of secrecy. Considerations of high propriety prevent me from saying more about it for the moment.

Without wishing to prejudge the reception which this new attempt may find among competent judges, I wish, in concluding, to insist upon this point: that the value of a cryptographic system intended for the needs of war is in inverse ratio to the secrecy which its handling or its composition requires. It will therefore depend upon the Administration to secure the future of military cryptography by granting its support only to the invention which rests upon the principle that du Carlet, one of the masters of our art in the seventeenth century, had inscribed as the motto at the head of his method,²⁵ a principle which, moreover, sums up my whole thesis, namely that a cipher is good only in so far as it remains indecipherable to the very master who invented it: *Ars ipsi secreta magistro*.

Aug. Kerckhoffs
Doctor of Letters
Professor at the École des Hautes Études Commerciales
and at the École Arago

²⁵ *La Cryptographie, contenant une très subtile manière d'écrire secrètement*, composed by Master Jean Robert du Carlet, 1644.