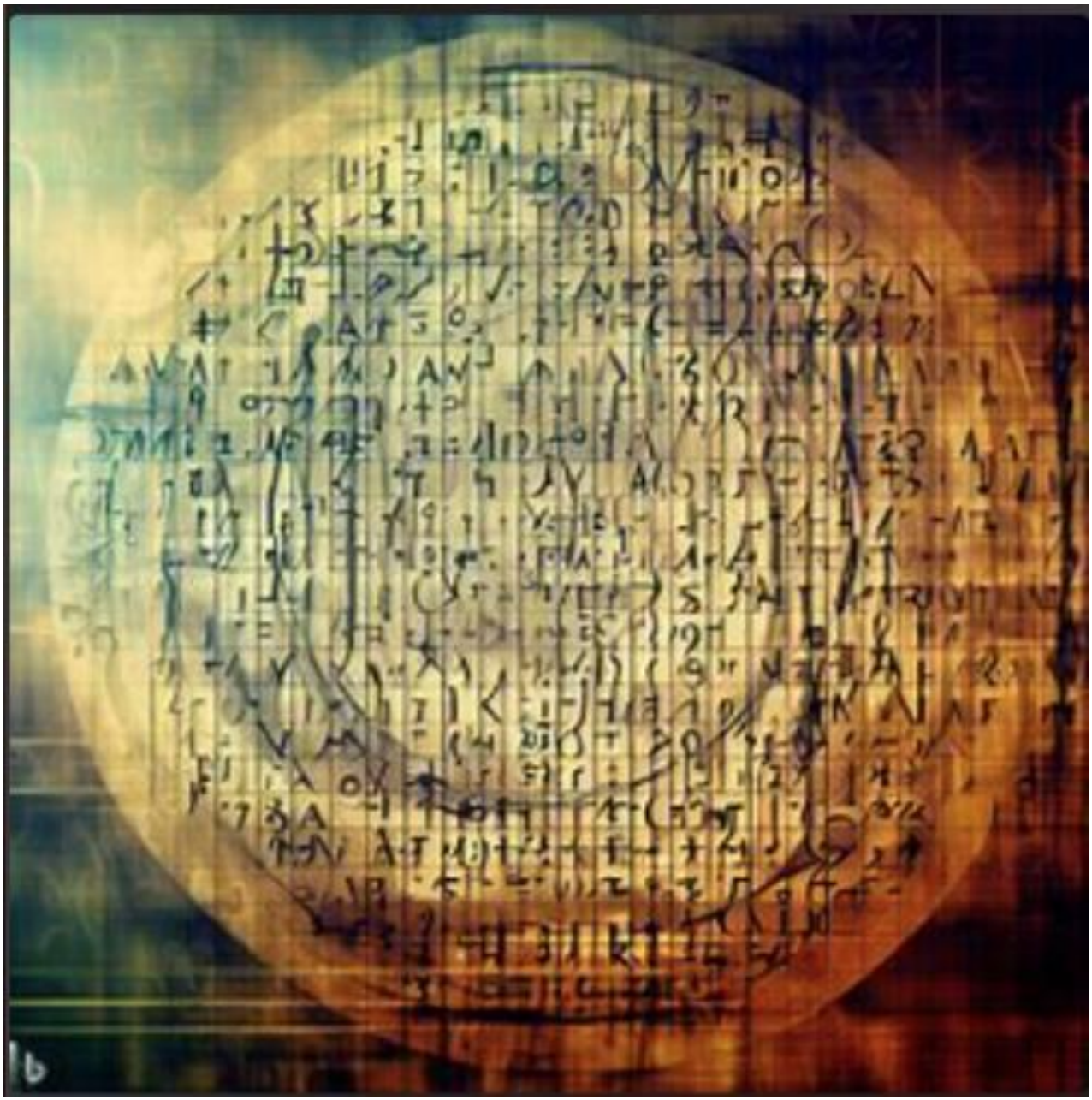


MILITARY CRYPTOGRAPHY

or

CIPHERS USED IN TIME OF WAR

With a New Process of

Decipherment Applicable to

Double-Key

Systems.

by

Auguste KERCKHOFFS

(1883)

Translated by “Warren Thomas McCready”

American Cryptogram Association

1964

PREFACE

A taste for cryptographic studies seems to be revealed among us since some years ago: cryptography is taught today in our military schools, popular magazines outline the elements of it, and new systems are proposed in the magazines to the Minister for War.

If the efforts made by different people to give our army a cipher both safe and practical are worthy of praise and testify to perfectly justified concern, it is no less true that, with hardly one or two exceptions, they show in their authors an incomplete knowledge of previous works as well as of different decrypting procedures.

I have therefore thought that it would be rendering a service to the persons who are interested in the future of military cryptography to summarize for them the works already published on the question, and to indicate to them the principles which must guide them in the creation or valuation of every cipher destined to war service.

The present work will be equally useful to officers who might be called upon to apply, at a given moment, some method of cryptographic correspondence: because it is only after being initiated into decrypting procedures that they will be able to avoid certain imprudences which jeopardize the security of the best systems.

Paris, 1883. Auguste Kerckhoffs

I.

CRYPTOGRAPHY IN THE ARMY.

A. Historical Review.

Cryptography, or the Art of ciphering, is a science as old as the world; confused at first with military telegraphy, it has been cultivated, since the greatest antiquity, by the Chinese,the Persians,the 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 Lacedemonians and the “tricks” invented or reported by Aeneas the Tactician (2), up to the famous drum of Kessler (3), men of war have invented many procedures for transmitting secret orders over a distance, or for protecting their instructions from investigation or surprise by the enemy.

We possess, however, only very incomplete facts about cryptographic processes, properly speaking, in use among the ancients; aside from the commentaries of Aeneas, one finds on the subject that occupies us, only isolated passages in Polybius (4), Plutarch (5), Dion Cassius (6), Suetonius (7), Aulus Gellius (8), Isidore (9), and Julius Africanus (10).

---

(1) Kerckhoff’s footnotes will be found at the end of this translation. See page 41.

During the Middle Ages, cryptography was scarcely cultivated except by monks and cabalists, and yet, where it did serve any practical purpose, the inventors sought to give a false scent as to the meaning of the communications transmitted, rather than to develop a more or less indecipherable method of correspondence; the fact is, that in those times of distrustful ignorance, it was just as dangerous to correspond in a mysterious or indecipherable language as to write in the clear the most compromising secrets.

Even in the 17th century, the simple fact of having corresponded in secret characters was still considered as an aggravating circumstance by the English courts; thus, in the famous suit against the Count of Somerset, for the crime of poisoning, Chancellor Bacon pointed out, as a grave charge against the accused noble, his habit of writing to his friends in cipher.

It was, then, steganography that our ancestors practised, artificiumsinesecretilatentissuspicionescribendi, rather than cryptography, in the meaning that we attach to this word today. One can read in the works of the Jesuit Schott (11) and in an old treatise on cryptography by the Duke of Brunswick (12), the thousand artifices that they successively invented. It is not until after the Renaissance that cryptography becomes a true art, arsoccultescribendi, as they used to day, and acquires a certain importance in the correspondence of princes with their ambassadors, and in the relations of great lords with their confidential agents.

It has been seen by his letters addressed to the Landgrave of Hesse, published some years ago by de Rommal, that Henry IV loved to make use of a cipher for his intimate correspondence.

It is equally well known that Henry IV, having intercepted some enciphered letters addressed by members of the League to the Spanish government, engaged the mathematician Viète to find the key to them. The latter succeeded, and the king was thus able, for almost two years, to keep an eye on his enemies' intrigues.

Under Richelieu, the art of deciphering secret writings was raised almost to the height of a State science; according to Field Marshal Beausobre (13), the minister of foreign affairs even had an academy where it was taught (14). Supported by the largesse of the rulers, encouraged by the absence of the political integrity that characterizes 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 blackchamber.

I have not, however, been able to find clear traces of the employment of cryptographic correspondence in the army in the 16th century; but it is known positively that, since the 17th century, orders are not sent to generals commanding frontiers or in enemy country, except by ciphers (15).

In the accounts of the wars of the first Empire, it is often a question of cryptographic communication; the generals had two ciphers for correspondence with each other and with the general staff: the "great cipher" and the "little" or "ordinary cipher." Baron Fain, the secretary of Napoleon I, reports that during the war with Russia the Emperor maintained correspondence in cipher (16). It is equally known that, during the war with Spain, a Spaniard found a means of stealing the cipher of Suchet, and used it to facilitate his countrymen's recapture of Mequinenza and Lérida.

Today, correspondence by secret ciphers is used in all the armies of Europe; but it is still not applied in a systematic fashion except in the offices of the chancelleries.

B. The Status of the Problem.

The Germans state as a principle that cryptographic correspondence should be employed most widely; the programs of their military schools prescribe not only instruction of officers in the composition and reading of secret dispatches, but also their introduction to all the theoretical principles of the art of decrypting.

Article 32 of the regulation of January 19, 1874 also states that military dispatches should whenever possible be enciphered.

Therefore, one might be astonished at first that, with rare exceptions, the use of enciphered correspondence should still be limited today, in the French army, to the commanders-in-chief. But a system of cryptography "of easy and safe use is a desideratum," says General Lewal, "that has always existed in our army" (17). The former commander of the War college adds, it is true, that there exist plenty of processes with that purpose, and that it would be sufficient to adopt one of them "that was portable and whose use was at the same time within the comprehension of everyone"; but would not certain deceptions suffered by the general staff in our recent campaign in Tunisia, as well as the methods taught and extolled in our high military schools, make one suppose that there exists a singular analogy between this "easy and safe system" and the philosophers' stone of the ancient alchemists?

The best generals are well aware, today, that it is indispensable that the different commanders of an army should have at their disposal a system of secret communication in order to correspond freely, not only among themselves and with their commander-in-chief, but also with their lieutenants; so, the tactician whom I have just quoted thinks that "it would be necessary to supply a cipher in time of peace as well as in war, to the generals, the regiment and service chiefs, all the column and post commanders." He even adds, and rightly, that it would be necessary, during peacetime, to train officers in the handling of this correspondence.

> "It is a matter to be foreseen and arranged before the war," he says; "once operations have begun, it is too late to dream about it. Besides, even in peace one needs, at any moment, to correspond secretly."

One reads in the Recherches historigues sur l'art militaire by General Bardin (18), that the use of ciphers came to an end in the conflagration of 1814, and that when Napoleon wanted to reunite with the main body of the army all the garrisons in foreign parts and several large French garrisons, it was in pure and clear French that Feltre and Berthier expedited his orders; also, few dispatches reached their destination, the enemy got hold of most of them. "Perhaps," says Bardin, "the fate of France and the face of Europe were brought about by the failure to use cryptography!"

But it is not enough to have a cipher for secret correspondence, it is also necessary that it present serious guarantees of indecipherability; now, this is the weak part of the majority of the systems invented up to the present time, and where this capital defect has been overcome, one finds himself in the presence of practical inconveniences just as serious.

Even in the Ministry for War they have not appeared very happy up tonow in the choice or composition of cipher. It is no secret to anyone that daring the

Turco-Russian war an enciphered dispatch was received, one Sunday, from one of the military attaches who were following the operations of the armies in combat, which could not be deciphered due to the absence of the head of the office in charge of cryptographic correspondence. The Minister decided that, since he did not know the key, he could only ask one of the officers on the staff to try to decipher it withoutakey: at the end of a few hours the cryptogram was solved! Luckily for the secrecy of the correspondence, the able decipherer was the son of the Minister himself (19).

It has been possible to see, in the obituary articles published in 1879 in the German journals, on the occasion of the death of Captain Max Hering, who discovered the cable of the Seine in 1870, what services were rendered to the besiegers by the absence of a safe system of secret correspondence between the army in Paris and the generals in the provinces.

I do not know what one is supposed to think of the assertions of the journalists from across the Rhine; but when I see competent judges declare that cryptography is a "powerful auxiliary of military tactics," and when I think that the destinies of a country, the fate of a city or army, might some time depend on the greater or lesser indecipherability of a cryptogram, I am stupefied to see our scholars and our professors teach and recommend for wartime use systems of which an ever so inexperienced decrypter would certainly find the key in less than an hour's time.

One can hardly explain this excess of confidence in certain ciphers except by the abandon into which cryptographic studies have been allowed to fall because of the suppression of black chambers and the security of the postal relations; it can also be believed that the wild assertions of certain authors, no less than the complete absence of any serious work on the art of decrypting secret writings, have contributed largely to giving currency to the most erroneous ideas about the value of our cryptographic systems.

Thus it is that General Lewal affirms categorically in his Etudes de guerre (20) that double key substitution ciphers are unreadable, or at least that they can only be decrypted with extraordinarydifficulty! And does not Voltaire himself say in an article devoted to cipher writing, and that at a time when the art of deciphering was at its peak, that "those who boast of deciphering a letter without knowing anything of the matter it concerns, and without having any preliminary help, are greater charlatans than those who would boast about understanding a language they had not learned." (21).

In the preface of Contr'espioh (22), in which "citizen" Dlandol made known, in 1793, the keys of some ciphers used the royalists in their correspondence with the émigrés, it is said that "destroying by publicity the most dangerous weapon of the secret enemies of the Republic in the circumstances existing at that time was not one of the least services to be rendered to the country." In my turn, I believe I am not acting like a bad citizen in exposing, to the light of day a state of affairs which, although it arises from a different point of view, is basically the same, and which our foreign enemies some day might only too well and too easily turn to account.

In the pages that follow, I shall examine first the desiderata for any system of military cryptography; then I shall say a few words about thedifferent ciphers; I shall next indicate a new process of decrypting applicable to the most usual systems

of double key substitutions; I shall end with some considerations on cipher dictionaries and cryptographic machines (23).

II.

DESIDERATA OF MILITARY CRYPTOGRAPHY.

It is necessary to distinguish well between a cipher system created for an occasional exchange of letters among a few individuals, and a cryptographic method destined to govern for an unlimited time the correspondence between different army chiefs. The latter, in fact, cannot, at well and at a given moment, modify their rules; besides, they must never keep upon their persons any object or writing that could reveal to the enemy the meaning of any secret dispatches that might fall into their hands.

A great number of ingenious contrivances can answer the purpose that one wishes to achieve in the first case; in the second, a system is necessary which fulfills certain exceptional conditions, conditions that I shall summarize under the following six headings:

1. The system must be practically, if not mathematically, indecipherable.
2. It is necessary that it not demand secrecy, and that it may without inconvenience fall into enemy hands.
3. The key must be able to be communicated and remembered without the help of written notes, and to be 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 and operation must not require the presence of several persons.
6. Finally, it is necessary, in view of the circumstances governing its operation, that the system be easy to use, not demanding intense mental effort nor the knowledge of a long series of rules to be observed.

Everyone agrees that the last three requirements are justified, but there is no such agreement on the first three.

Thus it is that some responsible persons claim that absolute indecipherability of the cipher could not be considered as a sinequanon condition of its admission into the service of the army; that enciphered instructions sent in time of war have only a momentary importance, and do not require secrecy beyond three or four hours following the moment at which they were given; that it therefore matters little that the meaning of a secret dispatch should be known to the enemy a few hours after its interception; that it is sufficient, in a word, that the system be composed in such a way that the decryptment of a message will demand at least three or four hours of work. They add, moreover, that the possibility of changing the key at will takes away all importance from the defect of non-indecipherability.

---

(23) Bibliographical information is given only for the benefit of those who might like to probe more deeply into the question; it will be found all the more useful since, with two or three exceptions, the works cited are all to be found in the Bibliotheque Nationale.

This argument, at first sight, seems quite just; at bottom, I believe it to be false.

In my opinion, it ignores the fact that the secret matter in communications sent over a distance very often remains important beyond the day on which they were transmitted; without enumerating all the contingencies that may arise, it well suffice for me to cite the case of the commander of a besieged city who sends information to the army that is supposed to relieve it. Besides, once an intercepted message has been decrypted, every new dispatch, written with the same key and suffering the same fate, can be read instantly. It will happen, consequently, that over a more or less long time, dispatches will be sent off in all directions, and their decryptment will be found, in a way, to have been done beforehand: unless we admit that in an army corps all enciphered instructions come from, or at least pass through the hands of, one single person, which would be to reduce secret correspondence to a singularly modest role.

The possibility of being able to change the key at will is certainly an essential condition of any system of cryptography, but it is a deceptive advantage, and one would be wrong to count on the practical application of it during the thousand and one turns of fortune in a long campaign.

In regard to the necessity for secrecy, which, in my opinion, constitutes the principal defeat of all our systems of cryptography, I wish to point out that it restricts in some way the use of enciphered correspondence to only commanders in chief.And here I understand by secrecy, not the key properly so-called, but that which constitutes the material part of the system: tableaus, code books, or whatever mechanical apparatus may be necessary for its application. In fact, it is not necessary to raise imaginary phantoms and to cast suspicion on. the incorruptibility of employees or subordinate agents, in order to understand that, if a system requiring secrecy were found in the hands of too large a number of individuals, it could be jeopardized in any engagement in which one or another of them took part. From this point of view alone, there would be reason to condemn the employment of code books, which are in use today in the army.

Someone may perhaps object to my including the second desideratum, since it is hardly possible to establish a completely indecipherable system. It must be understood: I know very well that to try to find, under these conditions, a mathematically indecipherable system is something mathematically impossible, but I affirm, and not without good reasons, that while bringing about the realization of the different desiderata that I have enumerated above, it is perfectly possible to compose systems that are, if not mathematically, at least practically indecipherable.

It seems that they are giving serious consideration, in the Ministry for War, to the replacement of the cipher dictionary by some other more practical system. Well, then! If the Administration wishes to turn to account all the services that a well constructed system, of cryptographic correspondence can render, it must absolutely renounce secret methods and establish as a policy that it will only accept a process that can be taught in bread daylight in our military schools, that our students will be free to communicate to anyone they please, and that our neighbors can even copy and adopt if it seems suitable to them. I will say more: it will only be when our officers havestudied the principles of cryptography and learned the art of decrypting, that they will be in a position to avoid the numerous blunders that

endanger the key of the best ciphers, and to which the ordinary ones are necessarily exposed; only then will that article of the regulation of 19 November 1874, which I mentioned above, be able to receive a practical and really satisfactory application.

III.

THE DIFFERENT METHODS OF CRYPTOGRAPHY.

The different systems of secret writing can be divided into three principal methods:

1. The method that is limited to a simple transposition of the plaintext.
2. That which has the composition of the cipher based on a change in the alphabetical order of letters.
3. That which represents syllables, words, or even whole sentences by means of numbers or groups of letters.(1).

A. Transposition Method.

The systems based on a transposition of letters are very ancient;they permit numerous variations and have served as the basis of some mechanical devices, such as the grilles, which still enjoy the favor of the public today (2).

Here is an example of elementary transposition: The letters of the message are first transcribed in their natural order on a certain number of lines containing a certain number of spaces, then they are recopied in an order agreed upon (3); it is the number representing the second arrangement that constitutes the key of the cipher(4).

“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	a	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	c	s	r	e	e	b	a	e

= nsuqteeuatamlrueuaiaeleanieumiamdihrtqnetauaufdcsreebae.

If the decrypter is in doubt about the process that has been adopted, and he

sees immediately the letter E, which in this case appears the most frequently, the decipherment is only a matter of trial and error. It is sufficient to count first of all the number of letters in the cryptogram and to break them down into two factors (55 = 5 x 11); the one represents the number of horizontal lines and the other that of the vertical columns. The mere presence of a q or an x, the first always being followed and the other generally preceded by u, betrays the secret of the key.

On the occasion of the last trials of the Nihilists, the Russian journals made known the secret cipher used by the accused: it is a system of double transposition; the letters, after having been once transposed by vertical columns, are transposed again by horizontal lines. The same word serves as a key for the two transpositions (5); for this purpose, it is transformed into a numerical formula, by placing an Arabic number at each letter, using them in such a way that the value of the number corresponds to the position of the letters in the alphabet (6).

Here is the procedure applied to the word Schuvalow:

a	c	h	l	o	s	u	v	w	=	s	c	h	u	v	a	l	o	w
1	2	3	4	5	6	7	8	9		6	2	3	7	8	1	4	5	9

If it were now a question of transposing a sentence, like this one: “Vous êtes invité à vous trouver ce soir, à onze heures précises, au local habituel de nos réunions,” one would proceed at first as in the preceding case, then one would perform the same operation with the horizontal lines.

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	e	h	e	u	r	e	a	p	r
6	e	c	i	s	e	s	a	u	l
7	o	c	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

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

= sciaueselavivonteuvtrersoucacabiolhtnelosuder, etc.

However complicated this transposition might appear to us, the decryptment of a cryptogram written in this system could never present insurmountabledifficulties in the languages in which certain letters can appear

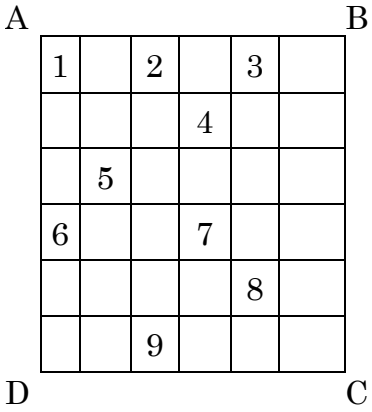
only in particular combinations, such as the Frenchq andx. The Russian decrypters also seem to have brought their work to a successful conclusion in a relatively short time.

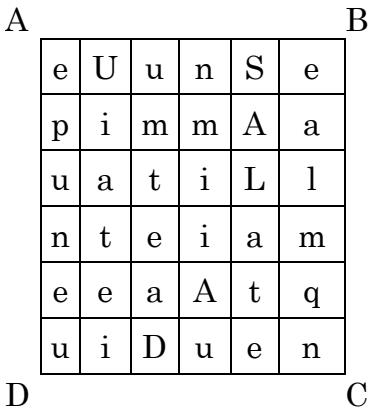
If one adopts a more complicated system, it ceases to be practical without becoming thereby much more difficult to decrypt.

I have said that the grille (7) is based upon the principle of the transposition of letters; 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 (8).

The figure below represents an ancient model: it is a square metal plate with 36 divisions, of which the 9 numbered ones have been cut out.

Let's suppose that you wish to write the sentence quoted in the first example, minus the last three words: you place the plate on a sheet of paper, after first having traced on it a square of the same dimensions, and you write, in the places left open, the first nine letters of the message; you then turn the instrument from right to left, so that side BC takes the place of side AB; you write the nine letters that follow, and you turn the plate again to continue the same operation up to the 36th letter. You will have the following cryptogram, in which, for greater clarity, I have indicated with capitals the initial letters of the words:





= euunserimmaauatillnteiameeaatquiduen.

The grille of Colonel Fleissner (neuePatronen-Geheimschrift) is the fruit of long and patient research, and it has infinite variations; but, besides some practical inconveniences, it cannot, in my opinion, be suitable for use in war for the reason that it requires utmost secrecy.

B. Substitution Method.

In the systems that belong to the substitution method, it is necessary to distinguish simple substitution—that is, where each letter of the alphabet is represented throughout a cryptogram by the same character or sign—from multiple substitution, in which the alphabet is changed for each word or for each letter. The first is commonly called simple key, and the second system double key.

The simple key systems do not present any security; only the double key systems permit some more or less indecipherable contrivances.

1. Simple Key Systems.

From the point of view of form, simple key systems can be infinitely varied; one can not only arrange the normal alphabet in an almost incalculable number of different ways, but one can also replace the alphabetical characters by numbers, by algebraic, astronomical, or arbitrary signs, by groups of letters or numbers, and even by words or whole sentences. Basically, however, and for the decrypter, all these combinations constitute one and the same system, giving way to one single process of decryptment.

The simplest and at the same time most practical system is that which consists of changing the value of the letters of the alphabet according to an agreed upon key.

We have seen above, how a key word is changed into a key number; the same procedure can be followed to establish the order of succession of the letters of the new alphabet. Let Champigny be the key; the numerical formula corresponding to it is 241685379. If we wanted to arrange the cryptographic alphabet according to this number, we would obtain:

2 4 1 6 8 5 3 7 9

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

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

"Tournez les positions de l'ennemi" would give with this alphbet the following cryptogram:

VNSRQHY JHT LNTIVINQT FH JHQQHOI.

This system is two thousand years old; the emperor Augustus was already using it to write to his children (9); and according to Suetonius and Aulus Gellius, Caesar himself had not known of anything better to use, in order to correspond secretly with his friends, than an alphabet in which each letter was advanced four positions (10). The generic term Julius Caesar method is also often used to designate any system that is based on a simple substitution of the letters of the alphabet (11).

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

The Bibliothèque Nationals possesses two volumes of letters in cipher, found in Offenbourg by Moreau in the baggage-wagons of the Austrian general Klinglin, in charge of the secret correspondence service; in these letters, which were very compromising for the royalist party of that time, each letter of plaintext is represented by a two-figure number, while the separation of words is indicated by a zero. It is probable that the general was stronger in military tactics than in cryptography, because he evidently was ignorant of the very elementary principle that I have just pointed out; he thought it was enough to divide some words arbitrarily to throw decrypters off the scent.

Here is, then, the first sentence of one of these letters, dated 31 December 1795:

899952450 44520 455625365211250 si ce n'est la 3152891499 14 254452

44520 231109425946752459499564 5 44118934 5294 445234 114544520.

89 99 52 45 0 44 52 0 45 56 25 36 52 11 25 0 si ce n'est la 31 52 89
r i e n d e n o u v e a u c e r-

14 99 14 25 44 52 44 52 0 23 11 0 94 25 94 67 52 45 94 99 56 45
t i t u d e d e l a s u s p e n s i o n

44 11 89 34 52 94 44 52 34 11 45 44 52 0
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.

I cannot enumerate here all the simple key systems; I must limit myself to citing among the ancient authors the names of Tritheim (12), Porta (13), Blaise de Vigenère (14), Bacon (15), Hermann (16), and Mirabeau (17), who have created more or less ingenious alphabets, of which the description can be found in the special treatises (18). In any case, these inventions can have for us only a purely archeological interest; they are not practical, and all of them, except Hermann's, can be decrypted with equal facility.

2. Decryptment of Simple Key Systems.

Whatever the system used may be, whether it is a simple key or double key, the decryptment of a message of which one does not have the key admits of two quite distinct operations: a calculation of probability and a job of tentative assumptions.

The calculation of probability rests upon a quality peculiar to all languages, that is, that certain letters occur more frequently than others, and that the ratio of these occurrences is expressed by a fairly constant average for the 9 to .12 principal letters of the alphabet. Thus, in the French, English, and German languages, the letter E is the most frequently repeated; in Spanish it is the 0, in Russian the A, and in Italian E and I; in French, there is on the average one E for every five letters.

Thus, if one had to cryptographize (19) a dispatch with the alphabet below, based on the keyword Orleans, one would know in advance that it is the cipher letter A that will recur most often.

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

"Votre dépéche a été déchiffrée"will give, in fact, a cryptogram in which, out of 26 letters, the A is repeated 9 times:

ZSRPA BATACLA E ARA BACLMDDPAA

A calculation which I have made on some circulars from the Ministry for war has given me an average of 560 consonants and 440 vowels out of 1,000 letters, as follows:

E-185	N-71	D-42	F-14	B	-5
S- 88	T-65	M-36	Q-10	H	-4
R- 78	0-57	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 and W	-0

When one works on messages of one or two lines, one cannot count on anything but the E, and it may still happen sometimes that the letter which occurs most frequently is an S, an R or an I (20).

Besides the repetition of letters taken singly, various binary or ternary combinations are to be noted, and a multitude of other particulars, which it would be too long to enumerate here.

So, for the binary combinations of E, one finds most often es and en; then come, in the order of their importance, se, te, et, de, me, el, em, le.

I do not speak of the structure of words themselves, since a system that preserved in the ciphertext the word divisions of the plaintext would not present a shadow of security.

As a general rule, it is enough, in the decrypting of a message, to know the character which represents the letter E in order to be certain of finding, whether by calculation or by tentative assumptions, the meaning of all the others. One could even state as a principle that the value of a cipher is measured by the guarantees it offers against the discovery of the sign corresponding to this letter (21).

Since my purpose is not so much to teach the reader how to decrypt as to indicate to him the course followed by decrypters, I shall content myself with showing him by a very elementary example how one proceeds in the decryptment of a text of which one does not have the key.

Suppose the cryptogram is: SP Z BOB CSRRSQSPB CB PSXB JBJ PBOOXBJ.

1 2 3 4 5 6 7 8

SP Z BOB CSRRSQSPB CB PSXB JBJ PBOOXBJ

The character occurring most often is B; I say that it corresponds to the letter E, and I make the following argument:

No. 3. BOB: concerning three-letter words beginning and ending with e, there is only été.

No, 2. Z: the French language has only two one-letter words, a and y; étécannot be preceded by y, therefore Z = a.

No. 7. JBJ: this group can only be ses; it is the only three-letter word having an e in the middle, preceded and followed by the same letter.

No. 8. PBOOXBJ: we already know five letters of this group, -ett-es; the only word that fits this pattern is lettres.

No. 1. SP: the only two-letter words that can go with aétéare ça, il,on; now P is an l, therefore SP = il.

No. 6. PSXB = lire.

No. 4. CSRRSQSPB: five characters are already known to us: -i--i-ile. The termination ile indicates an adjective; among adjectives in ile with nine letters and having two i's in the body of the word, the rhyming dictionary gives only difficile.

No. 5. CB = de.

We have, then, Ilaétédifficiledelireseslettres.

The longer a cryptogram is, the easier it is to decrypt; as a general rule, one line is sufficient.

General Lewal says in his Etudes de guerre (22) that a simple key cipher sufficiently guarantees secrecy for ordinary needs and "for matters without major importance".

I do not know what is supposed to be understood by "matters without major importance", but the reader can be sure from the cryptogram I have just analyzed, that a dispatch written in this way, when it is two or three lines long and one has not had recourse to any help, can sometimes be deciphered at sight.

The simple key cipher presents some slight guarantees only under the following three conditions:

1. Word divisions must not be indicated in the ciphertext.
2. Double letters must be suppressed.
3. Neither capitals, accent marks nor punctuation must be used.

To avoid errors in transcription it is even indispensable to break up the cryptograms into groups of four or five characters (23). Our last message should have been cryptographized as follows: ilaétédificiledelireses letres, = SPZBO BCSRS QSPBC BPSXB JBJPB QXBJ.

3. Double Key Systems.

We have seen that double key ciphers are those in which the alphabet is changed for each letter.

Many double key systems have been invented, but there are scarcely three or four that are really practical and that are still in honor in our days; however different in form, they are basically identical, and belong to the type explained at the end of the 16th century by Blaise de Vigenère. For almost three centuries they have served as secret ciphers to the majority of the small courts of Germany and Italy, and today they are still considered indecipherable in the eyes of people who are not up to date in the processes of decryptment.

Since every method of cryptographic writing destined to the needs of the army must be able to be sent by telegraph, we need concern ourselves only with systems that are based solely on the employment of letters or numbers, and that excludes any kind requiring the simultaneous use of both (24).

a. Porta System.

The invention of the first double key literal (25) system goes back, as I have said above, to the physician Porta (26); although he himself was quite far from perceiving all the importance of the introduction of a key properly so-called into the art of cipher writing, we must not consider him any the less as the founder of cryptography.

Porta employs eleven different alphabets, which he designates, as can be seen in the figure below, by the letters AB, CD, etc., or simply by A, C, or B, D.

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

If one wishes to write with one or another of these alphabets, one chooses, to represent the letters of the plaintext, those which are opposite them in the tableau. Thus, if one cryptographizes with alphabet D or C, one represents a by z, and vice versa, z by a; b by n and n by b, and so on. But in order to foil investigators' calculations, Porta, as a man who knows how to decrypt, recommends writing each letter with a different alphabet; moreover, in order not to oblige the correspondents to take the eleven alphabets consecutively, which would very quickly betray the secret, he proposes that only four, five, or six be used, and that a word be agreed upon whose letters will indicate the alphabets that it will be necessary to choose successively (27). This word constitutes the key of the cryptogram; it is written under the text to be enciphered, and it is repeated as many times as necessary.

Here is an example with the key roi:

v o t r e d e p e c h e e s t d e c h i f f r e e
R O I R O I R O I R O I R O I R O I R O I R O I R
d h ma y z x i n t o n x a mv y y y n p o y mn x

= dhmayzxintonxamvyynpoymnx

Porta's invention, we have seen, opens, in a way, a new era in the history of cryptography, but it presents two great inconveniences which caused it to be abandoned some time ago: first of all, the small number of its alphabets, and secondly, the necessity of representing the same alphabet by two different letters. As a consequence of this last circumstance, a word of four letters, such as poli, gives a key that actually calls for only two alphabets.

b. Square cipher or Vigenère tableau.

The square cipher, also called the indecipherable cipher or cipher par excellence, is nothing else but the Porta system, simplified by Blaise de Vigenere, who published it, just as it is in use today, in his Traité des chiffres(28). The square cipher enjoyed an extraordinary favor in the chancelleries of the 18th century and, what brings one to believe that scarcely a better one was found afterwards, is the fact that it was still used, after 1870, in the Ministry for War.

Dlandol made it known to the public, at the time of the Revolution, in a work that I have already cited. In chapter VI, he says that "this cipher has been called the cipher par excellence, because it contains the greatest number of advantages that one could desire for secret correspondence.It would contain them all without exception," he adds, "if it were not a bit slow in operation; but it quite makes up for this inconvenience by its incredible security. This security is such that the whole universe would not learn it if one did not know the keyword agreed upon

among the correspondents; one could show his message to everyone, without a single person being able to read it." Verily, citizen Dlandol was a better patriot than decrypted

The arrangement of the Vigenère tableau differs from that of the Porta tableau in that the alphabet is placed in it in a square number, and one obtains, thus, as many different alphabets as there are letters in the alphabet (29).

	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	l	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	in	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	a	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	a	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

As for the operation of this tableau, one proceeds as for the Porta system; it is only necessary to remark that the top horizontal alphabet represents the normal alphabet, and that the other 26 that follow are the cipher alphabets.

Let's say that "Détruisez le tunnel" is to be cryptographized with the three alphabets corresponding to the word BAC; we will have:

det rui sez let unn el
BAC BAC BAG BAC BAC BA
eev suk teb mev vnp fl

= eevsuktebmevvnpf1

Nothing is easier than to read a cryptogram written in this manner when one knows the key: the ciphertext is transcribed in groups equal to the number of the chosen alphabets; the key is written underneath, and the first operation is done in reverse.

Suppose that EYFDAOLRAKHHGMHNCFMK is to be deciphered. TUNIS being the key, we will find:

EYFDA	OLRAK	HHGMH	NCFMK
TUNIS	TUNIS	TUNIS	TUNIS
lesvi	vress	ontep	uises

= Les vivres sont épuisés.

As we shall see further on, messages written with the Vigenére tableau are very easily decrypted; it is only in exceptional cases that the system can provide some security.

c. The Saint Cyr System.

This system, which has been in use for a long time, is nothing but a disguised form of the Vigenère tableau; for lack of a proper name, I have designated it under the name of the school where it is taught and recommended today.

Here is the description of it, taken from the Cours d'Art militaireof the year 1880-81 as it was autographed by the students of the first division (30) :

"The instrument," it says there, "is composed of a fixed alphabet, underneath which slides a movable double alphabet; two strips of square-ruled paper suffice for it (31).

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	. . .

Any word of from 3 to 5 letters is taken to form the key (32). Let's choose the word BAC and take the following message: "Détruisez le tunnel."

Since the key has 3 letters, the sentence to be enciphered is likewise divided into groups of 3 letters, as follows: dét-rui-sez-let-unn-el; the first letters of each group are enciphered first, then the second ones, and finally the third.

To encipher the first letters, the first letter of the key, B, represented on the movable alphabet, is placed under the letter A of the fixed alphabet (see the figure above); and, reading the first letter of each of the groups in the message on the upper alphabet, the letter corresponding to it on the lower alphabet is written down.

Then the second letters of the groups are taken. To encipher them, the second letter of the key, A, is placed under the A of the fixed alphabet, and the same operation as we have seen is done. The same is done for thethird letters. The

message is then found to be as follows:

det rui sez let unn el
BAC BAG BAG BAC BAC BA
eev suk teb mev vnp fl

= eevsuktebmevvnpfl

In admitting, the text adds, that the instrument might be lost or captured, one is saying nothing; it is necessary to know the key."

It is easy to be assured that this process is only an abridgment of the preceding one, by comparing in the two systems the three alphabets that correspond to the key BAC.

Square Cipher

	A B C D E F G H I J K L MN O P Q K 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

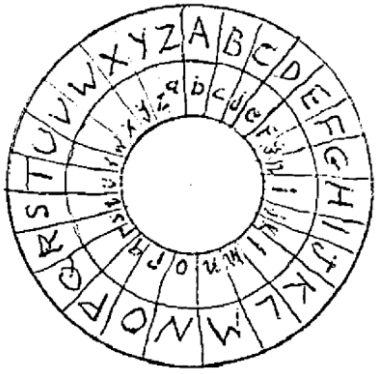
St. Cyr System

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 . . .
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 . . .
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 . . .

Since the same ciphertext is obtained with both systems, neither the correspondent nor the décrypter have to wonder with which of the two the message was written (33).

The only advantage that this process presents over the preceding is that, in case of loss, the instrument can be remade in two or three minutes' time. From the cryptographic point of view, it acquires a real value only if the order of the letters in the movable alphabet is reversed.

It is said in the Gours d'Art militairethat the instrument could be made in a way that would make it more portable, by forming it by means of two concentric circles, of which one would be movable and would turn around on its axis; this one would correspond to the double alphabet.



This arrangement, which is represented in the preceding figure, was invented as early as 1563, by Porta (34), and has received numerous applications since, such as the cryptographic device of Wheatstone and the boxes of moving dials that were sold at the time of the war with Italy. All these devices, of which some are shown in recent works on telegraphy as marvelous inventions, are really nothing but a simple Vigenère tableau.

d. Beaufort System.

A quite ingenious modification was made to the square cipher by the English admiral Francis Beaufort (1857). Although it appears at first sight to affect only the handling of the tableau, it alters the cryptographic text enough to give it, in the eyes of the uninitiated, a veritable air of indecipherability. Here, first of all, is the Beaufort tableau:

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	g
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	g	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
q	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	5	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	5	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	a	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	a	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	a	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	q	d	e	f	g	h	l	j	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z	a

"Emparez-vous des hauteurs," enciphered with the key BAC, will give the following cryptogram:

emp	are	zvo	usd	esh	aut	eur	s
BAC	BAC	BAC	BAC	BAC	BAC	BAC	B
xon	bjy	cfo	hiz	xiv	bgj	xgl	j

= xonbjycfohizxivbgjxglj.

Let's see now how one proceeds. Start at the letter e in the first horizontal alphabet, descend in a straight line as far as the b; there, make a half-turn either to the left or to the right, go to the end of the row, and the letter x, which you will find there, is the cryptographic sign needed; and likewise with the other letters.

English decrypters, whom the Beaufort system so amazed, certainly did not doubt that one could obtain the same result with the Vigenère or St. Cyr system simply by turning the normal alphabet around (35).

It is easy to be sure of it by inspection of the two figures that follow:

Square cipher.

	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

St. Cyr System.

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 . . .
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 . . .
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 . . .

The result would still be the same if, instead of reversing the order of the letters in the normal alphabet, one put in the body of the square the alphabet azyxwvutsrqponmlkjihgfedcb as in the following example:

	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. Gronsfeld System.

This system differs from the preceding two only in the fact that the work can be done in the head, instead of requiring the presence of a tableau or some such device.

Here is how M. Bontemps, inspector of telegraph lines, expresses himself on this subject (36):

> "Let's suppose that one has chosen as key any number at all; under the sentence that he wishes to transmit he writes it as many times as it can be contained there, by establishing the correspondence between the letters and the successive numbers. One takes for the letter to be sent that which is placed in the alphabet at a distance from the real one equal to the number placed underneath, and one

> constructs thus a tangle of which it is impossible to discover the key, even if one were endowed with the perspicacity that Edgar Poe supposes in his hero in the story of the Gold Bug, or with the intelligence of the agents employed to decipher the correspondence of the Duchess of Berry in 1832, according to the account that is found in the memoirs of M. Gisquet."

With all due deference to the author whom I have just quoted, the system of the Count of Gronsfeld is not much more difficult to decrypt than a modest simple-key cipher; it is, moreover, only a disguised form of the Vigenère tableau (37).

Let us take our example, and again encipher "Détruisez le tunnel", with the key 102: each letter of the plaintext will be represented respectively by another, one, zero or two positions further on:

det	rui	sez	let	unn	el
102	102	102	102	102	10
eev	suk	teb	mev	vnp	fl

= eevsuktebmevvnpfl.

If a key composed exclusively of numbers lower than 10 is chosen, this system fulfills perfectly our third desideratum, and even offers, if the numbers are very low, certain practical advantages; but these advantages lose much of their value in view of the facilities that this arrangement furnished to the decrypters' investigations.

f. Variable key system.

We shall see further on that the decryptment of double key systems is based mainly on the knowledge of the number of letters composing the key. People have thought up various combinations to prevent decrypters from making the calculation; one of the best ones is due to a member of the military telegraph commission. He proposes to interrupt, at irregular intervals, the order of succession of the alphabets, such as the key indicates it, by returning suddenly to the initial letter, or first alphabet. So, if the key is Epaminondas, instead of repeating it regularly in series of eleven letters, he cuts it off arbitrarily, and writes: epa-epaminondas-epaminondas- epami- epaminon- etc.

The point of interruption is indicated by one of the letters of the key, which is inserted at the desired places in the ciphertext. Here is an example, in which I have put as an indicator letter the second one of the key, that is, P:

Nous	–	partons	–	de	–	main		
EPAM		EPAMINO		EP		EPAM		
. . . .	P	. . . . .	P	. .	P	. . . .		

In order to avoid all confusion as to the meaning attributed to the indicator letter, this is replaced in the cryptographic text by an Arabic number corresponding to the place that it occupies in the keyword; thus, in the example below, where the

P is the second letter of the key, it will be replaced by a 2 in all the places where it is not supposed to play the role of indicator letter.

With the square cipher we would have the following cryptograms

rduePt2rfwagPhtPq2az.

To prevent the decrypter from making an entry on the first letters of the message, it is made to begin with some nulls, care being taken to indicate by the indicator letter the point at which the true text begins. Our cryptogram could then be finally written:

xmoprduept2rfwagphtpq2az.

4. Decipherment of Double Key Systems.

Except for a small work, written in 1863 by the German major Kasiski(38), there has not been published, to my knowledge, any essay on the decryptment of double key secret writings. All that is found in Porta, Cospi, Breithaupt, 'S Gravezande, Thickenesse, Klüber, Lacroix, Vesin, Joliet and others, applies only to simple key systems, and still these authors have scarcely touched on anything except deciphering cryptograms in which word divisions are clearly indicated(39).

A passage in the Interpretation des Chiffres by Cospi, the secretary of the Grand Duke of Tuscany, would tend to make one believe that decrypters have avoided at all times revealing to laymen their decrypting procedures. One reads on page 3: "There are two kinds of ciphers, the ones simple and the others compound; leaving aside these latter as almostimpossibletodecrypt, we shall speak only of the first ones, which are the simple"(40). Now, it is hardly probable that a man of Cospi's talent did not know how to decrypt the systems that Porta and Vigenère had published a half-century earlier.

Major Kasiski has based his system of decryptment almost exclusively on the determination of the letters of the keyword. While acknowledging the author's competence, I cannot help but conclude that that is a singularly complicated method which, in a great number of cases, must give a negative result. I am going to indicate a process which seems to me not only more certain, but still more simple and more methodical. Without wishing to present a complete work, for which I do not see too much need, I shall try nevertheless to develop the question enough so that the reader who wishes to practice the "art of deciphering" will be able to discover by himself and without difficulty all the little details of which a complete explanation would require at least fifty pages; fabricandofitfaber, one becomes a decrypter by decrypting.

I said further back, that, in every substitution system, the decryptment of a cryptogram of which one does not have the key requires a calculation of probability and a job of tentative assumptions» In the simple key systems, in which one makes use of only one alphabet, calculation and assumption are necessarily limited to determining the arrangement of that alphabet; in the double key systems it is a question of finding two unknowns: 1. thenumberofalphabets; 2. theirrespectivearrangement.

a. Number of alphabets.

It would seem at first sight that the means of investigation must be lacking

to establish the number of letters or alphabets of the key; nothing, however, is easier.

Let's suppose that a sentence like this is to be cryptographized:

"Vous ne pouvez vous défendre sans vous exposer," etc.

Since there is between the first two vousa distance of 8 letters, and between the second and third a distance of 12 letters, it will happen, if I choose a key of 4 letters, that the three vouswill be enciphered with the same alphabets, and they will give three similar tetragrams.If there were a fourth vousin the course of the text, it would give another similar tetragram, provided that it were spaced from the last one a number of letters forming a multiple of 4.

Let's take another example: "La présencede soldats ennemis nous a de nouveau été annoncée ce matin de différents côtés,"and let's omit the spaces:

lapresencedesoldatsennemisnousadenouveaueteannonceecematindedifferentscotes.

There are present, among these 75 letters, 18 repetitions, including 3 trigrams non, sen, nce; and 15 bigrams en, es, de, ce, no, te, ts, etc.

Even if one uses a key of 5, 6, 7, 8, 9, 10 different alphabets, it will always turn out that one or another of these repetitions will be found enciphered with the same alphabets, and one will thus have a ciphertext presenting, at the corresponding places, similar groups of letters (41). I shall now generalize the case, and state the following two principles: 1. Ineveryciphertext,twosimilarpolygramsaretheproductoftwosimilargroupsofletter,enciphered withthesamealphabets;2.thenumberofletterbetweenthetwopolygramsisamultipleofthenumberofletterinthekeyword (42).

To find the exact number of alphabets in the keyword, it is only necessary to look for the common factor contained in the numbers that represent the letters in the respective intervals.

Let's apply this reasoning to the following cryptogram:

RMUUWQPMQGXHWBGGKKKNITMUXWWTMGGXHEPH

We have here 4 repetitions: 1 trigram GXH, and 3 bigrains MU, GG, TM.

Now, from	MU	to	M' U'	there	are	21	spaces	=7 x 3
"	GG	"	G' G'	"	"	15	"	= 5 x 3
"	TM	"	T' M'	"	"	6	"	= 2 x 3
"	GXH	"	G'X'H'	"	"	21	"	=7 x 3

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

It is easily understood that the chances of finding combinations of letters produced by the use of the same alphabets are in inverse ratio to the length of the keyword and in direct ratio to the length of the cryptogram.

When the relationship of the letters of the keyword to those of the ciphertext is such that no repetition has been produced, decryptment presents some difficulties, and. it is necessary to have recourse to tentative assumptions; this is a point to which I shall return further on.

b. Arrangement of the alphabets.

Let us note first of all that the number of different alphabets can scarcely go beyond the number of letters in the alphabet; with a more or less large number it becomes in fact impossible to represent the key by one word, or at least there are certain difficulties in the management of the key. In addition, it is not the possibility of using a great number of different alphabets that gives value to a system, but rather the greater or lesser difficulty of determining the number of alphabets employed (43).

These 26 alphabets can be arranged in three different ways:

1. The letters follow each other in normal alphabetical order, as in the Vigenèze tableau.
2. This order is transposed in any way whatever (see page 30), but the 26 alphabets are still arranged in a square number.
3. The 26 letters are placed in a different order in each one of the 26 alphabets.

The decrypter generally has no trouble in ascertaining which of these three arrangements has been adopted.

a. Unmixed alphabets.—Let's take again the preceding cryptogram and divide it into groups of three letters:

123	123	123	123	123	123	123	123	123	123	123	123
RMU	UWQ	PMQ	GXH	WBG	GKK	KNI	TMU	XWW	TMG	GXH	EPH

We know that it is the letter E that occurs most frequently; if, then, I bring together the letters which in the different groups belong to the same alphabet, it will be easy for me to ascertain which are the three letters that represent the letter E. Moreover, since each of the 26 alphabets is characterized by the cipher letter that corresponds to the E, the knowledge of this single letter will necessarily bring with it the knowledge of all the others in the same alphabet, whether the cryptogram has been enciphered with the Vigenère tableau or with the St. Cyr or Gronsfeld system. We will have then:

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

If one looks now in our table on page 16 for the alphabets in which E is represented by the cipher letters G, M, H, one finds that they are the third, the ninth, and the fourth, that is, those which correspond to the keyword CID, or to the number 283 in the Gronsfeld system (44)(45). Here, then, are the three alphabets:

A E 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 1 m n o p q r s t u v w x y z a b a d e f g h
D d e f g h i j k 1 m n o p q r s t u v w x y z a b c

= Personne ne peut déchiffrer votre dépêche.

When the message is short, it sometimes happens that the coefficient of the repetitions, in such and such a series, leaves us in doubt about the cipher letter that corresponds to the E. This inconvenience is not very great, especially if the keyword has only 5 or 6 letters, because the context puts us immediately on the track.

It may even happen that, in a cryptogram of several lines, none of the most frequently repeated cipher letters correspond to the letter E. There exists a very simple means of determining, in spite of this anomaly, the differ rent alphabets of the keyword.

In order to grasp this procedure well, it is necessary to remember that, in unmixed alphabets, the relative position of the letters is always the same; in the alphabet in which l corresponds to E, the following letter, or m, necessarily corresponds to F, and the r corresponds to K and d to W; likewise, in the alphabet in which the letter E is represented by a p, the letters K and W will be represented by the cipher letters v and h. Now, since the K and the W are only rarely found in French, the decrypter will reject any alphabet in which the cipher letters corresponding to these letters have somewhat high coefficients.

Let's suppose now that, in the calculation of the letters in such and such column, I find for the strongest frequencies 12 l, 9 r, 8 d, 6 v, 5 h, 5 u, 4 x, 3 o, 3 g; I will see immediately, on inspecting the tableau, that thealphabet sought must be that in which the E is represented by the cipher letter h, because in the other 8 alphabets the cipher letters l, r, d, h, u, etc., correspond sometimes to a K, sometimes to a W, an H, a Y or a Z, which, in view of the minimum importance of these letters, is an inadmissible case.

From the point of view of the decipherability of the messages, the systems with unmixed alphabets do not present any more guarantees than a simple substitution in which word division is not indicated. (46).

b. Irregularly transposed alphabets.—When, in the decryptment of a cryptogram, it is impossible to make sense with the alphabets that the repetitions of the letter E seem to indicate, one must suppose that he finds himself in the presence of a mixed-alphabet system, and it is necessary in some way to try, one after another, the first letters of the message. If the cryptogram is long enough, the solution of the problem rarely presents insurmountable difficulties; it demands only a little patience and some inductive reasoning. In such a case, besides the calculation of repetitions of single letters, it is necessary to note the repetitions of certain bigrams and trigrams of which I spoke on page 12; it is also necessary to know how to put to account the facts that are furnished on the probable nature of the correspondence, and to keep in mind the style belonging to the particular circumstances or situation of the correspondents. Thus, to give an example, the bigram ez is extremely rare in correspondence between persons who address each other familiarly as tu, while, on the other hand, the majority of instructions sent, on campaign, to junior officers commence with vous or le.

We are going to decrypt a dispatch sent from London to the Havas Agency, concerning military affairs in Egypt.

London, 2 September.

RBNBJ JHGTS PTABG JXZBG JICEM QAMUV IVGAG NEIMV REZKZ SUABR RBPBJ CGYBG JJMHE
NPMUZ CHGWG UDCKC JKKBC PVPMJ NPGKV PWADV CPBVM RBZBH JWZDN MEUAG JFBMN KEXHZ
AWMW AQMTG LVGHC QBMW ZEUKV RETEW CPBVM CBAMN RBJCZ EAUUZ KBCBX RBJEJ DTEDR
LKCEY IFBHX JHSBO DFEHF ZAAAK SWMVZ SKAUZ IKCDR UBAVL NJSBJ SBPAL GDYFZ GBAQK
NBAUZ GDPVR SAJEX NDUBJ GDUJX IMXJL SKKBC HAMNZ IUGWC RBJEJ DTMKZ SBSBE DWZMJ
JQQJX JZMKZ JJYHG DIKIJ JUYPV JVXWA JLMHC JJBSO CEJTZ IJBWX EEXWJ JWGWZ JWSBE
JJMKX LDXJH DBOAJ JJQDJ CTMJZ LQXPZ HMJEF UEUIG DAAUV IVGAG NE.

Let's try first to determine the number of alphabets in the keywords

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

I have noted here only half the repetitions, but that is enough for us to see that the keyword must be composed of 5 letters.

If we divide the cryptogram then into groups of 5 letters and count the 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.

When we work on a fairly long cryptogram, we are authorized to believe that the cipher letter repeated most often in each column corresponds to the letter e; we admit also, and that as a necessary consequence, that the 2nd and 4th columns (B = e) represent the same alphabet.

As for the probable content of the cryptogram, we must watch for such words as Arabi, Wolseley, Suez, Ismailia, canal, general, soldats.

Let us note furthermore that of the first ten letters we already know 3, which represent e, to wit:

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

That being said, I ask myself with what part of speech a telegram addressed

to newspapers might begin, and I proceed, as must always be done, by elimination.

It is hardly probable that the first sentence would be interrogative or imperative; if the first word is a verb, it must be in the infinitive form or the present participle. The very simple style of this kind of communication does not permit the supposition that it is an infinitive; neither is it a present participle, because it would have to belong to a verb of four syllables with an e in each syllable, and régénérer, régénérant, which is the only one of this kind, does not fit the situation.

In regard to nouns, it is necessary to eliminate common nouns, which are always preceded by some determinative; the same must be done with the adjectives divers, différent, maintand certain,, the only ones that could begin the sentence without being preceded by de, but which do not have the e in the proper position.

Among proper names (those which are in use, of course), number-words, adverbs, prepositions and conjunctions, there is not a single word that has two e's in the 3rd and 4th positions.

The cryptogram, then, can only begin 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, the present participle of a verb must follow, such as recevant, revenant, and GTS will represent the termination ant; now, this is inadmissible, the t being a frequently used letter and the cipher letter S only occurring once in the 5th column.

It is necessary to reject also les, cet, ces, mes, ses, the third cipher letter, N, being scarcely able to represent the letter s or t, for the reason that it appears in its column only two times. Since the first cipher letter, R, occurs eight times, it is equally impossible that we are in the presence of a j (je); it is, then, leor ce, but rather lethan ce, because of the frequency of cipher R.

Le or cemust be followed by a noun, an adjective or a number-word, and, note it well, the word must have an e in the first two syllables. No number-word fits the case? the adjectives récent, décent and témétaire, which have the two e's, must be rejected since the coefficient 1 of cipher N is, as has already been said, too low for a détestable will not fit either, the12th cipher letter, T, not standing for the nouns désertand télégraphe are, because of their t, in the same case as décentand téméraire. One finds that only généralfulfills the desired conditions; we then decide on leinstead of ce. I write down these two words, and I continue.

	S	P	T	A	B	G	J	X
Le général	.	.	.	.	e	.	e	.

It is to be assumed that the dispatch tells what general is concerned: it is, then, a proper name that is going to follow. Cipher S must be a very little-used letter, such as k, w,Y, Z, because, as we have said, it appears only once in its column; we have, furthermore, an e in the 5th and 7th position, and this latter e is followed by a cipher letter with the coefficient l: that answers exactly to Wolseley.

	Z	B	G	J	I	C	E	M	O	A	M
Le général Wolseley	.	e	l	e	.	.	.	.	.	.	e

It is quite probable that the verb is going to follow its subject: we already know the value of the 2nd, 3rd and 4th cipher letters, and we know that the Z has a rather high coefficient; if Z is the auxiliary verb a, the participle that follows es élevéor électrisé; but these do not have the final e in the right position; so the verb is in a simple tense. Among the only possible verbs, dépend, dément, mène, retenuand télégraphie, the last one is to be preferred, because of the final e.

U W I V G A G N E
télégraphie . . . . a i l . a

There is reason to suppose that télégraphie is followed by que or qu'il, or by a place names it is not que, since I is not an e; it is not qu'il, because we know the l (= T) of the second column; so it is probably a place name.

The place name must be preceded by the preposition de; here, however, it must be a simple d', because the e of the 3rd column is represented by a B. In regard to place names beginning with a vowel, having an a in 4th position and an l in the 6th, one can cite only Ismailia.

I MWR E Z K Z S U A B R R B P B J C
d'Ismailia . . i l a t . e . d s e . l e . e n .

The structure of the sentence, as well as the presence of il, indicate immediately that IM stands for qu; the verb has to follow and one guesses easily, from the letters that we already know, that this verb is attend. As for the final group, the dictionary gives only the words selleand seulement, which fit the pattern: it is evidently the latter that we have here.

G Y B G J J MH E N P M
qu'il attend seulement . . e l e . e r . i . e

The adverb seulement is rarely followed by a que; but since the G occurs only once in its column, which applies very well to q, and since we have an e in the third position, we must admit the que. The last group is a word beginning with a consonant, since it is preceded by le, and this consonant appears quite often; there is, in addition, ani in fifth position: service alone fulfills these requirements.

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 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: detransportsetdecommunications. The end of the sentence is still easier: soitcompletemento.ga.ise.our.a.re.nen.u.ellemarcheen..ant, that is, soitcomplètementorganisépourfaireunenouvelle marcheenavant.

I shall stop here; it will be easy for the reader to decipher the rest himself.

Setting aside the question of number, it is not possible for the decrypter to determine the value of the letters that compose the key except when the message has been enciphered with the Saint Cyr system. Unless it be ad- mitted that they

key must necessarily be a French word or make some kind of sense, every message written with mixed alphabets contains 26 different keys, in relation to the initial alphabet of the tableau. Nothing proves better than this consideration how wrong Major Kasiski was to base his method of decipherment on the actual value of the letters of the keyword.

In the present casethe keywordis degel withthe Saint Cyr system,andpuluy with the tableau thatwill follow(page 30).

Once the number of letters in the keyword hasbeen determined, it beingassumedthat the message isfairly longand that somefacts areknown aboutthecorrespondents or the probable nature of the content, it is very rarely that a cryptogram can not be deciphered. In rather difficult cases, it is generally the first two or three words that come to play the role of traitorsz now, nothing is easier for the decrypter than to make for himself a list of the words that, in time of war, might begin a dispatch and to classify them according to the position of the E that is found in themz those which do not contain any E will be drawn all the more clearly to his attention.

c. Regularly transposed alphabets. Symmetry of position.—I have decrypted the preceding message without trying to find out whether it had been cryptographized according to a system that arranges its alphabets in a square number, or whether the correspondents had limited themselves to choosing five different alphabets at random. This, however, is a very important point that the decrypter should never neglect. In fact, once the alphabets are arranged in a square number, and the meaning of one cipher letter has been found in two or more alphabets, one can by simple addition, determine the place that any new cipher letter whose value can be established in one alphabet occupies in these different alphabets.

In order to present a clear account of this peculiarity, which has not been pointed out in any work on cryptography, let's consider for a moment the tableau that served to encipher our cryptogram.

The arrangement of this tableau differs from thatof Vigenère only in the fact that the normal order of the letters has been transposed; the letters themselves, while never appearing twice in the same place, in regard to the numerical order of the vertical columns, nevertheless always follow the same order in the horizontal rows (47). Thus, in each one of the latter, the R is always followed by E, and the E is always two spaces from P and five spaces from L. So, once one knows the position of the R in two alphabets, the position of the letters E, P and L will be known in the second alphabet, since it will already have been established in the first.

Let's take an example: I assume that in trying to decrypt a message cryptographized with a keyword of three alphabets, the value of the nineteen cipher letters indicated below has already been found; that is, E P B L A F N for the first alphabet, U A T for the second, and T D F H K M R S I C for the third. Since the letters of the three alphabets taken two at a time have one common letter, A and T, I can carry the letters of one alphabet

	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

---

over to the other, by the simple procedure of placing them, in the three alphabets, at distances respectively equal to 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	.	k	m	.	.	.	.	r	.	s	.	.	.	.	i	c	.
l	r	e	s	p	u	b	l	i	c	a	.	.	t	.	.	d	f	.	h	.	k	m	.	n	.	.
2	.	h	.	k	m	.	n	.	.	r	e	s	p	u	b	l	i	c	a	.	.	t	.	.	d	f
3	.	.	t	.	.	d	f	.	h	.	k	m	.	n	.	.	r	e	s	p	u	b	l	i	c	a

If I had realized this peculiarity in the decipherment of our dispatch, I would have been able to stop at the fifth word, the number of the letters already deciphered plus that of the letters learned by symmetry of position being more than enough to decipher the rest of the cryptogram almost as fast as I could write.

It will be easy to understand this by inspection of the tableau below, in which the letters known through decipherment of the first five words are written in capitals, while those whose value is revealed by the principle of symmetry of position appear in lower case:

	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		I	c	a	z		t	v	w
2,4	E	s	p	U	B		I	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 set in a square number, since there is hardly any occasion to decipher a cryptogram whose 26 alphabets have a random arrangement; that would be an impractical system and for that very reason inapplicable in time of war. Because, if the obligation of memorizing the arrangement of a single alphabet can sometimes present certain difficulties, what would the difficulty be if it were a question of learning 26 different alphabets, each one arranged according to a plan that excluded any regularity? It would be necessary to have written notes, and the value or security of the system would depend solely on the prudence of the agent called upon to apply it. Also, all the devices of any value that have been invented in recent years, such as, for example, the Wheatstone cryptograph, are based on a regular transposition of the alphabet, and the principle that I have just explained is perfectly applicable to them.

d. Indeterminate alphabets.—If in the decipherment of a cryptogram using transposed alphabets it is impossible to determine the number of alphabets in the key, whether it be because the message is too short or because the key is too long, the solution of the problem presents difficulties, if not insurmountable, at least capable of trying the patience of the most able cryptographer.

The situation changes if one finds himself in possession of several cryptograms written with the same key, however short they may be; by arranging them one under another, one can make a calculation of the repetitions of letters analogous to that which we have done, page 24, on the cipher letters grouped in sections or by columns.

Here are a dozen cryptograms, very short, which have been enciphered by the preceding tableau, and with a whole phrase: “Je me mets sur la défensive”; we shall see that the decryptment of them is quite easy.

No. 1. UHYBRJIMBCFAMMTJTDMRIQ
2. UHWPRBQLKIBLWREJRBKLGIXBQEXHM
3. IEWHCHQKQMTMVGJJEDZVA
4. UWVRRHIKMCWWEGHDCXSRQH
5. UHSHAHKSVCJWZVXJYNDMQQN
6. YHVHMAGQKCWXPVIHHWLZVLTHV
7. LHVHAAGRLPFMSOHIPWZZJELQRBW
8. SWUIRXICJUFSHGWRSZBAAL
9. UHWHVAGULCJWOUKDEBKQ
10. YWXHYHBALGBVPSWIWWJRRH
11. WQREXBIENHMVYMHSIYM
12. SWUHDHPJJCKXGMHL
13. GQVQRVOTQQSPWR

Let us note in passing that of the 22 letters of which the key is composed, there are 3 that are repeated and that we thus have in reality only 14 different alphabets; this is a case which it is hardly possible to avoid and of which the decrypter should know how to take advantage.

In order not to extend the demonstration beyond measure, I shall concern myself with only the first two words of numbers IV, V, VI and VII; in addition, in order that the reader can more easily follow my reasoning I shall place 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	fammtjtdmriq
II	u	h	w	p	r	b	q	l	k	i	blwrejrb, etc.
III	i	e	w	h	c	h	q	k	q	m	tmvgjjedzva
IV	u	w	v	r	r	h	i	k	m	c	wweghdcxsrqh
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	fmsohi, etc.
VIII	s	w	u	i	r	x	i	c	j	u	fshgwrszbaal
IX	u	h	w	h	v	a	g	u	l	c	jwoukdebkq
X	y	w	x	h	y	h	b	a	l	g	bvpswiwjrrh
XI	w	q	r	e	x	b	i	e	n	h	mvymhsiym
XII	s	w	u	h	d	h	p	j	j	c	kxgmhl
XIII	g	q	v	q	r	v	o	t	q	q	spwr

In applying the calculation of repetitions, we assume the presence of e in columns 2 (= H), 4 (= H), 5 (= R), 6 (=H), 7 (= I), 9(= L), 10(= C); we see besides that the cipher letter 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, belong equelly to the same respective alphabet; but since we are supposed not to know the key, it is only later that we shall be able to state it; we count, then, provisionally, on the 10 columns, 8 different alphabets. Let's begin with No. IV:

	1	2	3	4	5	6	7
No. IV.	U	W	V	R	R	H	I
	.	.	.	.	e	e	e

We have assumed that the cipher letters RHI represent, all three of them, the letter e. Since no word in French can begin with two e's, we have here a word ending in ée; the number of letters that precede this ending indicate to us at once that we are in the presence of the word armée, preceded by l'. We write down then 6 letters, of which 2 are given by symmetry of position (48).

	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 that follows le has an e in the 2nd and 4th positions; this is the same case as the dispatch that we deciphered on page 27; it is therefore useless to go over our reasoning again, and we say immediately that the word is général.

The decipherment of this last word gives us 10 new letters, that is, the 5 in the word général, S-A-KSV, plus 5 others furnished by symmetry of position; the placing of S in alphabets 8 and 9 shows at the same time that these 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	Q	K
	.	e	r	e	.	v	.	.	.

Since the M does not correspond to an n (=A), the first word can only be either ferez or serez; it is impossible for the moment to decide between f and s, but, whatever the verb may be, it must be followed by vous. We write down 15 new letters, of which 4 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	a

We have here: le renvoi, je renvoie, or ne renvoyez; now, symmetry of position is opposed to the R of the 8th column being an i; because we would then have in the 3rd alphabet an R placed just two spaces from the S, and another R placed 18 spaces from the S in the 8th alphabet; it is, therefore, ay, and we read: ne renvoyez.

Decipherment has given us here the meaning of only 3 new letters, but symmetry of position informs us, in all the different alphabets together, of 46; simply by placing the L in the alphabet of the 1st column, where we already know that U = l, we can determine the place of 11 new letters. We see at the same time that columns 3 and 5 are enciphered with the same alphabet.

The reader will not have any difficulty deciphering the rest himself, especially if he continues with Nos. XI and XIII.

We conclude from what precedes that, whatever the arrangement of alphabets adopted, correspondents are always kept from writing each of their messages with a different key.

c. Variable key system.

The variable key systems were mentioned on page 21. A message written by the system indicated is hardly decipherable unless the decrypter can recover the indicator letter. This is not easy with a very short message; but when it has four or five lines, one notices immediately a certain regularity in the very irregularity of the recurrences of the letter; it is the only cipher letter, for example, that is never found doubled. Now, once the indicator letter is found, the decipherment is certain; it is only a question of placing in columns the different groups formed by the intervals from one indicator letter to the next, and making the calculation that we are acquainted with. A valuable fact is, besides, furnished by the Arabic number that indicates the place occupied by the indicator letter in the key (49).

Decipherment can only offer some difficulties when the alphabetic order of the letters has been transposed irregularly; also I was able to decipher, in less than two hours, cryptograms composed in this system, which were sent to me by the Commission of military telegraphy.

5. A triple key cipher.

It results from our attempts at decipherment that of all the multiple

substitution systems of cryptography that are in use today, none presents any serious guarantees of indecipherability. Of course, it may happen that such and such a message, four or five lines long, enciphered with unmixed alphabets and with a keyword of only five or six letters, may resist the efforts of the best decrypter; nothing is easier, for one who knows how to decrypt, than to compose indecipherable cryptograms with the most common of systems. But if cryptography is ever to become, as one of our best generals has said, a powerful auxiliary of military tactics, it is necessary that the system adopted be able to defy, even when it is operated by inexperienced hands, the most laborious investigations of decrypters.

If it were permissible to neglect for an instant the essentially practical side that any system of cryptography destined to the needs of the army must present, in order to consider only the desideratum which demands the exclusion of secrecy, one could adopt a triple key system, and combine a transposition procedure with a multiple substitution system. The Saint Cyr system, combined with the transposition method described on page 8, would permit the minimum of written notes, and would give a cryptogram, if not mathematically indecipherable, at least not permitting any calculation of probability.

The two keys would have to be represented by different words, such as an adjective and a noun; the first word, composed of a small number of letters, would serve as key for the substitution work, and the second, of a greater number of letters, would give the transposition formula; for example: chose problématique, affaire exceptionnelle(50).

Let's encipher a message with this system: "Vous ferez ce soir une attaque simulée,"taking as key sénatromainand using the Vigen ere tableau.

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	e	e
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	A	T	S	E
n	s	h	s	y	w	v	r	z	v	w	w	b	i	k	m	r	r	a	m	1	e	d	u	x	k	m	z	u	e	w	i

Romain gives for a numerical formula 6 5 3 1 2 4; we have then:

A

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

B

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

= dcawibeumxkzrrkbiwyhnsswwzvrvudlame.

But, I repeat, this procedure dispenses with the need for secrecy and guarantees an almost complete indecipherability in vain, because it leaves too much to be desired from the practical point of view for it to be possible even to dream of applying it to the service of war. Also, it is only under the title of a curiosity that I wanted to indicate a system dispensing with the need for secrecy and fulfilling thus the principal desideratum of military cryptography.

C. Cipher Dictionaries.

It is difficult to learn precise facts about the different systems of cryptography that, since the last century, have been in use in the French army; nevertheless, it is known positively that, even before the Revolution, the general staff had had compiled, for the use of secret correspondence, tables analogous to those which the Ministry for Foreign Affairs still uses today. These tables contain, alongside set phrases, a certain number of ordinary words; opposite them were found one or two numbers to represent them. General Lewal has quoted, in the Journal des Sciences militaires, the fragment of a letter addressed, under date of 2 May, 1815, by Minister for War Davout to his colleague in foreign affairs, to ask him for two ciphers of this type for military correspondence. These ciphers, or ciphering tables, as they used to be called, have become the cipher dictionaries that are used today in the army.

As early as 1850, Bracket (51) had thought of composing for the public an analogous dictionary, in which each word is invariably represented by a five-figure number. M. Sittler (52) later compiled a small vocabulary of some fifty sheets, in which each page contains 100 words, represented by the numbers from 00 to 99; the word that one wants to write is determined by adding to this number the number of the page. The pagination, which is left blank, and which must be indicated by hand, according to some agreed upon system, constitutes the secret of the method. The plan of the work is well enough conceived; it is only the more to be regretted that the author forgot to indicate the precautions to be taken in order to assure the secrecy of the messages in case the dictionary fell into the hands of the enemy.

MM. Brunswick (53) and Gallian (54) have sought to fill this gap by compiling, the first named, a dictionary in which the letters with their binary combinations, and some thousands of words with their grammatical flexions, are represented by groups of numbers running from 0000 to 9999; and the second one by compiling an analogous dictionary, in which the groups of 4 numbers are replaced by combinations of three letters (55).

The method adopted by the two authors to thwart the calculations of decrypters is very ingenious. Here, in a few words, is the procedure of M. Brunswick: first of all, the figures of each group or number are transposed according to some formula agreed upon, then this transposed number is increased or decreased by another number; this last number, together with the transposition formula, constitutes the key of the cipher. Let's take an example: suppose we want to write avancez,and that the corresponding number given by the dictionary is 2143; this number can be transposed in 12 different ways: 2134, 4321, etc.; let's choose 2134. If the agreed upon number that is to be added is 214, the final cipher number will be 2134 plus 214 = 2348.

Since there is great latitude in the choice of the number to be added or subtracted, it is impossible, as long as one does not have the dictionary, to establish the slightest calculation on the groups thus obtained. But once in possession of the dictionary, it is sufficient to know any two groups in a message in order to recover at once the key of the whole thing. Now, the circumstances in which a message has been written being known, it is very easy to recognize by the repetitions of certain groups the presence of such and such word. Thus, the following four groups, 4213, 6555, 6555, 2140, placed at the beginning of a cryptogram, would probably contain the pronoun nous, vous or ce repeated; it would be in fact difficult to compose in French the beginning of a sentence in which some word other than nous, vous or ce could be found repeated in the second or third position; for example: Poavez-vousvous

défendre?Devons-nous nous retirer?Est-ce ce soir?

It would be too long to go into all the details that can enter into the decipherment of a message cryptographized with a cipher dictionary; I shall limit myself to a single example.

Suppose that certain indications authorize me to believe that in an intercepted dispatch group 9645 means colonel, and group 7457 régiment. Here is how I would proceed to recover the transposition formula as well as the key number.

Let's assume 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 in the presence of the 9 and the 7, left intact and placed in first position, that the key is composed of only three figures, and that, in the changing of the original number, the second figure has been carried to the first position; in addition, the figure 6 of the first number indicates clearly that the key calls for an addition and not subtraction.

The numbers 645 and 457 represent, then, the sum of the key number increased by the number produced through the changing of 413 and 234. Now, if I subtract successively from the first two numbers the six changes obtained, I shall have for the two operations a common difference, which will represent the agreed upon number, at the same time as it makes known what the transposition formula was.

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

I conclude that 214 is the key number, and b a d c the transposition formula.

The operation cannot give any common difference unless the groups of the cipher text really correspond to the supposed words.

Of all the known methods of cryptography, it is certainly the cipher dictionaries, at least those that are based on a double principle of composition, like those of Brunswick, Gallian and Niethe, that guarantee best the secrecy of the correspondence. But, along with this real advantage, they present such great disadvantages in their application to correspondence in time of war, that one cannot help being astonished at the favor they have enjoyed up to now among certain army chiefs.

The greatest complaint that can be made against cipher dictionaries is that they require secrecy, and that they constitute, by the very fact of their adoption, an obstacle to the widespread use of crytographic correspondence. This condition of secrecy can moreover cause the greatest embarrassment.

It is reported that, on January 8, 1871, a cryptogram was sent from the general headquarters of the King of Prussia to General de Werder, who could not decipher it immediately, because the dictionary containing the key of the secret correspondence was locked up in a valise placed in a carriage that had been driven away.

During the Russo-Turkish war, Selim Pasha, political sub-chief of Mehemet Ali, absented himself for a few days in September, 1877, and carried off inadvertently the deciphering book. During that time, the general-in-chief received a great number of enciphered dispatches that he was unable to read.

But, besides the fact that a printed vocabulary can be purchased by the enemy, and the fact that the adoption of a dictionary must necessarily restrict secret correspondence, there are the greatest disadvantages in making the meaning of a word or an entire sentence depend on the correct transcription of a number; let a single figure in a group be wrong, let a telegraphist or copyist put, for example, a 3 where a 5 should be, and the meaning can be completely changed. Generally there is only a simple misconstruction, or an incomprehensible phrase; but the error can have most unfortunate consequences, and it has happened more than once that a badly transmitted or wrongly read cipher has distorted completely the meaning of an order or of an item of information. If it is not rare to see persons used to handling ciphers make, in an excited moment, errors in simple addition, nothing is more common than to see telegraph employees make mistakes in the transmission of cipher groups. This drawback, which was strongly felt during the war of 1870, in which half the dispatches sent by the military authority to the prefects contained illegible parts, was again encountered several times during our campaign in Tunisia? more than once it was impossible, in the Ministry for War, to decipher the dispatches from the army in Africa.

Not very long ago, the Italian ministry was singularly intrigued by the news that its ambassador in St. Petersburg sent it: that Count Andrassy was expected in the Russian capital. It was all simply a cipher error, which had caused the name of an embassy attaché to be taken for that of the celebrated statesman.

Cipher dictionaries are really of practical and safe use only for the chancelleries, whose personnel, with their papers and their baggage, are inviolable in all civilized countries, and who have their dispatches enciphered and deciphered by employees experienced in this type of work and having the means of verifying, at their ease, the faithful transmission of correspondence.

IV.

CRYPTOGRAPHIC DEVICES.

If the few examples of decipherment that precede have stressed the weak side of our principal systems of secret correspondence, they likewise permit us to appreciate the difficulties presented by the construction of a cryptographic process that fulfills the desideratum that I have indicated as the basis of every method of military cryptography, that is, the non-necessity for secrecy.

We have seen that it is impossible to replace sentences and words with groups of letters or numbers without creating by that very act a dictionary that demands secrecy; we also know that transposition procedures guarantee indecipherability only on condition that they be based upon some secret apparatus? it follows, and I insist on this point, that a method that is both safe and practical can only be established with an arbitrary substitution of letters. It is true that, if the system is simple and rests upon some regular process or some systematic combination, it necessarily exposes its flank to the calculations of decrypters; if, on the other hand, it is al all complicated and calls for numerous combinations, then it demands secrecy or 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 on the principle of substitution,

that is to say, in the employment of a cryptograph.

This idea, moreover, is not new.

The Lacedemonian scytale, the planchette of Aeneas (pierced with twenty-four holes representing the letters of the alphabet, holes through which a thread was passed to indicate the order of succession of the letters of the secret missive), Kessler's drum, were true cryptographs.

The first model of a cryptograph worthy of the name is found in the Traité des Chiffres by Porta; it is the dial system of which I have already had occasion to speak.

Father Kircher had also invented a mechanical apparatus that he had called Areaglottotactica (56); it was a kind of movable catalogue, in which the words were classed in a certain order corresponding to the different letters of the alphabet. The aerial telegraph of Chappe, like the Morse telegraph, are other true cryptographs.

In recent times, cryptographic devices have been invented by MM. Mouilleron, Vinay and Gaussin, Rondepierre, Wheatstone, Silas and others.

M. Mouilleron's system, the description of which is found in the Exposé des applications de l'électricitéof Du Moncel (57), is a mechanism mounted on a desk, quite complicated and not presenting any practical advantage. The author does not seem to have made a very deep study of double key ciphers, because his voluminous mechanism only ends by giving us a cryptogram enciphered by the Vigenère tableau. It is easy to confirm the perfect exactitude of what I claim by cryptographizing the example that the author gives, Lavictoireestànous, with our tableau on page 16; with the key kzirh, one will obtain the same cryptogram as that which is given by M. Mouilleron's apparatus, with the key paris (58), thus:

l	a	v	i	c	t	o	i	r	e	e	s	t	a	n	o	u	s
K	Z	I	R	H	K	Z	I	R	H	K	Z	I	R	H	K	Z	I
v	z	d	z	j	d	n	q	i	l	o	r	b	r	n	y	t	a

= vzdzjdnqilorbrnyta

The cryptograph of MM. Vinay and Gaussin is a printing mechanism by means of which the dispatches are printed and cryptographized at the same time. While more portable than the preceding one, it is still too voluminous for its use to be possible in time of war; from the strictly cryptographic point of view, it has, furthermore, no value at all (59).

The cryptograph or phyrograph of M. Rondepierre is based on the transposition system that has been explained on page 8. The vertical columns are represented by ivory rods on which are traced divisions destined to receive one letter; they are first transposed according to a numerical formula, then the message is written in pencil on the rods themselves. These are then returned to their original place, and the letters are copied in the new order in which they appear» The system is, from a certain point of view, quite practical, but it offers only a relative security (60).

I shall say nothing of the cryptograph of M. Silas, former attaché of the French embassy in Vienna; although it is a serious and very well constructed work, it is too complicated, in my opinion, for war use.

Of all the cryptographs that have been invented in recent years, that of Wheatstone seems to me to be, if not the safest, at least the simplest. Since I have not been able to obtain a copy of the apparatus, I borrow my description of it from the Report of the Military Commission on the Universal Exposition of 1867 (61):

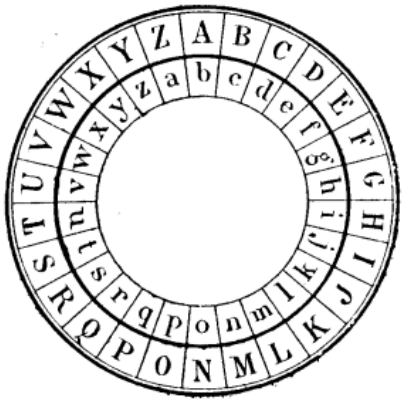
The very simple instrument proposed by M. Wheatstone for writing messages in cipher is easy to use, says the reporter, and assures the most absolute secrecy (?) for those who do not have the key of the system.

Here is the principle on which the cipher alphabet is formed: Any word is chosen to serve as keyword, France, exposition, projectile, etc. Let's suppose that the word projectile is selected; the word is written down spacing the letters that compose it, and underneath are written the letters of the alphabet that it does not contain, in 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

By taking the letters in the order in which they appear in the successive vertical columns, the alphabet following is obtained:

pasrbuodvjfxegychztkwimlng



The letters of the cipher alphabet are written on a circular piece of cardboard. This circle is placed concentrically on a metal dial, which bears on its circumference an ordinary alphabet, completed by the stop-sign†, to which one returns at the end of each word, but which does not appear in the cipher. Two hands, 1 and 2, move simultaneously around this double dial, but at different speeds and in such a way that on moving the first hand to the letter B again, the second one will not come back to the same letter, such as V, indicated in the diagram, but to a different letter on the inner dial.

When one wishes to translate a given letter into cipher language, one moves the large hand to the place occupied by this letter in the normal alphabet, and marks down the letter on which the small hand has stopped in the cipher alphabet. The system thus has two keys: the arrangement of the cryptographic alphabet and the starting point.

Whatever Colonel Laussedat, the author of the report I have just quoted, may think of it, messages written with the Wheatstone cryptograph are perfectly decipherable.

The system gives only a very limited number of different alphabets; the same alphabetical arrangement recurs after a certain number of stops.Let's suppose that this happens after the 26th or 30th letter; I then only have

to consider the cryptogram to be deciphered as being written with a key of 26 or 30 alphabets and to put it into columns in series of 26 or 30 cipher letters, as we did for the message on page 26. But the greatest disadvantage that the apparatus presents is that it demands absolute secrecy; for once fallen into the hands of the enemy, it is enough to make a few assumptions on the first letters of the message to recover the starting point.

When several messages, written with the same key, have been intercepted, it is not necessary to possess the apparatus in order to make the decipherment. One applies the procedure that I have indicated on page 32.

There has just been presented to the Commission on military telegraphy a new system of cryptography, which seems to me to fulfill all the desiderata that I explained at the beginning: complete indecipherability, simplicity, non-necessity for secrecy? highly important considerations prevent me from saying any more about it for the moment.

Without wishing to prejudice the reception that this new proposal may get from competent judges, I must, in conclusion, insist on this point, that the value of a system of cryptography destined to the needs of war is in inverse ratio to the secrecy that its operation or composition requires. It will depend, then, on the Administration to assure the future of military cryptography, by accepting only the invention that rests upon the principle that du Carlet. one of the masters of our art in the XVIIth century, had Inscribed as a motto at the head of his method, a principle that summarizes, moreover, my whole thesis, that is, that a cipher is good only as long as it remains indecipherable even by the master who invented it: Arsipsisecretamaqistro (62).

NOTES TO SECTION 1.

(1) Under the term steganography, ciphers, or secret writing, certain encyclopedic dictionaries give the facts pertaining to cryptography. Ancient writers call it more or less correctly: ars notarum, ars zypherarum, polygraphia, scotographia, cryptologia, steganologia, cryptomenytices, etc.; the Germans say today Geheimschrift or Chiffreschrift, and the English, cryptography.

(2) Letters placed between the shoe soles of the messenger, communications hidden in a wound of the carrier, or in women's earrings, pierced with 24 holes through which a thread passes, carrier pigeons, etc. Aeneas (4th century B. C.) is the most ancient of the military authors whose writings we have; chapter XXXI of his Commentaires sur la défense des places (translated by Field Marshal Beausobre, 1757) is devoted to enciphered letters and the way to send them secretly.

(3) The invention of Kessler, which Colonel Laussedat recalled in one of his lectures, is explained in a little book that has become very rare, published in 1616 in Oppenheim and entitled: Unterschiedene bisshere mehrern Theils secreta oder Verborgene geheime Kunste.

(4) Roman History, Bk. X, chap. 44-48.

(5) Lysander, chap. 19.

(6) Chap. XL, 9; chap. XLI, 3.

(7) Caesar, chap. 56; Octavian, chap. 88.

(8) Attic Nights. Bk. XVIII, chap. 9.

(9) Origines, I, 24.

(10) What one finds in the Cestes, a work on military art attributed to Julius Africanus, and of which a French translation was given in the Mémoires critiques et historiques de Guischardt, is hardly more than a copy of Aeneas's Commentaires.—Philon of Byzantium, the author of the Poliorcétique, who lived in the 2nd century B. C., had composed an entire treatise on the Sending of secret letters, but this work has been lost.

(11) Gaspari Schotti, Schola steganographica, 1665; classis viii.

(12) Gustavi Seleni, Cryptomenytices et cryptographiae, libri IX, 1624.

(13) See: Commentaires sur la défense des places, p. 145, translator's note.

(14) One finds the following precept in the Breviarium politicorum of Cardinal Mazarin: "Scribere secreta manu tua ne graveris, nisi per zifras scribas."

(15) Cf. Bardin, Dictionnaire de l'Armée de terre, 1843.

(16) Manuscrit de 1812, contenant le précis des événements de cette année, pour servir a l'histoire de Napoléon, 1827.—Colonel Fleissner (Handbuch der Krvptographie) even attributes to him, but wrongly, the invention of a new cipher.

(17) Tactique de marche, 1876.

(18) See the article Chiffre stéganographique.

(19) Captain Henri Berthaut, to whom I allude, is certainly one of the most capable dearypters on the general staff.

(20) Volume III, p. 76.

(21) Dictionnaire philosophique, article Poste. It is quite curious to see Count Clarendon, in a letter written a hundred years before to Doctor John Barwick, express himself in analogous terms with regard to decipherers: "I have heard

of many of the pretenders of that skill, and havespoken with some of them, but have found them all to be mountebanks."

(22) Le Cont'espion, ou les clefs de toutes les correspondence secrètes.

NOTES TO SECTION 3.

(1) I intend to publish soon a complete work on the different systems of cryptography; I shall be grateful for any new method that anyone cares to communicate to me, provided that it has some value from a practical point of view.

(2) See Klüber, Kryptographik, chap. XIII; Du Moncel, Exposé des applications de l'élecricité, III, p. 530

(3) Since the sum of the letters in plaintext must form a multiple of the number of horizontal rows, one adds, if there are spaces left, the necessary number of nulls to fill the final row; five are needed here.

(4) A device invented by an architect of Paris, M. Rondepierre, and to which he has given the name of Phyrographe, is constructed on this principle.

(5) This is a very serious fault on the part of the one who invented the system.

(6) I suppose that if the same letter is repeated, one counts the repetitions as so many more letters following in alphabetical order. For example:

Taganrog = aaggnort = 81325764
12345678

(7) This process seems to have been invented in the 16th century by the Italian mathematician Jerome Cardan. See his book De subtilitate, translated into French by Richard Leblanc, De la subtilité et subtiles inventions, Paris, 1556. —See also De Prasse, De Reticulis cryptographicis, Leipzig, 1799.

(8) Handbuch der Kryptographie, by Fleissner von Wostrowitz, Vienna, 1881.

(9) Suetonius, Octavian, chap. 88; Isidore, Orig., I, 24.

(10) Suetonius, Caesar, chap. 56; Aulus Gellius, Attic Nights, Bk. XVII, chap. 9.

(11) In the Bible are found similar examples of substitution: the prophet Jeremiah (chap. XXV, 26) writes, for example, Sheshach instead of Babel, replacing thus the two consonants b, l by the letters sh and ch, which occupy the same position in the Hebrew alphabet, when one counts them from right to left.

(12) Polygraphiae libri VI; composed, according to the preface, in 1508. A translation of it was made by Gabriel de Collange: La Polygraphie et universelle escriture cabalistique de Jean Trithème. Paris, 1561.
Several works of cryptography or steganography have been published under the name of abbot Tritheim (1402-1516), without anyone being able to tell exactly how much in them is really from him (Cf. Schott, Sohola steganographica, VII). I do not believe anything else should be attributed to him except the invention of a system of secret writing in which the letters are replaced by words chosen so as to form, when they are joined together, a missive or a prayer, under the appearance of which it is impossible to suspect the existence of a secret message (imitated in the Cryptographieof Du Carlet, 1644). He thereby realized the great dream of his time, the modussinesecretisuspicionescribendi. I do notsee therefore by what right the Germans and others have proclaimed him the father of modern cryptography.

It seems to me that this title can only belong to Porta (1540-1615), the inventor of the first double key literal system, and I believe I render unto Caesar that which belongs to Caesar in associating with the name of the Italian physician that of a French diplomat, Blaise de Vigenère (1523-1596), who was the first to explain, in his Traité des chiffres, the operation of the square cipher, as it has been used for three centuries.

(13) De furtivis litterarum notis, vulgo de ziferis. Naples, 1563.

(14) Traicté des chiffres, ou secrètes manières d'escrire. Paris, 1586.

(15) See Klüber, Kryptographik, p. 122.

(16) Memoire of Beguelin, Academy of Sciences and Belles-Lettres of Berlin, vol. XIV, p. 369.

(17) See Klüber, loc.cit., p. 79.

(18) Besides the authors already cited, one may also consult: Hanedi, Steganologia et stenographia nova (German text), Nuremberg, 1617; Seleni, Cryptomenytices et cryptographiae libri IX, 1624; Frederici, Cryptographia oder Geheime correspondentz, Leipzig, 1685; the article "Cypher" in the Encyclopedia of Rees, 1819; the article "Cryptography" in the Encyclopedia Britannica, 1877; Lacroix, La Cryptographie, ou l'Art d'écrire en chiffres, Paris, 1858.

(19) Since we already have the terms cryptography, cryptographic, cryptogram, and cryptograph, it should be permissible to complete the series of compounds with the adoption of the verb to cryptographize.

(20) The letters that occur most often in German are, in order of their frequency: E, N, i, r, s, t, u, a, h. In English, they are: E, T, a, o, n, i, r, s, h, d, l.

(21) The first treatise on cryptography in which the principles of decryptment are mentioned is due to Porta; it is the book that I have mentioned above: De furtivis litterarum notis.

The principal works that have treated the same subject are, in chronological order: L'Interprétation des chiffres, taken from the Italian of Cospi, by F. I. F. N. P. M. (Father Nicéron), Paris, 1641; Gravezande, Introduction à la philosophie, Leyden, 1737, chap. XXXV (This chapter has often been reproduced, and can be found, among others, in the Dictionnaire encyclopédiqueof Diderot and in the Cryptographieof Lacroix); Breithaupt, Ars decifratoria sive occultas scripturas solvendi et legendi scientia, Helmstadt, 1737; John Davys, An Essay on the art of decyphering, 1737; Conrad, Cryptographia denudata, sive ars deciferahdi, Leyden, 1739; Thickenesse, A treatise on the art of decyphering, 1772; Klüber, Kryptographik, Tubingen, 1809; Vesin de Romanini, La Cryptographie dévoilée, Paris. 1857; Kasiski, Die Geheimschriften und die Dechiffrirkunst, Berlin; 1863; Fleissner von Wostrowitz, Handbuch der Kryptographie, Vienna, 1881. One can also read to advantage chap. XV of the Scarabée d'or, the Escritures secrètes dévoilées, by Charles Joliet, as well as an excellent article by Prodhomme in the Dictionnaire des connaissances humaines by Lunel.

(22) Tactique des renseignements, p. 76.

(23) Since the telegraph administration counts secret messages by groups of five, breaking up into pentagrams is preferable.

(24) There is every probability that the Minister of Posts and Telegraph willnot delay in applying to domestic service the principles of the international

convention of London, according to the terms of which the simultaneous use of letters and numbers is excluded from secret language.

(25) I say literal, that is, based on the use of letters, because Tritheim had already thought, fifty years before, of employing series of words and phrases to correspond to the letters of the plaintext.

(26) De furtivis litterarum notis, bk. II, chap. 16.

(27) M. Fleissner attributes the invention of this system to Napoleon I; this is not the only historical or bibliographical error with which the Austrian writer is to be reproached.

(28) See p. 50, b.

(29) Father Kircher (Polygraphia nova et universalis; Rome, 1663) replaced the letters of the Vigenere tableau with numbers, whence the name Abacus numerails given to his system. Only, instead of writing the cryptographic text in the ordinary way, Kircher takes any page of writing and indicates the numbers of the cryptogram by dots placed under the letters, at intervals corresponding to the value of the numbers obtained. Schott commented on Father Kircher's system in his Schola stenographica: because of this, many authors, Larousse among others, have attributed the invention of it to him.

(30) A description of this system is also found in Bartels, Leitfaden für den Unterricht auf den königlichen Kriegsschulen; Berlin, 1881.

(31) A Berlin firm (Egert, 62 Kochstrasse) has manufactured a mechanical apparatus for cryptographizing with this system.

(32) We shall see further on that if the correspondents followed this recommendation to the letter, it would require scarcely half an hour to decipher without a key any cryptographic message using this system.

(33) When the alphabet is "reversed" (see further on), the St. Cyr system gives a different text.

(34) Cf. Colorni, Scotographia, overo Scienza di scrivere oscuro, Prague, 1593.

(35) It is probable that the English admiral himself never believed in the possibility of transforming his system into an ordinary square cipher; one cannot explain, otherwise, why Mr. Morris Beaufort still claims energetically at this moment, for his illustrious father, the honor of having presented his country with an indecipherable cryptographic system (Cryptography, a system of secret writing, by the late admiral Sir Francis Beaufort).

(36) Les systèmes télégraphiques aériens, électriques, pneumatiques; Paris 1876, p. 261.

(37) In a lecture given in 1873 in the Société des Sciences militaires of Vienna, Dr. Orges maintained that this cipher had been invented by General Trochu (see Fleissner, loc.cit.,p. 19).

(38) Die Geheimschriften und die Dechiffrirkunst.

(39) Colonel Fleissner (Handbuch der Kryptographie) had adopted, without any modification, Major Kasiski's method of decryptment.

(40) I quote from the translation of Père Nicéron.

(41) By cryptographizing this sentence 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 one would have none witha key of 11, 14 or 18 alphabets.

(42) I do not need to point out that it may very well happen that two similar bigrams (with a trigram it is quite rare) may be produced by two different groups of letters.

(43) A German author, Krohn (Buchstaben- und Zahlensysteme für die Chiffrirung von Telegrammen, Berlin, 1873), did not have a clear idea of this principle, and he composed, for use in cryptographic correspondence, a dictionary containing 3,200 alphabets; it is, at the same time, too much and too little.

(44) Since the first alphabet in the Gronsfeld system is represented by zero, it is necessary to decrease the order number of each alphabet by one.

(45) When the decrypter knows that a text in a foreign language has been cryptographized in this way, he does not have to worry, for the success of his work, about whether he understands the language or not: it is enough for him to learn what letter in that language appears most frequently (see p.12).

(46) M. Auriol (Manuel de la correspondence secrète, postale ou télégraphique, Paris, 1867) has published a tableau that permits enciphering the plaintext letters two at a time. Leaving aside the fact that one can perform on combinations of letters the same calculation as on letters taken singly, the system leaves itself too open to tentative assumptions, and moreover requires absolute secrecy.

(47) It matters little, and this is an essential point to be noted, that the order of succession of the letters in the vertical columns should be the same as in the horizontal rows; this order is generally only observed in order to permit the correspondents to establish their tableau from memory more easily.

(48) The reader will not grasp well what is said here about the application of the principle of symmetry of position unless he sets up for himself on a sheet of paper a tableau with the normal alphabet at the head, leaving blank spaces for eight alphabets (1, (2, 4, 6), 3, 5, 7, 8, 9, 10), spaces that he will fill as we proceed.

(49) In case of unforeseen difficulties, one tries out each of the 26 letters of the alphabet.

(50) The simultaneous employment of the two cryptographic procedures will not excuse the correspondents from changing the key for each message.

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

(52) Dictionnaire abréviatif chiffre, Paris, 1868.

(53) Dictionnaire pour la correspondance télégraphique secrète, par un secrétaire de légation, Paris, 1868.

(54) Dictionnaire télégraphique économique et secret, par Mamert-Gallian, Paris, 1874.

On the same principle are based the German dictionaries of Niethe (Berlin, 1877) and Walter (Winterthür, 1877), as well as that of Bolton for English correspondence.

M. Louis, a director of the Journal des Postes, has likewise published a Dictionnaire pour la correspondance secrete, containing more than 20,000 words,

(55) In the category of cipher dictionaries is placed the system that consists of replacing the most important words of the correspondence by other words, whose usual meaning is ignored. This procedure has been used quite often, but it is practical only in exceptional circumstances. In the correspondence relating to the plot organized in 1831 by the Bonapartist party is found a

piece, written in the hand of Prince Louis-Napoleon, which contains a list of code words used by the conspirators to designate the persons or things that had to be referred to most often: Queen Hortense was designated by M. Antoine, Prince Louis-Napoleon by Mme. Charles, England by Mme. Lirson, the Bonapartists by Mme. Gock, the army by Mlle. Amélie, the police by M. Pamberg, etc. (See Mémoires de Gisquet, former prefect of police; 1840, p. 351).

(56) See Schott, Schola steganographica, p. 27.

(57) 3rd edition, vol. III, p. 529.

(58) Kzirh is nothing else but Paris, written with the alphabet reversed.

(59) See Du Moncel, loc. cit.

(60) For private reasons, the apparatus has not been able to be put on sale, but one can see copies of it in the shop of M. Luard, sheath-maker, 16 Dauphine St.

(61) Cf. Bontemps, Les systèmes télégraphiques, p. 257; Du Moncel, Exposé des applications de l'élecricité, bk. III, p. 532.
Wheatstone deciphered, in 1858, several very interesting letters of Charles I, entirelywritten in Arabic numbers (See Report of the Royal Commission on Historical Manuscripts, 1870).

(62) La cryptographie, contenant une très subtile manière d'escrire secrètement , composes par maistre Jean Robert du Carlet; 1644.