FOR OFFICIAL USE ONLY.

NOTE.

The information given in this book is not to be communicated, either directly or indirectly, to the Press, or to any person not holding an official position in His Majesty's Service.

MANUAL

OF

CRYPTOGRAPHY.

PREPARED BY THE GENERAL STAFF,

WAR OFFICE

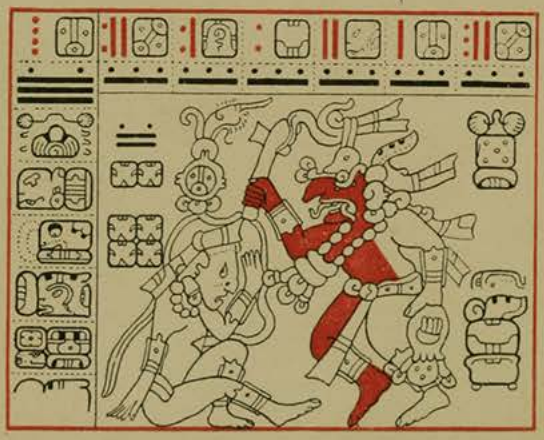
W. F. Friedman
1st Lieut. M. I. D.
G2-A6-GHQ AEF
1919

Umol-huun tah-tiyal

William Frederick

yetel

Elizebeth Smith Friedman



Lay ca-huunil kubenbil tech same.
This our book we entrusted you a while-ago.
Ti manaan apaclam-tz'a lo toon
It not-being you-return-give it us,
Epahal ca-baat tumen ah-men.
Is-being-sharpened our-axe by the expert.

I think this is the only copy in the United States - or maybe in the Western hemisphere, or maybe in the whole world!

[N.D. but this manual was printed in 1911]

The
GEORGE C. MARSHALL RESEARCH
LIBRARY

LEXINGTON, VIRGINIA

WILLIAM F. FRIEDMAN COLLECTION

Manual of Cryptography.

CORRIGENDUM.

Page 32.—The second or lower set of columns of letters should read as printed below—

N	K	E	O	P	I
J	M	I	J	E	B
F	B	N	O	N	A
L	G	A	Z	D	M
Y	Z				

(B63) 950 2/12 H&S 73wo

[FOR OFFICIAL USE ONLY.]

MANUAL

OF

CRYPTOGRAPHY.

PREPARED BY THE GENERAL STAFF,

WAR OFFICE

(B364) 200 10/14 H&S 1139wo

LIST OF WORKS CONSULTED.

Handbuch der Kryptographie. Eduard B. Fleissner von Wostrowitz, K. K. Oberst. Seidel and Son, Vienna, 1881.

De la Cryptographie. P. Valério, capitaine d'artillerie. Librairie Militaire de L. Baudoin. Paris, 1893.

La Cryptographie Militaire. Aug. Kerckhoffs. Librairie Militaire de L. Baudoin. Paris, 1883.

La Cryptographie et ses applications à l'art militaire. H. Josse, capitaine d'artillerie. Librairie Militaire de L. Baudoin. Paris, 1885.

Cryptographie. Le Marquis de Viaris, ancien officier de marine. "Le génie civil," 6, rue de la Chaussee d'Antin. Paris, 1888.

Traité élémentaire de Cryptographie. F. Delastelle. Gauthier-Villars. Paris, 1902.

CONTENTS.

DEFINITIONS.

CRYPTOGRAPHY is the art of writing a communication in ordinary language (commonly called the "text") according to an agreed system, so that it can be understood only by those who are acquainted with the method employed.

A CRYPTOGRAM is a communication so written.

TO ENCIPHER a communication is to write it out according to the agreed system, thus forming a cryptogram.

TO DECIPHER a cryptogram is to reconvert it into ordinary language by knowing the system employed, and, if necessary, the keyword.

TO SOLVE means to discover the true meaning of a cryptogram without such knowledge of the system and keyword.

TO CODE a communication is to substitute for the ordinary language the conventional words or figures given in the code book used.

TO DECODE is to reconvert such a communication into ordinary language by help of a similar code book.

"IN CLEAR" is the technical term for a communication written in ordinary language.

A CONVENTIONAL or arbitrary alphabet is one in which the letters are arranged in other than the usual order.

KEYWORD (used in many systems) is a word, the knowledge of which is necessary to encipher or decipher a message.

MANUAL OF CRYPTOGRAPHY.

CHAPTER I. (HISTORICAL AND GENERAL.)

The necessity of some means whereby secret correspondence can be carried on between the Government or directing authority at home and the commander of an army in the field, or between commanders of constituent parts of an army, has been recognized from the earliest times. Different methods, varying considerably in ingenuity, have been employed from time to time.

At first these consisted chiefly of various mechanical devices; for instance, when the Spartan Ephors wished to send instructions to their commanders in the field, they wound a narrow strip of parchment slantwise round a staff, known as a "scytale," so that the edges lay close together, and then wrote the message along the joint. The writing was in this way cut throughout its length by the edges of the parchment, and the strip when unwound presented a series of broken letters on each edge. The intention was that the message should be illegible until it reached the hands of the commander for whom it was intended, who, on winding it round a staff of exactly the same size, was able to read the orders conveyed. It is evident that such an elementary device could have afforded only temporary security, and might have been discovered by the exercise of a little ingenuity.

Grecian history furnishes an account of another stratagem used to carry on secret correspondence. A Greek at the court of the Persian King, Darius, wishing to send important information to a colleague, Aristagoras, in Greece, shaved the hair from the head of a young slave, and had the message pricked in with ink on his bare head; after the hair had grown again, the boy was sent to Aristagoras with instructions to inform him of the procedure adopted.

From the earliest times various contrivances have been used to convey information in war, for example, bundles of ribands of different colours, notches on a stick, knots tied in various ways. Fires or beacons have been employed by all the nations of antiquity, and Polybius describes a system employed by the Greeks, whereby different letters were signalled by means of beacon fires. The letters of the alphabet were divided into groups of 5, and the number of fires lit in two separate places denoted the group of letters and the position of the letter in that group. Fires were made use of as late as the year 1746 in Italy to signal messages; the code for this purpose which was given to General the Marquis de Mirepoix, then in command of the mixed corps of French, Spanish, and Genoese troops, is still in existence.

At the present day, in many of the less developed portions of Africa, events are announced and news conveyed by the beating of drums. Only chiefs of tribes and headmen are initiated in this system of communication, and to the bulk of the native population

messages sent by such means are quite unintelligible. A French traveller who had studied the subject writes that this form of the musical art seemed at first hearing to be limited to the performers making as much noise as possible, but that after a time "*on distingue dans cette cacophonie infernale un certain rythme et une certaine mesure.*"

The earliest authentic cipher system employed during military operations, of which there is any account, is the co-called Julius Cæsar cipher. In one form of this cipher each letter of the text is replaced by the letter which stands a certain agreed number of places before or after it in the alphabet, while in another variation a conventional alphabet is used, *see* page 29. The invention of this system, which is known by different names in different countries, has been attributed to Julius Cæsar, but it was used many centuries earlier by both the Carthaginians and Phœnicians. With various modifications this cipher continued in use for hundreds of years, and variations of it were employed by the Germans in 1870–71 and by the British forces during the South African war.*

For many centuries after the Roman invasion of Britain cryptography was almost entirely neglected, one reason being that the art of secret writing was for long regarded as an invention of the Evil One. There are many instances of students of it being accused of sorcery, among whom may be mentioned Trithème,† the Abbé of Spanheim, who tried to revive the study of cryptography, and to this end about the beginning of the 16th century wrote a book on the subject, but, his contemporaries being unable to follow his methods or to understand the terms employed by him, he was found guilty of witchcraft. It was therefore considered safer to correspond on dangerous topics in plain language and to take the risk of the correspondence being intercepted, than to court greater danger by employing a system of secret writing.

This attitude towards ciphers survived until the 16th century, and an incident which occurred in the reign of the French King, Henri IV., shows the perilous position of experts in cryptography even some years later. Henri IV. intercepted correspondence which was passing between the Court of Spain and the chiefs of the Anti-Royalist party in France. The documents were in cipher and were handed to a celebrated French mathematician, named Viète, to unravel. He discovered the system employed to be a conventional alphabet expressed by 50 different signs, and was soon able to furnish the King with the message "in clear." As soon as the Spaniards heard of the incident they accused the Court of France of having the devil in its employ and denounced Viète as a sorcerer before the ecclesiastical tribunal at Rome. Viète was, however, eventually able to clear himself of the charge by explaining his methods.

---

* The Wolseley or Soudan cipher is a form of conventional alphabet cipher, *see* page 30.

† Trithème (Tritheim) invented the earliest known cipher system, whereby the letters of the message were not always represented throughout the despatch by the same cipher letters. This form of cipher is now known as the multiple alphabet or complex cipher.

The only cipher systems known to have been employed between the time of Julius Cæsar and the beginning of the 16th century, of which we have details, are two systems mentioned by a Frenchman, Raban Maur, who lived in the 16th century.

In the first of these systems the vowels are represented by dots, as follows :—

i = . a = : e = : . o = : : u = : . :

According to this system the words "The town capitulated" would be represented thus :—

Th : . t : : wn c : p . t : . : l : t : . d

In the other system also the consonants remain unaltered, but each vowel is represented by the consonant which immediately follows it in the alphabet.

Neither of these systems could be expected to cause much delay or to be otherwise effective. They are of interest, however, as showing that reliance has been placed at different periods on methods which give no real security. This is a point to which further reference will be made, for it is of the highest importance that systems should not be employed in war which, while appearing at first sight insoluble, are not in reality capable of withstanding the organized efforts of a body of experts.

From the 16th century onwards cryptography became an important factor in military and diplomatic correspondence, and the necessity of some means of carrying on secret correspondence was urgently felt, owing to the intrigues which were characteristic of the time and the risks to which messengers even of high rank were often subject. Many cipher systems were invented and eminent men in different countries employed special tables and alphabets of their own. Among many others Lord Bacon, Richelieu and Louis XVI. are known to have enciphered part of their correspondence, but the systems they employed were not capable of resisting careful investigation.

The following device was employed by Richelieu. In a card, a facsimile of which must be in the hands of the person to whom the message is written, holes are cut irregularly in various places. The card is placed on a sheet of paper and the message written through the holes. Thus there are at first only a few disconnected words on the paper. The plate is then removed, and it is left to the ingenuity of the writer to fill in the lines so as to read naturally, though in a sense different from that of the real message.

In the following message the words in *italics* constitute the message, and the remainder is merely padding, "Si *vous* pensez que vous *n'avez* presque *rien* de sérieux *à* faire, envoyez-moi des blés sans *craindre* le prix. *Entrez résolument* dans votre rôle et *dans* l'esprit de la coutume qui veut qu'un marchand sache dépenser de l'argent au bon moment, à fin de profiter de *la* hausse qui ne manquera pas de se faire sentir bientôt en votre *ville*." The recipient of the message on placing his card over this document would see only the original message.

Another example of this type of secret communication is the following letter, which was written by Cardinal Richelieu to the French Ambassador at Rome. It will be seen that the meaning of the left half of the letter, the true one, is exactly the converse of the sense of the whole; the true significance of the message is obtained by reading the left half of the letter only, while exactly the opposite meaning is conveyed if the letter is read through in the ordinary manner:—

M. Compigne, Savoyard de naissance, frère de l'ordre de Saint-Benoit,
est la personne qui vous présentera cette lettre comme un passe-port pour arriver à votre protection;
C'est l'homme le plus discret, le plus sage et le moins
médiocre que je connaisse, et avec qui j'ai eu le plaisir de converser;
il m'a longtemps sollicité de vous écrire en sa faveur, et
de lui délivrer un certificat convenable ainsi qu'une lettre de crédit,
ce que j'ai enfin accordé à son mérite réel plutôt qu'à son
importunité, car, croyez-moi, Mr., sa modestie n'est surpassée que par son mérite;
je serais fâché que vous fussiez dans le cas de négliger de lui rendre service, faute
de méconnaître son caractère réel, je serais faché que vous fussiez
comme l'ont été quelques-uns de mes amis intimes, induit dans une erreur qu'ils reconnaissent.
Je crois de mon devoir de vous prévenir que vous me ferez un sensible plaisir
de porter une attention particulière à tout ce qu'il fera, et de lui témoigner tout le respect possible,
et de ne pas vous hasarder à rien dire en sa présence qui puisse l'offenser ou lui deplaire
en aucune manière; je puis dire qu'il n'y a personne que j'aime autant que M. Compigne,
personne que je regrettasse plus de voir négligé, parce qu'il n'y a personne plus digne d'être
reçu et admis dans la bonne société, il serait donc odieux de lui manquer
et je suis persuadé qu'aussitôt que vous connaîtrez ses vertus et que vous
l'apprécierez tel qu'il est réellement, vous l'estimerez comme je fais, et alors
vous me remercierez de mon avis; la confiance que je mets dans
votre obligeance me force de m'abstenir de m'étendre davantage sur cette matière, ou
de rien dire de plus à ce sujet. Croyez-moi, Mr., &c.

Richelieu.

The above system of secret communication is interesting, though of no value for military purposes, for it demands more than ordinary ingenuity and literary ability, even if it should be possible to treat a military despatch in such a manner.

One of the earliest instances of the advantage gained in the course of military operations by the capture and subsequent solution of a message sent by the enemy took place in the year 1626. It occurred during the siege of Réalmont, a town of Languedoc, then in the possession of the Huguenots, but besieged by the King's troops under the command of the Prince de Condé. The garrson made such a determined resistance that the Prince was on the point of raising the siege, when a cipher message, which had been sent from the town, was intercepted.

For a long time the cryptogram baffled the efforts of the military men who tried to decipher it, but being handed over to a certain Antoine Rossignol, an expert in cryptography, he in a short time produced the message written "in clear." It proved to be a letter to the Huguenots of Montauban, informing them that the garrison had almost run out of powder, and that, if a further supply were not immediately sent, the town would be compelled to surrender.

The Prince de Condé, who was not without a sense of humour, sent the cryptogram together with the message written out "in clear" to the commander of the garrison, enclosed in a letter in which he stated that if the message really indicated the state of affairs in the besieged town, it hardly appeared worth while continuing the struggle and putting both parties to further inconvenience. The commander of the garrison apparently saw the force of the argument, for the town capitulated without further ado. When it is considered that a relieving party had actually set out, with supplies of food and ammunition for the garrison, it will be realized how important was the timely assistance of M. Rossignol, and how great a danger is incurred if important military despatches are enciphered on an insecure system.

It is unnecessary here to endeavour to trace the various systems which were invented during the 18th and 19th centuries, but it is recorded that during the operations in the Peninsula a code known as Marmont's Figure Code was employed by the French. This is a short code in which important names, military terms, and numerals are represented by groups of 2 or 3 figures. The letters of the alphabet are represented either by single figures or pairs of figures, and, in order to obtain greater security, from 2 to 5 alternate pairs of figures are allotted to letters which occur frequently (*see* page 91).

The absence, however, of a sufficient number of trained staff officers in Napoleon's Army often prevented the effective exchange of secret correspondence and indeed at times necessitated important despatches being sent "in clear." For instance, in 1807, when the Russian Army in Eastern Prussia was about to be drawn into a dangerous position by the strategy of Napoleon, the Duc de Fezensac, who was bearer of despatches to Bernadotte, was captured by some Cossacks. The despatches, which were not in cipher, contained a

detailed description of the positions of the French Corps and the manner of their intended employment by the Emperor. They were at once sent to the Russian Commander, who, warned of the danger he ran, retired to Eylau.

The French did not profit by this dearly-bought experience, for in 1814 when Napoleon wished to concentrate various French forces, both from abroad and from distant parts of France, his staff officers, Feltre and Berthier, were compelled to send the necessary orders "in clear," for at the time no cypher system was in use in the army. Again, a short time before Waterloo, Davoust, who was then War Minister, had to ask the Foreign Minister to furnish him with cipher tables for the use of the Army.

An instance of the disastrous consequences of neglecting to encipher important despatches occurred during the American Civil War while the battle of Gettysburg was in progress.

There is reason to believe that on the evening of the second day of the battle General Meade, the Federal commander, had decided to retire from the Gettysburg position and had even caused the order for retreat to be prepared, when a cavalry officer, Captain Dahlgren, arrived with a captured despatch. It had been written by President Davis to General Lee, and informed the latter that it was impossible to assemble an army under Beauregard at Culpeper to threaten Washington as he wished. Meade, thus assured that no Confederate force threatened Washington except that immediately in his front, thereupon decided to maintain his position at Gettysburg. If the above despatch had been even in some simple form of cipher, so that two or three hours must have elapsed before it could be understood, the Federal retreat would probably have been carried out and the whole course of the operations changed.

The Franco-German War furnishes many instances of the danger of not having some secure means of secret communication between the different parts of an army in the field. Thus, when the 3rd German Army reached the banks of the Meurthe during the 15th and 16th August, its headquarter staff at Lunéville did not know the exact position of the 5th French Corps, and it was thought that the French troops were continuing to retire on Châlons in order to concentrate. On 17th August a party of German cavalry captured a French orderly in Commercy, and the despatch he was carrying, which was not in cipher, contained information on the following points :—The presence at the camp of Châlons of the cavalry of the 6th Corps ; the calling out of all men between the ages of 25 and 35 ; the formation of the 12th and 13th Corps under Generals Trochu and Vinoy respectively ; and the retreat of the 1st and 5th French Corps.

The above examples taken from history show that the necessity of some means of secret correspondence in war time has always been recognised, and that failure to encipher despatches has sometimes led to serious consequences.

In modern times the multiplication of the means of communication in the field, such as telegraphs and telephones, signalling by flags, heliographs and lamps, and wireless telegraphy, have rendered the

necessity of some safe means of correspondence of vital importance. The difficulty, however, of finding a secure system has increased in proportion to the need, for the study of cryptography has progressed to an extent which makes it difficult to devise a cipher system not generally known, and of which the weak points have not been discovered by the long-continued efforts of expert decipherers. It was for a long time considered even by men who had studied the subject that certain systems in vogue both in this country and abroad afforded security for all practical purposes. For instance, at a time when much attention was paid to the solution of cryptograms, Voltaire, in an article on the subject of cipher messages, expressed the opinion that people who boasted of their ability to read secret messages without knowing the keyword and the system employed were mountebanks and liars, in the same degree as men who boasted of their ability to understand a language which they had never studied. General Lewal, in his "Etudes de guerre," published in 1881, has written that "Cryptograms formed on the 'sliding alphabet system,' when several alphabets are employed, are, as a rule, insoluble, or, at least, their solution presents enormous difficulty." It is now known, however, that a cipher message of any length formed on this system can usually be solved.

In England a similar mistake has been made, and the point is alluded to by various French writers on cryptography. A "Beaufort cipher" was invented in 1857 by the late Admiral Beaufort, and several persons claimed that cryptograms formed on this system were absolutely insoluble. French critics of the system, however, have shown that the Beaufort system is practically identical with the system known in various countries by the following designations:— Sliding Alphabet Cipher, Tableau de Vigenère, Système de St. Cyr, Tableau de Porta, which systems are not now considered to afford a great measure of security.

It is now recognized that most cipher messages of any length can usually be solved if time is available for investigation by experts.

CHAPTER II.

EXTENT TO WHICH OFFICERS NEED STUDY CRYPTOGRAPHY. GENERAL CLASSIFICATION OF MEANS OF SECRET COMMUNICATION. CONDITIONS WHICH MILITARY CIPHER SYSTEMS SHOULD FULFIL. GENERAL RULES TO BE OBSERVED WHEN ENCIPHERING AND DECIPHERING. CHOICE OF KEY-WORDS.

While a general knowledge of cipher work is useful to every officer, it is not necessary that all officers should enter deeply into the study of cryptography. The subject is one to which much time and labour must be devoted if a high degree of proficiency is to be attained. In the first place a prolonged study of the peculiarities of different languages is necessary, and also of the different cipher systems which have been employed from time to time in various countries. Moreover, in order to become an expert (that is to say to be able to solve cryptograms without knowing the system or the keyword employed), in addition to previous study certain natural qualities are necessary, such as a quick intelligence, the faculty of analysis and the dogged, untiring patience which enables a man to return to the attack by different methods until he finds that he is on the road towards a solution of the problem. It is also essential to possess the instinct or "*flair*" which guides a skilful operator to discard improbabilities and limit the field of his labours, while omitting nothing from which a useful deduction may be made.

During the evolution of the science of Cryptography a large number of different systems were introduced, of which typical examples are given in Chapter III., while descriptions of less important or less reliable systems employed from time to time in different countries will be found in Chapter V. It is not necessary that officers who do not desire to become experts in the subject should study the latter class, but it is desirable that all officers should be familiar with the systems described in Chapter III. and should practise enciphering and deciphering messages by the most important of them, and should also follow carefully the solutions described in detail in Chapter IV.

There is a tendency on the part of those who have not made a study of Cryptography to over-estimate the security of various systems and to regard a cryptogram as insoluble, merely because the system on which it has been formed is not at first sight apparent. Such a cryptogram might not, however, be proof against the efforts of an expert for sufficiently long to cause any material delay, for by applying a series of previously thought-out tests on systematic lines he would soon discover the system employed.

Codes and Ciphers.—Military cryptograms may be divided into two main classes, Codes and Ciphers. Codes will first be considered, but as they do not fulfil the conditions required of a means of secret communication in the field, they need not be dealt with here at length.

They are the usual means for diplomatic and commercial correspondence, on account of their economy, secrecy and simplicity. Codes are conventional dictionaries, in which combinations of letters or figures are allotted to words and phrases likely to be required, and provision is made for spelling words not included in the code. In order to communicate by this method each correspondent must have a code-book, but as for obvious reasons a wide distribution of such books is, during military operations, undesirable, it is improbable that this means of correspondence would be available to commanders of units smaller than divisions and cavalry divisions. If code-books were distributed more widely, the possibility of loss or capture would be greatly increased, for in the event of the defeat or capture of a small unit, the code might fall into the hands of the enemy before it could be destroyed. It is unnecessary to describe the method of using the various codes at present in use, for the books contain full directions, so that they can be used without any previous instruction or practice.

The general use of codes is due to the following advantages :—

(1.) The operations of coding and decoding can be done with ease and rapidity.

(2.) The security afforded may be regarded as absolute, unless the code is lost, stolen or captured, or until it has been in use for so long a time that the enemy may have become familiar with it by intercepting a large number of messages.

(3.) The comparison of one message in code and in clear does not necessarily assist the reading of another message in the same code.

(4.) Codes are economical, for in most cases the message when coded is shorter than the original text.

Codes, in a greater degree than ciphers, are subject to the disadvantage that a mistake may obscure or even seriously alter the meaning of a message, while if one copy of the code-book be lost the code can never again be employed with safety.

Very serious trouble may also result if a correspondent has not the code-book at hand to code or decode a message. This is illustrated by an incident which occurred during the Franco-Prussian War. On the 23rd August, 1870, the Commander of the French Territorial Division at Châlons telegraphed to the War Minister in Paris as follows :—" By mistake my code-book has been sent with the rest of my office papers to Château-Thierry. Impossible to decode your despatch; Please send the message in clear before 8 a.m. to-morrow, at which hour I start for Rheims, in compliance with orders of Marshal MacMahon." At least one similar accident occurred on the side of the Germans : a telegram was sent from the Prussian General Staff to General Werder on 8th January, 1871, which the latter was unable to read because his code-book was packed in a wagon which had not accompanied him.

Necessity for cipher systems.—As code-books will probably not be issued to commanders of small units, some form of cipher will often be necessary for the purpose of secret communication in the field. Such communications might be necessary between the commander-in-chief and commandants of fortresses, commanders of columns and detachments, chiefs of administrative services—such as railways, posts, telegraphs—and agents in foreign countries. Objections have been made to the use of cryptograms on the grounds that their employment causes delay, that serious mistakes may occur when they are used by officers unaccustomed to them, and, lastly, that any cryptogram may be solved if time is available.

Although this last statement may be true, the use of cipher is still of great value, for if a sound system be employed and the keyword be frequently changed, the enemy cannot solve the cryptogram without considerable delay, and delay in military operations may be of decisive importance.

Transpositions and substitutions.—Cipher systems may be divided into two main classes—

(1.) *Transposition ciphers*, in which the words or letters remain the same, but their order is changed.

(2.) *Substitution ciphers*, in which other letters are substituted for the letters of the text.

Substitutions of other words or groups of figures for the words of the text are termed codes, which have been already dealt with.

Transposition ciphers.—Of the above ciphers Class 1, or Transposition Ciphers, may be subdivided into word transpositions and letter transpositions. Of the former type, or word transposition, the only system which has been practically tested in war is the Federal Army Cipher.*

Letter transposition ciphers, or "anagrams," as they are sometimes termed, are systems in which the letters are not altered, but their order is changed. The simplest form of anagram is to write the letters backwards; thus the word ALDERSHOT becomes TOHSREDLA.

There are many other simple ways of changing the order of the letters, one of which is to write them out in columns vertically and to read them off in columns horizontally. Thus the words "the enemy attacked at dawn" might be written out—

T	E	T	D	W
H	M	A	A	N
E	Y	C	T	X†
E	A	K	D	Y†
N	T	E	A	Z†

and the cryptogram be read off in horizontal lines, thus:—

TETDWHMAANEYCTXEAKDYNTEAZ.

Systems of this nature are the Hebrew Transposition Cipher (page 21), Zig-zag (page 21), Diagonal (page 79), Nihilists' Cipher (page 26), and many others.

---

* *See* page 27. † Dummy letters to complete last column.

Substitution ciphers.—In letter substitution ciphers other letters are substituted for the letters of the text either singly or in pairs.* Cæsar's Cipher is a type of substitution by single letter (*see* page 28), and the Playfair Cipher is an example of substitution by pairs of letters (*see* page 37). It will be seen, when the Playfair Cipher is explained in detail, that systems of this nature have a great advantage as regards security over single-letter substitutions.

The latter class may be subdivided into :—

(*a.*) Single alphabet ciphers, in which so long as the key remains the same, each letter of the text is represented by the same letter in cipher. Thus, each letter of the text might be represented by the letter which stands fourth after it in the alphabet :—

M A R C H A T D A W N
q e v g l e x h e a r

A being taken as the next letter after Z. Such systems afford little or no security.

(*b.*) Multiple alphabet ciphers in which, though the keyword remains the same, each letter of the text may be represented on different occasions by different cipher letters.

The Sliding Alphabet cipher (*see* page 32) is an example of the Multiple Alphabet cipher. Systems of this nature afford a considerable degree of security, unless long messages or a number of shorter ones are enciphered with the same key, for, with a sufficient amount of material to work upon, cryptograms formed on such systems can usually, in course of time, be solved.

The substitution of pairs of cipher letters for pairs of original letters of the text is a comparatively recent innovation, and the best-known system of this nature is the " Playfair cipher," which affords great security.

Conditions which Military Cipher Systems should fulfil.

Ciphers intended for use in the field must conform to certain conditions as regards security and practicability of working under service conditions. These conditions are :—

(1.) Security.
(2.) Suitability for transmission by signal or by telegraph.
(3.) Absence of written tables or notes.
(4.) Knowledge of keyword, as well as of the system employed, necessary to solution.
(5.) A simple method of working not requiring much previous practice.

(1.) The most essential condition which a military cipher system should fulfil is security—that is to say, comparative security, for a message enciphered on any system which is sufficiently simple to

*Systems in which the letters of the text are represented by digits are of no practical value for military purposes in the field. As there are only 10 digits and 26 letters in the alphabet, it follows that most of the letters must be represented by more than one digit, and the cipher would thus be longer than the original text. Moreover, the signalling of the digits by the Morse alphabet is more complicated than that of letters.

be of use in the field can never be absolutely secure. A cipher can be made considerably safer by a frequent change of the keyword, for during military operations the danger lies in the fact that a cipher message may have been intercepted and the system discovered by the enemy without this being at once known throughout the area of operations. Consequently, later messages enciphered by the same system and with the same keyword might be at once read by the enemy.

It has already been stated that there is a tendency among those who have not made a study of cryptography to over-estimate the difficulty of solving a cryptogram merely because it presents a strange appearance and the system by which it has been formed is not at once apparent.

For example, the following groups of letters might at first sight seem difficult to understand :—

FOFNZ DPODF OUSBU JOHTF OESFJ OGPSD FNFOU T.

They represent, however, the words, "*Enemy concentrating. Send reinforcements,*" enciphered according to the most elementary form of the Sliding Alphabet cipher, each letter being represented by the letter following it in the alphabet, the letters being then arranged in groups of 5.

The following message sent by President Lincoln in November, 1862, to Major-General Burnside is an instance of the employment of an insecure cipher during military operations. The message is written backwards and the meaning is to a certain extent obscured by the introduction of bad spelling, the substitution of the word "flesh" for "meet," and so on. It probably did not take the Confederates long, if they intercepted the message, to discover its meaning :—

Washington,
November 25, 1862.

Burnside, Falmouth, Virginia. Can Inn Ale me withe 2 oar our Annpas Ann me flesh ends N.V. Corn Inn out with U cud Inn Heaven day nest Wed roe Moore Tom darkey hat greek a Why Hawk of Abbott Inn B chewed I if.

BATES.

The message, when read backwards and written out "in clear," read as follows :—

Washington,
November 25, 1862.

Major-General Burnside, Falmouth, Virginia. If I should be in a boat off Aguia Creek at dark to-morrow (Wednesday) evening, could you, without inconvenience, meet me and pass an hour or two with me?

A. LINCOLN.

(2.) The system must be suited to transmission by telegraph or signal—that is, both for purposes of economy and rapidity of transmission the cryptogram must not be much longer than the original.

The above condition precludes the use of such systems as Bacon's cipher (*see* page 86), by which the word "enemy" would in cipher be :—

AABAAABBAAAABAAABABBBABBB.

(3.) The system must not require written notes for its use, and any key employed must be easy to remember.

It has already been stated that a wide issue of code-books will not be made, owing to the possibility of loss or capture. For the same reason cipher systems, in order to be suitable for use in the field, must not require long lists of words, complicated tables or mechanical appliances, as in the various forms of Disc Ciphers (page 90), which involves the use of a disc or "cipher wheel," and the Stencil Cipher (page 80), which necessitates the use of a stencil plate.

(4.) The keyword must be necessary to the ready solution of a cryptogram, even though the system used may have been discovered. That is to say, it should not be sufficient to know that a particular system is being employed. A knowledge of the keyword should also be necessary in order to solve the message without great delay.

This condition is illustrated by the Sliding Alphabet cipher, used by the Germans in 1870. In this system a keyword is used, the letters of which regulate the employment of different alphabets (*see* page 32).

(5.) The method of enciphering and deciphering must be simple, *i.e.*, an officer should be able correctly to manipulate the message without an amount of experience which may not have been attainable. For this reason it should be possible to encipher and decipher a message by a single simple process. Almost absolute security could be obtained if a message were treated by a double process. For instance, the message might first be enciphered by the Playfair system, and the resulting cipher then treated by some transposition method. The cryptogram obtained would afford little or no material for solution, but the complicated double process, besides taking a great deal of time, might lead to frequent mistakes, and would therefore be unsuitable for military purposes.

Moreover, in order to ensure accurate results, the employment of a cipher system should not require uninterrupted work under such favourable conditions as are usually found only in time of peace. The staff officer, to whom a message is given to encipher or decipher, may have to work rapidly out of doors and under unfavourable conditions. Consequently it is of great importance that the system adopted should be simple to work, and such that with the exercise of ordinary care and intelligence reliable results may be ensured.

General Instructions regarding Enciphering and Deciphering.

1. No cipher message should ever contain words in clear or in code, but should be wholly in cipher with the exception of the name and address of the person for whom it is intended.* If the framework of a message is left "in clear" and only the important words are enciphered, it will probably not be difficult to guess these from the context, and to discover the system employed.

* It is not intended to prohibit the sending of messages of which one or more entirely independent paragraphs may be in clear while the remainder are in cipher. The intention is that the part of the message "in clear" should give no clue to the meaning of the part that is in cipher.

2. No information should ever be given in any clear or code message which might connect it in any way with a previously sent cipher message, nor should a cipher telegram be replied to in clear.

3. Ciphers or deciphers should never be written on the same sheet of paper as the original message, so that in the event of loss there will be less likelihood of the cryptogram being compared with the original message.

4. It is advisable that every cipher message should be checked before despatch in order to avoid errors. The best method, when the staff is available, is to hand over the message when enciphered to another person to decipher and then to compare carefully the decipher and the original message.

5. Reference to the transmission of messages in cipher should as far as possible be avoided in ordinary correspondence.

6. Care should be taken that no copy of a message which has been deciphered or of a message sent in cipher should be allowed to fall into the hands of unauthorized persons, nor should a copy of such message be shown or communicated to any person not in His Majesty's Service and duly authorized.

7. When cipher messages are to be telegraphed or signalled the letters should be arranged in groups of five.* It will be found convenient always to group cipher letters in this manner, for thcugh the enemy will not be deceived by the artificial grouping of letters,† yet if the letters indicate the real length of each word solution will be much facilitated.

8. The work of enciphering and deciphering should be done in an absolutely mechanical manner. Each letter or pair of letters should be treated separately, and when deciphering, no attempt should be made to make out the sense until the work is completed. Shortly after work is commenced, however, the results obtained should be considered in order to see whether the right method is being followed. This having been ascertained, the letter should be deciphered mechanically until the despatch is completed.

9. As soon as a message has been enciphered or deciphered all the papers used in the process must be immediately destroyed. If it is necessary to retain records, a paraphrase should be kept in which the wording is altered sufficiently to prevent a close comparison being made with the original. When paraphrasing a message a sentence may often be conveniently altered by using the active instead of the passive voice, and *vice versa*. If the exact wording of a particular phrase or sentence appears to be specially important the original words should be left unaltered. The beginning and end of a message require special attention, for these portions are generally first attacked when solution is attempted. The fact that the message has been thus paraphrased should be indicated by the prefixing of the letter "P" to the message, and no further allusion should be made to the fact that the original was transmitted in cipher.

---

* It is a useful precaution to commence each cipher message by a statement in clear of the number of such groups to follow, so that should a group be omitted during transmission, the error will be more readily observed.

† In the "Handbuch für Truppenführung und Stabsdienst" by Cardinal von Widdern, published in 1884, the Sliding Alphabet cipher is explained, and it is advocated that the cipher letters should be re-arranged in false groups in order to increase the difficulty of solution. Such a device would not be advocated at the present time.

The following is an example of a deciphered telegram and its paraphrase :—

Deciphered Telegram.

Chitral.—Your telegrams of the 18th and 20th April. I have no objection to your sounding the tribes as to the terms and conditions on which they would consent to opening up and maintaining Peshawar—Chitral road, should this road be hereafter decided on ; but I do not wish to be committed to the policy of the military occupation of Chitral or maintaining a British officer there permanently with or without support of this road, till Her Majesty's Government have had an opportunity of fully considering your detailed views and arguments on questions stated in my telegram of 19th April for your consideration.

Paraphrase.

(P) Referring to your telegrams of the 18th, 20th April, regarding Chitral. There is no objection to tribes being sounded by you as to the conditions and terms on which, if the Peshawar—Chitral road should be decided on hereafter, they would consent to its being opened up and maintained. I do not, however, desire to be committed to the policy of occupying Chitral with a military force or maintaining there permanently a British officer, with or without support of the Peshawar—Chitral road, until your detailed arguments and views on the points referred to you for consideration in my telegram of the 19th April, have been fully considered by Her Majesty's Government.

Choice of Keywords.

Though the suitability of a keyword is not of great importance to the security of a cipher system, for the determination of the keyword is generally the last step in the process of solution, yet the following considerations should be borne in mind when selecting a key.

(1.) The keyword should be easy to remember, so that it need not be committed to writing.

(2.) The word should be easy to spell and not capable of being spelt in more than one way.

(3.) In the case of transposition ciphers the keyword should be composed of letters well distributed through the alphabet. Thus "clique" would be a more suitable keyword than "abdicate."

(4.) In the case of substitution ciphers the keyword should contain as many different letters as possible in order to employ a large number of different alphabets ; thus "hieroglyphic" would be a more suitable keyword than "element."

When endeavouring to solve a cipher, the first efforts of the solver are generally directed towards determining the length of the keyword (*i.e.*, the number of different alphabets used). Various devices have been suggested in order to vary the length of the keyword, or a key of indefinite length has been proposed.* Such a procedure, however, adds considerably to the labour of ciphering or deciphering, and is apt to lead to mistakes.

* *See* page 34 (5).

CHAPTER III.

Typical Cipher Systems.

(*a.*) Transposition ciphers—Hebrew Transposition cipher—Zigzag Transposition cipher—Permutation cipher—Nihilists' cipher—Federal Army cipher (A).

(*b.*) Substitution ciphers—Cæsar's cipher—Wolseley or Sudan cipher—Sliding Alphabet cipher—Beaufort cipher—Playfair cipher.

A knowledge of the cipher systems described in this chapter, which exemplify the main principles of transposition and substitution, is sufficient for those officers who may be called upon to encipher and decipher messages in the field. Those who wish to study the subject more thoroughly will find in Chapter V. a description of other systems, which have been employed from time to time in Europe. An examination of these will show that some of them are unsuited to military use because they do not conform to the conditions laid down in Chapter II., while others are merely variations of some of the ciphers described in this chapter. For instance, the same result would be obtained by using the Sliding Alphabet cipher, the Tableau de Vigenère, the Tableau de Porta, or the Beaufort cipher, and consequently a description of only the first and last of these is given.

The best way of grasping the methods of enciphering and deciphering is to work out each example on a sheet of paper, and to compare it when completed with the result* here given.

(*a.*) Transposition Ciphers.

Transposition ciphers, which, owing to the greater attention now paid to the science, are no longer looked upon as sufficiently secure, will first be dealt with. These systems were formerly considered to afford great security, and a form of Word Transposition cipher, used during the American Civil War, proved very satisfactory* (*see* page 27). It is doubtful, however, if this would be the case in the future, for it is essential for military purposes that the system of transposition should be simple and straightforward in order to avoid errors and delay, and consequently the number of methods of transposition is limited, and the work of solution comparatively simple.

In Transposition ciphers the letters or words of the text are not changed, but their order is altered according to some pre-arranged plan. The most usual method is to rule the paper both ways so as to divide it into a certain number of spaces, each of which is to contain a letter or word. The message is then written letter

* It was necessary, however, to use a number of code words in this cipher in order to conceal names of persons and places.

by letter, or word by word, in these spaces in a pre-arranged order, and the cryptogram is formed by reading off the letters in another order.

NOTE.—When describing Cipher Systems, the terms "line" and "column" are used to denote horizontal rows and vertical rows of letters or words respectively.

1. *Hebrew Transposition Cipher.*

In this cipher lines containing a certain number of letters are agreed upon, and the message is then written out in lines of this length.

Thus, if the words—"A reconnaissance made yesterday across the river found no traces of the enemy"—were to be sent, and the number of letters in each line were to be 23, it would be first written out as follows:—

a	r	e	c	o	n	n	a	i	s	s	a	n	c	e	m	a	d	e	y	e	s	t
e	r	d	a	y	a	c	r	o	s	s	t	h	e	r	i	v	e	r	f	o	u	n
d	n	o	t	r	a	c	e	s	o	f	t	h	e	e	n	e	m	y	e	n	d	s

The cryptogram is formed by reading of the lines consecutively backwards:—

t s e y e d a m e c n a s s i a n n o c e r a
n u o f t e v i r e h t s s o r c a y a d r e
s d n e y m e n e e h t f o s e c a r t o n d

In order to decipher the above cryptogram, the receiver writes the letters backwards in lines of the arranged length, and then reads the message in the ordinary way.

It need hardly be pointed out that such a system affords little security, and its simplicity is its only recommendation. It is, however, of interest as being the earliest and simplest form of transposition.

It was formerly the practice when using this cipher, to fill up the last line with dummy letters as above, if it was still incomplete when the word "ends" or "full-stop" had been written. Such a practice, however, is not only unnecessary but even harmful, for the cryptogram, even if the last line is left incomplete, can be read easily by anyone who knows the number of letters in the lines, and if the last line is always completed, solution is facilitated, for the total number of letters will always be exactly divisible by the number of lines, and consequently the number of alternatives will generally be limited.

2. *The Zigzag Transposition Cipher.*

In this cipher the letters of the text are written out in columns, each containing a pre-arranged number of spaces. The letters are written up and down alternate columns, beginning at the top or bottom of a certain column, and the cryptogram is formed by reading off the lines of letters.

Taking the same words as before—"A reconnaissance made yesterday across the river found no traces of the enemy"—and the number of letters in each column as 8, the message is written out as follows, dummy letters being used, if necessary, to complete the table :—

a	m	a	o	s	n	o	m	y
r	e	d	r	s	d	t	e	f
e	c	e	c	t	n	r	n	u
c	n	y	a	h	u	a	e	l
o	a	e	y	e	o	c	e	l
n	s	s	a	r	f	e	h	s
n	s	t	d	i	r	s	t	t
a	i	e	r	v	e	o	f	o

and the cryptogram would be :—

A M A O S N O M Y R E D R S D T E F E C E C T, &c

In order to decipher such a cryptogram, the receiver divides the total number of letters by the number of letters agreed upon for each column, and thus obtains the number of columns. He then writes the letters of the cryptogram in lines containing this number of letters, and obtains the above diagram, from which he can read the text.

The system employed in this cipher is somewhat similar to the Federal Army or Route Cipher, described on page 27, the difference being that in the latter the words, and in this cipher the letters, are transposed.

3. *The Permutation Cipher.*

This is a further development of the Letter Transposition system, but it is more complicated without being safer. The letters of the text are set down according to such permutations of 3, 4, 5, or more figures, as may be arranged between the correspondents.

Supposing that the following message—"Delay departure of transports until you receive further orders from headquarters"—were to be enciphered, and that it were arranged to use the following permutations of four figures, viz., 1324, 1243 and 3214, a table would be constructed thus :—

No. 1.

1324	d	l	e	a
1243	y	d	p	e
3214	t	r	a	u

In the above table the first four letters of the text are written in the 1st line, the 1st letter of the text in the 1st column, the 2nd letter in the 3rd column, the 3rd in the 2nd, and the 4th letter in the 4th column, following the order of the figures 1324. The 5th letter would then be written in the 1st column of the 2nd line, the 6th in the 2nd column, the 7th in the 4th, and the 8th in the 3rd column following the order of the figures 1243. The 9th letter would be written in the 3rd column of the 3rd line, and so on, the first 12 letters of the text being written as above.

A second series is then begun, the letters being written on the right of the letters already inscribed and following the same system, and this process is repeated until the message is completed, thus :—

No. 2.

1324	drtcoa	louidq	eeserd	afnveu
1243	yttera	drifsr	pnyrre	ealuft
3214	torehx*	rpuhms	asotor	urerez*

* Dummy letters.

The cryptogram is formed by reading off the lines of letters, and, when divided into groups of five letters for transmission by telegraph, would read thus :—

DRTCO ALOUI DQEES ERDAF NVEUY TTERA, &c.

In order to decipher such a cryptogram, the recipient who knows the figure key and therefore the number of lines and columns divides the total number of letters by the total number of spaces (12 in the

above table), which gives the number of letters in each space. The letters of the cryptogram are then written in groups containing this number of letters, as in table No. 2; the first letters of each group are read off in each line in succession in accordance with the figure key, then the second letters of each group, and so on.

The above system is not recommended, for it is troublesome to work and affords little security.

4. *The Nihilists' Cipher.*

This cipher, which is said to have been used by Nihilists, is based upon the principle of double transposition. A keyword is agreed upon by the correspondents, and a number is obtained from the alphabetical order of the letters forming it. Thus the word "Thames" would represent 631425, T being the 6th letter in alphabetical order of the six letters forming the keyword, H the 3rd letter, and so on.

A square is then formed, each side of which contains as many divisions as there are letters in the keyword, and the letters of the message are then inscribed in their natural order in the square. For instance, if the message "The sixth division will attack at dawn" were to be enciphered with the keyword "Thames," it would first be written out thus :—

	1	2	3	4	5	6
1	T	H	E	S	I	X
2	T	H	D	I	V	I
3	S	I	O	N	W	I
4	L	L	A	T	T	A
5	C	K	A	T	D	A
6	W	N	Q	X	Y	Z

N.B.—Any spaces left blank after the message has been written out are filled in with dummy letters, the less frequently occurring letters of the alphabet being used for this purpose.

The next step is to prepare another square similar to the previous one, but the numbers are now written in the order obtained from the keyword, *i.e.*, 631425. The letters are then inscribed in the new square in the same relative position to the numbers as in the first square. Thus the letter W given by the co-ordinates 5 and 3 (5th column, 3rd line) in the original is placed in the column marked 5 in the line marked 3 in the cryptogram square.

	6	3	1	4	2	5
6	Z	Q	W	X	N	Y
3	I	O	S	N	I	W
1	X	E	T	S	H	I
4	A	A	L	T	L	T
2	I	D	T	I	H	V
5	A	A	C	T	K	D

The cryptogram is then formed by reading off the lines of letters :—

Z Q W X N Y I O S N I W X E T S H I A A L T L T
I D T I H V A A C T K D.

The receiver of the cryptogram in order to obtain the text reverses the above operation, that is to say, he first writes the cipher letters as received in the second table, and then from his knowledge of the figure key, which he obtains from the keyword, he re-constructs the first table and reads the message.

This system has the disadvantage that the tables used must always be completely filled. Consequently, if a message contains rather more letters than can be inscribed in one or more tables, the incomplete table must be filled in and thus unnecessary work is the result.

5. *The Federal Army Cipher* (*A*).

During the American Civil War this type of cipher was employed by the Federals with eminently satisfactory results, for although many messages were intercepted by the Confederates, it is said that none were solved. It is doubtful, however, if the same security would be afforded by this type of cipher in future, for the general knowledge of cryptography has improved considerably since that period.

In this system the words are not altered, but the order in which they are written follows a certain route arranged beforehand. In the earliest form of the cipher only one " route " was used, which was to write the text out in six columns, going up the sixth, down the first, up the fifth, down the second, up the fourth and down the third. Equivalents were substituted for proper names and a column of dummy words was introduced, and the cryptogram was formed by reading off the words in horizontal lines. Supposing it were required to encipher the message " The Cavalry Brigade is to move on Thursday next to the neighbourhood of Dorchester, the Corps Artillery to remain at Yeovil till further orders. Headquarters will be at Bath," and the words " ship," " uncle " and " Arabia " were to stand for " Dorchester," " Yeovil " and " Bath," we should obtain :—

1.	2.	3.	4.	5.	6.	7. (*Dummies*)
Move	Corps	Quarters	Head	the	to	polite
on	Artillery	will	orders	ship	is	curse
Thursday	to	be	further	of	Brigade	hasty
next	remain	at	till	neighbourhood	Cavalry	kind
to	at	Arabia	uncle.	the	the	just.

A word agreed upon between the correspondents was prefixed to indicate the number of columns used, and if this word were " June "* the cryptogram would read as follows :—

" June move corps quarters head the to polite on Artillery will orders ship is curse Thursday to be further of brigade hasty next remain at till neighbourhood cavalry kind to at Arabia uncle the the just."

* The word " June " is chosen purely arbitrarily, and the number of letters in the word has no connection with the number of columns.

In order to further obscure the meaning, it was customary to mis-spell words, putting "wood" for "would," "counsel" for "council," &c.

The receiver of the cryptogram, knowing the number of columns in which the words are written and being informed of the column of dummies, reconstructs the above table and reads off the words according to the route adopted.

The above system is easy to work, but requires a list of substitutes for proper names, which become too numerous to remember, and in addition is probably not sufficiently secure for present day requirements.

(*b*) Substitution Ciphers.

In these systems other letters are substituted for the letters of the text, either singly or in pairs. At first sight it might appear that, if the original letters of the message were all changed, there would be no material on which to base solution, and the cryptogram might be regarded as practically insoluble. This, however, as will be seen from the solutions described in detail in the next chapter, is far from being the case. It is an unvarying law that in any given language certain letters occur more frequently than others, and this relative frequency is, in a message of any considerable length, fairly constant. Moreover, certain groups of letters occur with regularity, especially such terminations of words as "tion," "sion" in English and French, and "ung," "eit," "en" in German, while certain letters are in the majority of words followed by certain other letters, *e.g.*, in English "t" is often followed by "h," "s" by "t," &c. These peculiarities are found in all languages, and they cannot be avoided, if a passage of any length has to be written. They invariably constitute reliable material for working out solutions, and consequently substitution ciphers unless framed with unusual ingenuity are by no means proof against solution.

It may be accepted as an axiom that substitution ciphers, in which each letter of the text is always represented by the same letter in cipher, or in other words when only one alphabet is employed,* can always be solved if the message is of any length. This fact has led to the further development of substitution systems, for it has been realised that their value depends chiefly upon the ingenuity of the method employed in order to make use of different alphabets.

6. *Cæsar's Cipher.*

This simple form of letter substitution is attributed to Julius Cæsar, but, as already stated, it is in reality much older.

In this cipher, each letter of the text is replaced by the letter which stands a certain number of places before or after it in the alphabet. For instance, if it were agreed to take the second letter after each letter of the message (A being considered to follow Z), the

* For example, when each letter of the text is always represented by the letter standing a certain number of places, say 6, after it in alphabetical order, *i.e.*, *a* would always be represented by *g*, *d* by *j*, &c.

words "Enemy's concentration completed" would be enciphered thus :—

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

In order to decipher such a cryptogram, the letter standing two places before each cipher letter must be written down.

Another form of this cipher is to employ a conventional or arbitrary alphabet, in which the letters are not in alphabetical order. As used in the time of Julius Cæsar each correspondent was obliged to have a copy of this arbitrary alphabet, and there was always a danger that it might be lost or stolen. Many methods are now known of forming a conventional alphabet with the aid of a keyword, by which means this risk is avoided.

In order to encipher a message, the conventional alphabet is placed under the ordinary alphabet. Each letter of the text is then looked up in the latter and represented in cipher by the letter of the conventional alphabet directly beneath it. If the words "Enemy's concentration completed" were to be enciphered with the following conventional alphabet, the successive stages would be as follows :—

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

Text .. e n e m y s c o n c e n t r a t i o n c o m p l e t e d

Cipher .. S Z S C K X G T Z G S Z I F J I Q T Z G T C B H S I S P

In order to find readily the cipher letters in the conventional alphabet when deciphering the above, it will be found convenient to construct a deciphering key, which for the above alphabet would be as follows :—

Conventional Alphabet (re-arranged) 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

Ordinary Alphabet (re-arranged) f p m u j r c l t a y v b w g d i x e o k h z s q n

Such ciphers are fairly secure for short messages provided the conventional alphabet is frequently changed, but messages of any length enciphered on such systems can usually be solved without delay.

7. *The Wolseley or Sudan Cipher.*

(Also known as the Square Cipher.)

In order to use this cipher, which was employed during the British operations in the Sudan and in the South African War, a keyword is agreed upon by the correspondents. A square is then divided into 25 spaces, which are numbered as shown below, and in these squares the keyword is first written, followed in regular order by the remaining letters of the alphabet, omitting J, for which the letter I is made use of. If the keyword were "bridge" the square would be filled in as follows :—

1 B	2 R	3 I	4 D	5 G
8 E	9 A	10 C	11 F	6 H
7 K	12 L	M	12 N	7 O
6 P	11 Q	10 S	9 T	8 U
5 V	4 W	3 X	2 Y	1 Z

In the above table there are two spaces each marked with the same figure and each letter of the text is represented in cipher by the letter which stands in the other space bearing the same number, while the letter in the central space, which has no number, is not changed. If the message to be sent were "Convoy moved forward," the process would be :—

Text letters ..	convoy	moved	forward
Cipher letters ..	SKLGKR	MKGUW	QKYDTYW

and the cryptogram would read as follows :—

SKLGK RMKGU WQKYD TYW

To decipher the cryptogram, the receiver forms the same table by the aid of the keyword, and reverses the process by writing down for each letter in the cryptogram the letter which stands in the space similarly numbered.

This cipher is merely a modification of the Cæsar's cipher (*see* page 28), for it will be found that the result obtained from the preceding table can also be arrived at by using the following conventional alphabet :—

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

or by using the following table, which is an even simpler method :—

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

This system affords even less security than the conventional alphabet, for the substitution of each half of the alphabet is in this case reciprocal (*e.g.*, E stands for U, and U for E), solution being thereby considerably facilitated.

* Each letter of the vertical pairs is represented by the other letter of the same pair.

8. *The Sliding Alphabet Cipher.*

This cipher has been in use for many years in different countries, and was employed by the Germans in 1870. In France it is known as the "Système St. Cyr," because it is taught to the students at St. Cyr.

In order to use the cipher, each correspondent must prepare a fixed and sliding alphabet, written on strips of stiff paper or cardboard. The sliding alphabet contains the alphabet twice over, so that, whatever the position of the sliding alphabet, there will always be some letter of this alphabet under each letter of the fixed alphabet.

A keyword is chosen (*see* page 19) and the letters of the message are written out in as many columns as there are letters in the keyword. For instance, if the keyword agreed upon were "Thames," and the message to be sent were "Great activity in arsenal here," the letters would be written out in six columns, thus* :—

G R E A T A
C T I V I T
Y I N A R S
E N A L H E
R E

Now, the first letter of the keyword, "T," in the sliding alphabet is brought under the A of the fixed alphabet, and the first column of letters is enciphered, each letter being looked up in the sliding alphabet and represented in cipher by the letter standing immediately above it in the fixed alphabet. The second letter of the keyword is then brought under the A of the fixed alphabet, and the second column of letters is similarly enciphered, and the same procedure followed with the remaining columns of letters. Each column of letters is thus enciphered by a different alphabet, and the number of alphabets used corresponds to the number of different letters in the keyword.

The above columns would be represented in cipher thus :—

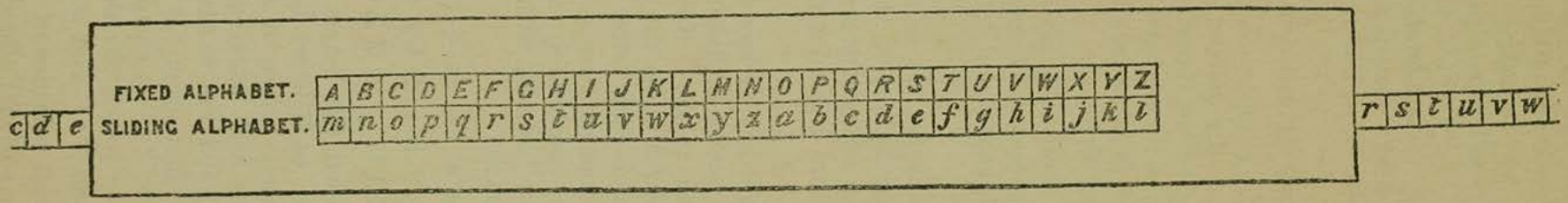
N K E M P I
J M I J E B
F B N O N A
L G A Z D M
Y X

and the crytpogram, arranged in groups of five letters, would read as follows :—

NKEMP IJMIJ EBFBN MNALG AZDMY X

* With practice in the use of this cipher, it will be unnecessary actually to write out the letters of the message in columns, as it will suffice to tick off the letters in groups of six, thus : Great a | ctivit | y in ars | enal he | re. Writing the letters in columns is recommended, however, for beginners, as it does not take long and reduces the possibility of mistakes.

Sliding Alphabet in position for enciphering the fourth column of letters, *i.e.*, with the fourth letter, M, of the keyword under the A of the fixed alphabet.



In order to decipher the cryptogram, the receiver writes the letters out in the same number of columns as there are letters in the keyword, and then, by reversing the process employed when enciphering, finds the true letters represented by the letters of each column successively.

This cipher affords a considerable degree of security provided the message sent is short; but for long messages it is untrustworthy, as will be seen by following the solutions described on pages 57 and 61.

The above cipher may be varied in the following ways :—

(1.) When the sliding alphabet is in the position indicated successively by the letters of the keyword, the method of enciphering before described may be reversed. In this case the letters of the text are looked up in the fixed alphabet, and each letter is represented by the letter standing below it in the sliding alphabet.

(2.) By setting the sliding alphabet so as to bring the letters of the keyword successively under some letter other than A of the fixed alphabet, and by varying this letter from time to time.

(3.) By using the alphabet set to the first letter of the keyword to encipher the letters of the first word of the message, changing to the second letter of the keyword for the second word, to the third letter for the third word of the message, and so on.

(4.) By using a figure key or key number instead of a keyword. This system is known in Belgium as Count Gronfeld's cipher, and in England as the "Key Number" cipher. The key number is repeated under the letters of the message as often as required, and each letter is represented by the letter standing the same number of places after it in the alphabet as the figures immediately under the letter. The words "Great activity" would, with the figure key "24681," be enciphered thus :—

g r e a t a c t i v i t y
2 4 6 8 1 2 4 6 8 1 2 4 6
I V K I U C G Z Q W K X E

(5.) In another method the letters of the text themselves form the key letters, each letter being enciphered by using the letter immediately before or after it. For instance, if the letter preceding each letter of the text is to be taken as the key letter, and the words "Great activity" are to be enciphered, the first letter "g" remains the same in cipher, the second letter "r" is enciphered by using the first letter "g" as the key letter, the third letter "e" by the aid of the second letter "r" and so on.

(6.) The security of all varieties of this system is much increased by using a conventional alphabet.

There are many substitution ciphers which are practically the same as the Sliding Alphabet Cipher. Some of these, as will be seen from the description of the Beaufort cipher which follows, are worked with the aid of a table, such as Tritheim's letter cipher, Tableau de Porta,* Tableau de Vigenère, Multiplication cipher, &c.; but all of these can be worked as easily with a sliding alphabet. None of this class of ciphers differ in any essential particular from the latter system, and consequently examples of all of them need not be given.

* *See* page 88.

9. *Beaufort Cipher.*

This cipher, though not generally regarded as such, is another form of the Sliding Alphabet cipher, and as generally used, necessitates the use of the following table :—

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

It will be observed that in the above table each column, both vertical and horizontal, begins and ends with the same letter of the alphabet, and that i and j are treated as one letter.

The method of employing the table is as follows :—

A keyword or motto or sentence, which is easy to remember, is agreed upon by the correspondents. This is written under the text of the message, letter for letter, and is repeated as often as may be necessary.

Text—J o i n m e a t P e s h a w a r t o m o r r o w

Key—K i n g E d w a r d K i n g E d w a r d K i n g

Cipher—B V E U T Z W H C Z S B N L E N D N F Q T S Z L

The method of enciphering is as follows :—

Find the first letter of the text (J)* in the left-hand column, and look along this line for the first letter of the key (K) ; then at the top of the column in which (K) stands will be found the letter (B), which will represent in cipher the first letter of the despatch. Proceed in the same manner for each letter of the text.

---

* i and j are treated as the same letter.

To decipher the cryptogram, write the keyword or phrase under it, letter for letter, and then proceed in a precisely similar manner as when enciphering the despatch. Thus, look for the first letter, B, of the top line (now the cipher line) in the left-hand column ; then look along this line for the first letter of the key (K) ; then at the top of the column in which K stands will be found the required letter (J).*

This cipher may be used, without employing the above table, in the following manner :—

Write out the alphabet, omitting J, and number it from 0 to 24, thus :—

0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24
A	B	C	D	E	F	G	H	I	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z

Then, if— a = key letter,
b = text letter,
c = cipher letter,

a message can be enciphered by applying the following formula :—

$$a - b = c,$$

or, where a is less than b, by the formula :—

$$25 + a - b = c.$$

Using the above formula in order to encipher the first word of the same message, we get :—

$$\begin{aligned} K - J &= 9 - 8 = 1 = B \\ I - O &= 25 + 8 - 13 = 20 = V \\ N - I &= 12 - 8 = 4 = E \\ G - N &= 25 + 6 - 12 = 19 = U, \end{aligned}$$

the same result as before.

(*b.*) The same result can be obtained by employing the Sliding Alphabet system. The same cryptogram will be obtained as before, if the following letters are used as key letters :—

ITET TF EM NFAGNLWE QBHYYZPL.

Of course, this series of letters could not be remembered, and so would not be suitable for use as a key, but they serve to show that the two systems are practically identical.

10. *Playfair Cipher.*

According to this system the letters of the text are enciphered in pairs instead of single letters, a peculiarity which greatly increases the security afforded. It has already been stated that in the case of substitution ciphers in which letters of the text are with the same key always represented by the same letter in cipher, solution is usually possible without much delay ; also that Sliding Alphabet ciphers, even when several alphabets are employed, can be solved,

* i and j are treated as the same letter.

if the despatch be of considerable length or if a number of shorter messages be available, though solution will in this case be more difficult.

In the Playfair cipher, however, the letters of the text are enciphered in pairs, and one letter of a pair is represented in cipher by the same letter only when the other letter of the pair remains the same. This fact greatly increases the difficulty of solution, and it may be said that messages enciphered by the Playfair system, if not actually insoluble, would generally cause sufficient delay to prevent the enemy from deriving advantage from the solution of a cryptogram.

The method of using the Playfair system is as follows :—

Example.

Keyword—" Soldier."

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

Construct a square, containing 25 spaces,* and inscribe first the letters of the keyword, omitting repetitions, and then the remaining letters of the alphabet.

There are other ways of inscribing the letters of the alphabet in the table, and these variations are as a rule adopted in order to avoid the constant occurrence of the less frequently used letters of the alphabet V, W, X, Y, Z, in the last line of the table. For instance, the last 5 letters may be written along a diagonal, or all the letters may be written in alternate squares, or in every third square, until the alphabet is completed.

To encipher the message the letters are taken in pairs, and equivalents are found for each pair of letters. A pair of letters will be found to occur :—

(*a.*) In the same vertical column,
(*b.*) In the same horizontal line, or
(*c.*) At opposite angles of some rectangle.

* By using K for both K and Q a rectangle of 24 spaces can be employed instead of a square of 25, and this variation is often introduced in French cipher systems, in which language the letter K seldom occurs.

In case (*a*) each letter is represented in cipher by that which stands below it, and the bottom letter by the top one of the same column, *e.g.*, F V would be represented by N S.

In case (*b*) each letter would be represented by the letter on its right and in the same line, and the letter on the extreme right by that on the extreme left, *e.g.*, R C would be represented by A E.

In case (*c*) the two letters to be enciphered are represented by those on the other diagonal of the rectangle, each by that which is in the same horizontal line, *e.g.*, S G would be represented by O F.

If, on dividing the letters of the text into pairs, a pair is found to be composed of a double letter, a dummy letter such as Q, X, Y or Z, which is not likely to mislead the receiver of the message, should be introduced, care being taken that the dummy letter employed is constantly varied.

Thus the message—" Your messenger not arrived "—when divided into pairs would be :—

YO UR ME SQ* SE NG ER NO TA RX* RI VE DZ*,

while the sentence—" The pass was too difficult "—requires no dummy letters, the pairing being :—

TH EP AS SW AS TO OD IF FI CU LT

If the message contains an uneven number of letters, a dummy letter should be added to complete a pair, in order that the last letter may be enciphered.

Example.—If the message—" Enemy attacked at noon and were repulsed "—were to be enciphered with keyword " Soldier " (*vide* perceding table), the letters would be divided into pairs as follows :—

EN—EM—YA—TY*—TA—CK—ED—AT—NO—ON—
AN—DW—ER—ER—EP—UL—SE—DE—ND—SX.*

The pairs of letters would be enciphered thus :—

FV—CF—XB—YD—QB—BM—BS—BQ—PS—SP—
EQ—OY—RA—RA—RN—QI—EF—SB—TS—LV.

The cryptogram, when grouped for transmission by telegraph or signalling, would be :—

FVCFX—BYDQB—BMBSB—QPSSP—EQOYR—ARARN—
QIEFS—BTSLV.

In order to decipher the cryptogram, the receiver who knows the keyword constructs a similar table. He then divides the letters into pairs, and from his table finds the equivalents for each pair ; taking the letters next above each when they are in the same vertical column, those next on the left when they are in the same horizontal column, or those at the opposite angles of the rectangle.

---

* Dummy letters.

CHAPTER IV.

Solution of Cryptograms.

Cryptograms never quite insoluble—Military cryptograms easier to solve than other despatches—Change of opinion regarding security afforded—Experts working in combination—Books and papers necessary to work of solution—Solution of transposition ciphers—Solution of substitution ciphers.

It has already been stated that the term "security," when used in connection with cipher messages, means only comparative security, for any system suited to use in the field must be simple. Consequently, if the enemy intercepts a sufficiently long cipher message or a number of short messages enciphered with the same key, and if expert assistance be available, as will generally be the case, a solution will invariably be effected sooner or later.

When considering the question of security, it must be remembered that military cipher messages are generally more easy to solve than a despatch of a general nature, the subject of which may not be known and which consequently affords little ground for guesswork. In the case of military despatches which fall into the enemy's hands, the general contents of a message may frequently be guessed. Moreover, as the situation in the theatre of war, position of troops, besides the names of prominent persons and places will be known, and it may be assumed that certain words and technical terms will be likely to occur, solution is greatly facilitated; for, when one or two letters have been fixed, it may be possible to guess words such as "communications," "embarkation," "division," "mobilization," "attack," "position," "retreat," &c., and this may lead to the discovery of the system employed, and to the solution of the whole cryptogram.

Opinions have changed considerably in recent years regarding the amount of security afforded by various systems, and some systems which have been known by different names in different countries and considered to be quite distinct are now recognised as being merely variations of the same system. For instance, it has been claimed in England that the Beaufort cipher affords absolute security, but it is practically identical with the "Système St. Cyr" which is taught to the pupils of the French Military College of that name, and has been shown to be a variation of the Sliding Alphabet cipher, the solution of which is generally considered to be by no means difficult. Again, many forms of transposition ciphers, of which the American Route cipher is a typical example, were formerly considered to afford complete security, whereas with the increased knowledge of the

subject now available, it is improbable that such systems would withstand systematic investigation for any length of time.

Allusion has already been made to the advantages of the services of a body of experts working together, for it may often be assumed that one or other of a limited number of systems has been used it will thus be possible to allot to each expert the task of attempting the solution of the cipher by one of these systems. All of them will thus be tried simultaneously until a clue is obtained to the system which has been used, when the whole party will turn their attention to solution by that method. The preliminary work of discovering the system used is by this means much simplified, while a supposed clue can be followed up by one of the party without interrupting the work of the remainder. The value of such a body has been recognised abroad. During the American Civil War all Confederate cipher despatches which were intercepted were handed over to a party of civilian experts at the Federal headquarters, and an organization of a similar nature was attached to the German General Staff in 1870–71.

Books and papers necessary for effecting a solution.—It has already been stated that certain natural qualities and much previous study are necessary to become an expert solver of cryptograms. The following books and papers should be at hand before work is commenced :—

(1.) A dictionary of the language in which the message is written.

(2.) A rhyming dictionary, in which the words are arranged according to their terminations.

(3.) A dictionary of synonyms.

(4.) All code books, and tables of a similar nature, in the language of the message, if procurable.

(5.) Tables of the peculiarities of the language, frequency of recurrence of individual letters and of groups of letters, &c. (*see* page 42).

(6.) All available particulars which might assist solution, such as the name and title of the sender and recipient of the message, place and date of despatch, destination, circumstances under which captured or intercepted, names of important localities and prominent commanders and officials.

The work of solution will be considerably facilitated if the services of a certain number of assistants are available, who, without being themselves experts, could tabulate recurrences of letters, count the distance between recurrences, &c.

Some of the Principal Characteristics of the English, French, and German Languages.

It will be seen from the solutions in this chapter that in the case of substitution ciphers, the chief aid to solution is the frequency with which individual letters and groups of letters recur, and in the case of

transposition ciphers the frequency of recurrence of groups of letters, added to the fact that particular letters are often, and in some cases always, followed by certain other letters.

In most European languages the letters which occur frequently are very similar, *e* being usually the most common letter. In the three languages under consideration the other frequently recurring letters are t, o, i, a, n, s, r, the order of frequency of these letters being slightly different in each language. In a passage containing 300 or more letters, the occurrences of different letters will generally approximate to the normal tables of recurrence given below, but in a short message or in a single sentence there may, of course, be wide discrepancies between the actual and normal recurrences of certain letters. This is illustrated by the following sentences in English and German :—"Infantry go into camp forthwith. Two troops of Fourth Hussars to occupy right block of cavalry barracks till arrival of Fourth Dragoon Guards," where the letter *e* does not occur at all, or "*Ich war am Rückzug als mir das Schriftstück von Dir durch Ordonnanz zukam*" where there is no *e*, and *a* occurs twice as often as *n*.

English.

The English alphabet consists of 26 letters, and the normal scale of frequency* for single letters is as follows :—

e — 12·0	c — 2·8
t — 9·4	m — 2·7
a — 7·8	f — 2·5
o — 7·5	p — 1·9
n — 7·3	g — 1·8
i — 7·3	y — 1·8
s — 6·9	w — 1·75
r — 5·9	b — 1·7
h — 5·7	v — 1·1
d — 3·9	k — 0·6
l — 3·6	q — 0·3
u — 3·0	x — 0·3

j — 0·27 and z — 0·18.

The order of frequency for combinations of two letters is :—*th, he, in, an, on, re, ti, er, it, nt, es, to, st, at, en, of, is, ed, nd, ou.*

The order for combinations of three letters is :—*the, ion, tio, and, tha, ing, ent, eth, fth, hat.*

The order for combinations of four letters is :—*tion, that, fthe, nthe, ther.*

The order for double letters is :—*tt, ss, ee, ll, dd, mm, nn, oo.*

The following peculiarities are useful :—The letter "*t*" is very frequently the first letter of a word. At the beginning of a word *h, l, m, n, v* or *y*, must be followed by a vowel ; *q* must always be

* The scale of frequency given in different books varies slightly, but the variation is of no importance as regards working out a solution.

followed by *u* and some other vowel, a fact of great importance in the case of transposition ciphers.

The first word of a written message, *i.e.*, a message not sent by telegraph, is very often "*the.*"

French.

The French alphabet consists of 25 letters and is the same as the English alphabet with w omitted.

The normal scale for single letters is as follows :—

e — 17·6	d — 3·7
s — 8·2	c — 3·2
a — 8·11	m — 3·0
n — 7·2	p — 3·28
t — 7·1	v — 1·71
i — 7·1	f — 1·08
r — 7·0	g — 1·05
u — 6·2	q — 1·02
l — 5·5	b — 0·94
o — 5·3	h — 0·82

j — 0·49
x — 0·43
y — 0·25
z — 0·15
k — 0·03

The order of frequency for combinations of two letters is :—*es, le, de, re, en, on, nt, te, er, et ou, se, ai, ne, el, it, qu, me, em, ti.*

The order for combinations of three letters is :—*que, ent, les, ion, des, res, ait, ous, ont, tre.*

The order for combinations of four letters is :—*tion, ment, nous, quel.*

The order for double letters is :—*ll, mm, nn, rr, pp, ff, cc, tt, ss, bb, dd, ee, gg.*

h is most frequently preceded by *c*, and often by *p* or *t* ; *e.g.*, *manche, alphabet, théâtre.*

z occurs nearly always at the end of a word, except in the words *douze, dizaine, onze, quinze, zone,* and a few others.

q is always followed by *u*, except when at the end of a word, as in *coq, cinq.*

y is always preceded by the vowels *a, o,* or *u, e.g., essayer, envoyer, fuyard,* except in a very few words, such as *dynamite,* and in *y* and *yeux.*

c is very often followed by *t, e.g., aspect, section.*

x is generally preceded by *u, e.g., deux, travaux.*

v always follows a vowel, except at the beginning of a word, *e.g., avancer, boulevard, civil,* and *vrai, vengeance.*

of is always preceded by *pr,* unless the next letter is another *f* ; *e.g., profusion, officier.*

If two groups of three similar letters are separated by a single letter, the latter will usually represent *a* ; *e.g., peu à peu, vis à vis.*

Two adjacent groups of four similar letters will generally represent *nous nous* or *vous vous*: and adjacent groups of five similar letters will represent *faire faire.*

When the letter *e* has been fixed, it will sometimes be possible to guess the letter *s* and the word *les,* and then to determine the length of the next two or three words; *e.g., les grands ponts construits, les bataillons auxiliaires.*

If the last letter and the fourth letter from the end of a word be *e,* the two intervening letters will often be *nt* or *nc*; *e.g., vente, descente, régence.*

The terminations *tion, sion, ice, ilite, ite, ant,* are frequent.

Orders and instructions frequently commence with the word *vous* or *le.*

German.

The full German alphabet contains 29 letters, viz., a, ä, b, c, d, e, f, g, h, i, j, k, l, m, n, o, ö, p, q, r, s, t, u, ü, v, w, x, y, z, but in telegraphic messages and cryptography the "modified" letters ä, ö, ü are usually replaced by the "unmodified" form, and the alphabet becomes identical with the English.

The normal scale for single letters is as follows:—

e — 18·66	h — 3·98*	w — 1·45
n — 11·33	g — 3·96	k — 1·21
i — 7·88	o — 3·25	v — 1·08
r — 7·25	l — 2·91	p — 0·33
s — 6·75	b — 2·67	j — 0·12
t — 5·04	m — 2·58	q, x, y — hardly ever occur.
u — 5·00	f — 1·67	
d — 4·83	z — 1·62	
a — 4·79	c — 1·58	

The order of frequency for combinations of two letters is:—*en, er, ch, de, ge, ei, ie, in, ne, be, el, te.*

The order for combinations of three letters:—*ein, ich, den, der, ten, aht, sch, che, die, ung.*

The order for combinations of four letters is:—*icht, keit, heit, chon, chen, cher, urch, eich.*

The order for double letters is:—*ee, nn, ss, tt, ll, rr, mm, ff.*

The following peculiarities may be useful:—*c* is used in German chiefly in conjunction with *h* or *k,* and is rarely doubled. When used in conjunction with *h,* these two letters not infrequently stand near the end of a word. When they are followed by a single letter, the latter is usually *e* or *t,* as in *Wache, Nacht;* when they are followed by two letters, these generally form the infinitival termination, *e.g., wachen, machen.* The letters *ch* are frequently preceded by *s, e.g., schon,* and this group of letters is frequently found at the beginning of a word.

d is often succeeded by *e,* as in *der, den, des, dem,* or by *i,* as in *die, dir.* It is seldom doubled.

* The figure when modern spelling is used.

e, which is generally recognizable by its frequency of recurrence, is often found repeated with but one intermediate letter, *e g.*, *Leben*, *gegeben*. It is often the penultimate letter of a word, *et*, *er*, and *en* being of frequent occurrence.

f is seldom used singly, but is used fairly often as a double letter, *e.g.*, *Kaffee*, *Riff*, *Pfaff*.

g does not occur very frequently, and chiefly in the prefix *ge* of the past participle, and in the termination *ung*, *e.g.*, *gegeben*, *Hoffnung*, *Rettung*, *Ziehung*. In the latter case it can often be recognized, for as *u* and *n* are among the letters of most frequent occurrence, one or both may have been previously fixed.

h is often preceded by *c** and *p*, *e.g.*, *Wache*, *Philosoph*, or occurs between two *e's*, *e.g.*, *stehen*, *sehen*. It is only doubled in compound words such as *Kirchhof*.

l is often preceded by *g*, or by the consonants *b*, *f*, *k* and *p*. Any other letter preceding it must be a vowel. If *l* is followed by any other consonant than *g*, the letter immediately before it must be a vowel, *e.g.*, *also*, *selbst*. *l* is frequently found doubled, *e.g.*, *alle*, *soll*, &c.

n is frequently found in the termination *en*, and is often doubled as in *können*, *Sonne*, &c.

p is often succeeded by *f*, *e.g.*, *Pferd*, *Pfund*, or by *h*, as in *Philosoph*, *Telegraph*, &c., and is not often doubled.

r is frequently found in conjunction with *e*, but *er* occurs more frequently in the middle than at the end of a word. It is doubled fairly often, *e.g.*, *Herr*, *Pfarrer*.

s is frequently preceded or followed by *e*, and is also followed by *t* and by *ch*. If *s* is followed by *p*, the next letter must be *r*, *l*, or some vowel, *e.g.*, *Sprache*, *Splitter*, *Sporn*. It is often doubled as in *Messer*, *besser*, &c. It is also trebled in compound words, *e.g.*, *Massstab*.

t is often followed by *z*, as in *trotz*. It is frequently doubled, as in *Ritter*, *Schritt*, &c.

v usually forms part of the syllables *vor*, *von*, or *ver*. It is never doubled.

z is often preceded by *s* or *t*. It is never doubled.

Russian.

Composition of the Alphabet.

The Russian Alphabet consists of 36 letters :—

А, Б, В, Г, Д, Е, Ж, З, И, Й, І, К, Л, М, Н, О, П, Р, С, Т, У, Ф, Х, Ц, Ч, Ш, Щ, Ъ, Ы, Ь, Ѣ, Э, Ю, Я, Ѳ, Ѵ,

but, of these, Ъ, Ѳ and Ѵ are not ordinarily used in cipher, and sometimes Й and І are both represented by И, and Э by Е.

* In the former method of spelling it frequently occurred after *t*, *e.g.*, Thal, Rath.

There is a special adaptation of the Morse code to the Russian alphabet, which gives 31 letters only, as follows :—

Russian Morse Telegraphic and Signalling Codes.

Russian.	Equivalent.	Symbol.	Russian.	Equivalent.	Symbol.
А	A	• —	Р	R	• — •
Б	B	— • • •	С	S	• • •
В	V	• — —	Т	T	—
Г	G	— — •	У	U	• • —
Д	D	— • •	Ф Θ	F	• • — •
Е Э	E	•	Х	KH	• • • •
Ж	J	• • • —	Ц	TS	• — • —
З	Z	— — • •	Ч	CH	— — — •
І И	I	• •	Ш	SH	— — — —
Й	I	• — — —	Щ	SHCH	— — • —
К	K	— • —	Ъ Ь	MUTE	— • • —
Л	L	• — • •	Ы	I	— • — —
М	M	— —	Ѣ	YE	• • — • •
Н	N	— •	Ю	YU	• • — —
О	O	— — —	Я	YA	• — • —
П	P	• — — •			

Scales of Occurrences.

(i.) The scale of frequency of single letters is as follows :—

О	...	11·02	Д	...	3·02	З	...	1·64
Е	..	7·56	К	...	2·96	Ч	...	1·20
Н	...	7·48	П	...	2·83	Й	...	1·17
А	...	7·45	У	...	2·49	Ж	...	1·07
Т	...	5·83	Я	...	2·14	Х	...	1·05
С	...	5·51	Ы	...	2·03	Ю	...	·77
И	...	5·34	Ъ	...	1·93	Ш	...	·67
Р	..	4·83	Б, Г	...	1·73	Щ	...	·36
В	.	4·66				Ц	...	·28
Л	...	4·09	І	...	1·67	Э	...	·24
М	...	3·21	Ь	...	1·66	Ф	...	·13

Note.—If only one symbol is used for И, Й and І, and one for Е and Э, И becomes 8·18 and Е 7·80.

(ii.) The scale of frequency of double letters is :—

НН ОО СС ТТ

The only double at all frequent is НН ; ОО, СС and ТТ are very uncommon, and other doubles only occur in words borrowed from foreign languages.

(iii.) The scale of frequency of combinations of two letters is :—

НО NO	ВО VO	ОМ O M
СТ ST	НІ NI	АВ } A V
ЕН EN	КО } KO	КА } K A
ОС O S	ОТ } OT	ВА } V A
ОВ O V	ТА TA	ЕР } E R
ПО P O	РЕ RE	НЫ } NI
РА R A	РО RO	ОД } O L
НА N A	АН } AN	НТ } I T
ТО T O	ОР } OR	ОЛ } O L
ГО G O	АТ AT	ТЕ } T E
ПР P R	ЛЬ } L(mute)	ЛО L O
НЕ N E	ОН } O N	ЕС E S

(iv.) The scale of frequency of combinations of three letters is :—

СТВ S T V	ТЕЛ T E L	АГО } AGO
ЕНІ E N I	ННО N N O	ПРІ } P R I
ЕНН E N N	ЛЬН } L(mute) N	ПРО } P R O
ОСТ O S T	НОС } N O S	ІТЕ } I T E
ПОЛ P O L	ЧТО } C H T O	НІЕ } N I E
ЕЛЬ E L (mute)	ТОР } T O R	ОВА } O V A
СТА S T A	ЕГО } E G O	НІЯ N I Y A

(v.) The scale of frequency of combinations of four letters is :—

ТЕЛЬ T E L (mute)	ЕНІЯ E N I Y A	ЛЕНІ } L E N I
ІТЕЛ I T E L	ПРАВ P R A V	СЛЪД } S L Y E D
ЕННО E N N O	ЛЬНО } L (mute) N O	ЕННЫ } E N N I
НОСТ N O S T	ЛЬСТ } L (mute) S T	НАГО } N A G O
ЕНІЕ } E N I E	ПРЕД } P R E L	КОТО } K O T O
СТВО } S T V O	ЕТСЯ } E T S Y A	ОПРО O P R O

Peculiar Features of Certain Letters and Groups of Letters.

(i.) Single letters.

І must be followed by a vowel.
Й „ „ preceded „ „
Ь „ „ „ „ consonant; it cannot begin a word, and only occasionally occurs in the body of one.
Э is usually followed by Т.
П is generally followed by О or Р.
Щ very frequently occurs in participial terminations, after Ю or Я.

Ы never begins a word.
Ю very seldom begins a word.
Ъ ,, ,, ,, ,,
Г, Ж, К, Х, Ш, Ч and Щ cannot be followed by Ы, Ю, or Я.

(ii.) Combinations of letters.

ЕН	is very often followed by	НО, НЫ, or	ІЕ, ІЯ, ІЮ.			
АН	,,	,,	,,	,,	,,	,,
ЛЬ	,,	,,	,,	НО or СТВ.		
НР	,,	,,	,,	А, Е, О or И and frequently begins words.		
ЧТ	,,	,,	,,	О.		
СТВЕ	,,	,,	,,	НН.		
СТВУ	,,	,,	,,	Ю.		

(iii.) Diphthongs.

The only diphthongs which occur frequently are :—
ІЙ, ОЙ, ЫЙ, and АЙ—in order of frequency.

(iv.) Initial letters of words.

The most frequent beginnings of words are :—
Single letters—П, В, Н, С, О.
Two letters—ПО, ПР, НА, НЕ, ВО, ВЫ, ОТ, СО.
Very few words begin with vowels, with the exception of О.

(v.) Terminations.*

As Russian is a much inflected language, it is impossible to do more than treat the terminations generally.
The commonest are :—

(*a*) Ordinary nouns—А, О, Ы, ОВ, У Я, Ю, ОМ, Ъ, АХ, АМ.
(*b*) Abstract nouns—НОСТ, СТВ-, ЕНІ-, АНІ-.
(*c*) Adjectives—НЫМ, НЫХ, НЫЯ, НЫЕ, НАГО, НОЙ, НОМ, НОМУ, СКІЙ and inflections.
(*d*) Verbs—ЕТ, ЮТ, УТ, АЛ, ІЛ, АЛІ, ІЛІ, АТЬ, ІТЬ, ВАТЬ; followed by СЯ, when the verb is reflexive or neuter.
(*e*) Gerunds—Я, ІВ, АВ. These are not very often used.
(*f*) Participles (declined like adjectives)—АЮЩ-, УЮЩ-, ВШ-, ЕНН-, ОВАНН-.
(*g*) Adverbs—НО, СКІ, ЕННО.
(*h*) The following are also found frequently:—ТЕЛЬН-, ТЕЛЬНО, ТЕЛЬНОСТ, ТЕЛЬСТВ-, ТЕЛЬСТВЕНН-; usually preceded by И, *e.g.*, ИТЕЛЬН-, &c.

* The terminal mark ъ not being, as a rule, used in cipher (*see* page 45), it has been omitted from those terminations of which the last letter is a consonant.

Solutions of Cryptograms.

Five solutions are now given, two of Transposition and three of Substitution ciphers.* It is not intended that, by following these solutions, an officer, without giving more time and attention to the subject, should be able unaided to solve cryptograms, but a careful study of these solutions will enable a judgment to be formed of the general factors upon which the security of cipher systems depend.

1. *Solution of Transposition Cipher (in English).*

TRORNMTOIOETCNRRMALGROIACOAOSFGDKCT PTHE
WKFMOHTOIAOOSEFNLNUIELTLATNAHBIENEOMKMYF

The above cryptogram, of which a solution is required, is in the English language, but it is not known by what system or type of system it has been formed. The first point is to determine whether it is some form of Substitution or Transposition cipher. For this purpose the recurrences of different letters are counted and compared with the normal recurrences of these letters. This gives the following result :—

O	occurs	11	times,	I and R	occur	5	times.
N	,,	7	,,	M, F, and L	,,	4	,,
T	,,	8	,,	C, H, and K	,,	3	,,
A and E	,,	6	,,				

G, S, and W occur twice, and P, B, V, D, occur once each.

The above does not agree entirely with the normal scale, for E might be expected to occur more than 6 times. There are, however, no frequent occurrences of unusual letters, such as B, J, X, Y, or Z, so the cipher may be assumed to be some form of letter transposition.

As an illustration of the above, the cryptogram may be compared with the following cipher, which consists of the same letters represented by the letter standing next after each in the alphabet.

USPSONUPJPFUDOSSNBMHSPJBDPBPTGHELDUXQUIF
XLGNPIUPJBPPTFGOMOVJFMUMBUOBICJFOFPNLOZG

It is at once evident that the latter cryptogram is not a transposition of the original letters of the text owing to the frequent

* When studying the solutions given in this chapter, the student should write consecutively the various steps on a sheet of paper to ensure his seeing clearly the material by the aid of which each further step towards solution is made. By this means he will obtain a grasp of the main factors which make a cipher system safe or unsafe to use.

repetition of such letters as U, P, and B, but is some form of letter substitution. An experienced cryptographer can generally determine this point by merely glancing at the cryptogram, for in the case of substitution ciphers, the frequent recurrence of uncommon letters gives the collection of letters an unnatural appearance. If the two cryptograms are compared, the contrast between them will be at once apparent.

It having been decided that the cryptogram is a transposition cipher, the next step is to experiment with the letters and arrange them in different ways, until a sequence of letters is obtained which forms a syllable or a word, and indicates the road to solution. There are 80 letters in the cryptogram and it has therefore probably been written out in a rectangle either 4 × 20, 5 × 16, or 8 × 10.

The letters of the cryptogram, must now be written out in each of the above forms. The first, 4 × 20, gives the following result :—

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

This is not promising in whatever way the letters are read, so the parallelogram, 5 × 16, is next tried :—

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

This is no better, nor is the following, which is a parallelogram of 10 × 8 :—

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

The above rectangles afford no clue, if the letters are read off either horizontally, vertically, diagonally, or by a zigzag method,

or reversed. In no case is any sequence of letters obtained, however short, that indicates the system used. Leaving, therefore, systems by which the letters are written down in horizontal or vertical lines, another form of transposition must be tried in which the letters of the text are written diagonally in a rectangle, starting at one of the corners, and the cryptogram is formed by reading them off in horizontal lines.

A rectangle of 4 × 20 is, as before, first tried :—

T O M O N A O O F C T
R N I C M R C S K P
R O T R G A O D W
T E R L I A G T

The start of the above is not very promising, but the first few letters may form the begining of one or two words, though the rectangle used has not yet been discovered. A 5 × 16 rectangle is next tried, with the following result :—

T O M O R G C
R N I N L A
R O C A I
T T M O
E R R

This result is no better than before, and it can be seen that it is no use to proceed further with the above, so the rectangle 8 × 10 is tried :—

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

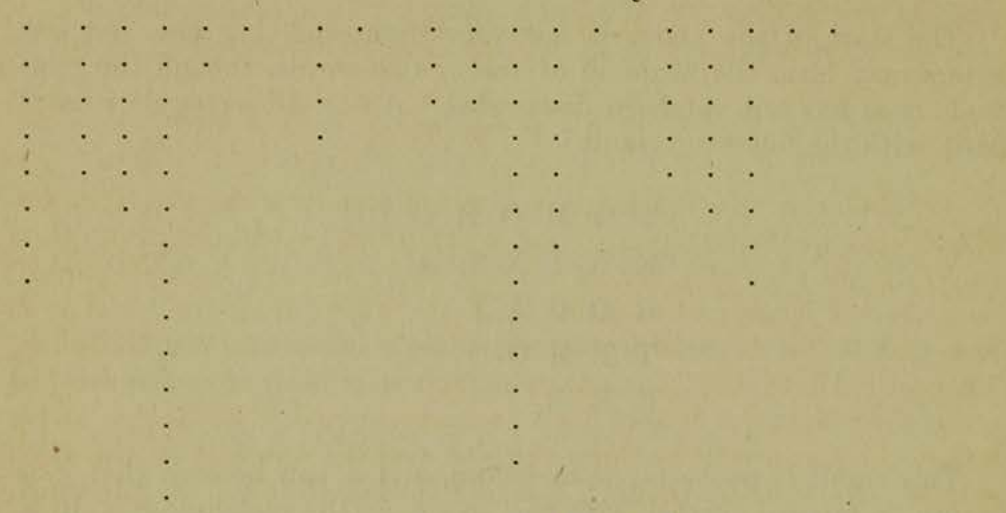
The system has at length been discovered, and by reading off the horizontal lines the text of the message is obtained, "*To-morrow morning at four o'clock an attack will be made on the right flank of the enemy's position.*"

2. *Solution of Transposition Cipher (in French).*

SILRTL	EEEENT	NTDATS	ONCEEE
MNROOF	IRMIDE	NAAPVC	IEANNN
OCOGDE	RRNIET	NDTEOS	DJSCAA
CNNDAE	TMUOSS	ELFNTA	

The above cipher message is in the French language, but the system by which it has been formed is not known. The repetitions of different letters are counted as before in order to ascertain whether it is a Transposition or Substitution cipher. A convenient method of doing this is to write out the alphabet, and to place a dot under each letter every time it occurs, thus :—

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



From the fact that the letters N, E, T, A, S, which occur most frequently in the cryptogram, are among the letters of frequent recurrence in the French language, and that there is no undue proportion of unusual letters, it may be assumed that a transposition and not a substitution method has been used.

The number of letters in the cryptogram is 90, and we conclude, therefore, that it has probably been formed by some arrangement of 10×9, 15×6, 18×5, 30×3, or 45×2 columns of letters. It is improbable that very long columns of letters have been used, as these would be inconvenient to manipulate as well as insecure, for the method of altering the order of the letters would be easily discovered. We commence, therefore, with a rectangle of 10×9 :—

S	I	L	R	T	L	E	E	E
E	N	T	N	T	D	A	T	S
O	N	C	E	E	E	M	N	R
O	O	F	I	R	M	I	D	E
N	A	A	P	V	C	I	E	A
N	N	N	O	C	O	G	D	E
R	R	N	I	E	T	N	D	T
E	O	S	D	J	S	C	A	A
C	N	N	D	A	E	T	M	U
O	S	S	E	L	F	N	T	A

The above diagram furnishes no sequence of letters making a syllable or word from which a clue can be obtained when the

are read off in either vertical, horizontal, or diagonal columns or by a zigzag route ; so the rectangle, 15 × 6, is tried :—

S I L R T *L*
E E E E N T
N T D A T *S*
O N C E E E
M N R O O *F*
I R M I D E
N A A P V *C*
I E A N N N
O C O G D *E*
R R N I E T
N D T E O *S*
D J S C A A
C N N D A *E*
T M U O S S
E L F N T *A*

On first examination no useful result can be obtained from the above, and so the letters are next written out in 18 lines of 5 letters each. Lines of 2 or 3 letters are not likely to have been employed, so a second examination is made of the above diagrams, and it is seen that if the last and first letters of each successive line are taken, LES/OFICIERS/DETA is obtained, and it is clear that the method of writing out the letters has been discovered. With the above letters the last line is reached, and, by working upwards on the same system (*les officiers d'eta*), TMAJORDEVRONTET is obtained. Following the same process, down and up successive columns, the full text of the message can be read :—" *Les oficiers* (*sic*) *d'état-major devront être accompagnés d'un fonctionaire* (*sic*) *de l'intendance dans les cantonnements.*"

In case the method of obtaining the full text of the message is not understood, the following diagram will explain the ingenious system of transposition employed :—

90	61	60	31	30	1
2	29	32	59	62	89
88	63	58	33	28	3
4	27	34	57	64	87
86	65	56	35	26	5
6	25	36	55	66	85
84	67	54	37	24	7
8	23	38	53	68	83
82	69	52	39	22	9
10	21	40	51	70	81
80	71	50	41	20	11
12	19	42	49	72	79
78	73	48	43	18	13
14	17	44	47	74	77
76	75	46	45	16	15

The numbers show the order in which the cipher letters should be read off from the cryptogram.

The above is an illustration of an ingenious form of letter transposition, and the system employed is as difficult to detect as any variation which is likely to be employed in the field.

3. *Solution of a Substitution Cipher (in German).*

The following cryptogram is in the German language, but the system by which it has been formed is not known :—

H W F A W Q K H T O W L O Q P X W T W K O G Q M L W K K B
M L Q K T W Q K W F Z W T O F Q Z W K R J A T O W G G J K
Z H R T A F R K I B T Q T M L W G R Z W F D W Q P B T M B
J A W F P W J K H G W Q U I Q Z T O W L O K B M L

The recurrences of different letters are as follows :—

W = 18 ; K = 11 ; Q and T = 10 ; O = 7 ; L and F = 6 ; G. M. B. Z. = 5 ; H, A, R, J, = 4 ; P = 3 ; I = 2 ; and X, D, and U each occur once. This result admits of no doubt that it is a substitution system, for the letter W occurs 18 times, while there is no E at all, a result quite impossible with a transposition cipher.

From the table of recurrences of letters and combinations of letters in the German language, on page 44, it is clear that W represents *e* in clear, owing to the large number of times it occurs. The letter K, which occurs most frequently after W, probably represents *n*, while either Q or T may be taken to stand for either *r* or *i* ; but, as both occur equally often, there is at present no material to determine which of these letters either represents.

The next step is to count the recurrences of pairs and groups of letters. Of pairs of letters which occur twice or more there are :—

ML, TO, WQ and WF=4 ; and WK=3 ; KH and JK= 2.

The groups of three letters are TOW = 3, and MLW = 2.

The groups of four letters are KBML = 2 ; and of five letters TOWLO = 2.

The next step is to look for a group of letters, among which there is a frequent recurrence of those letters, of which the probable equivalents are known, *i.e.*, W, K, Q, and T. Such a group occurs in the second line of the cryptogram—viz., Q K T W Q K W F ; and if the probable equivalents to the cipher letters are written out, and it is assumed that Q = *r*, and T = *i*, *rnierne*—is obtained. This does not look very hopeful, so the values of Q and T are changed, and Q is taken to stand for i, and T for *r*, which gives us *inreine*, a far more promising result. The last letter of the above group of cipher letters is F following W. It is seen from the above table that WF occurs four times, and so should represent one of the most frequently recurring pairs of letters *en* or *er*. As *F* is not *n*, for it has been assumed that *n* is represented by K, it should be *r*.

This makes the supposition that T=*r* incorrect and gives :—

Q K T W Q K W F
i n e i n e r

Another value for T must now be sought. In order to do this recurrences of T with other letters are examined, and that TO is found to be a frequent combination. According to present assumptions, neither of these letters stands for *e*, *n*, *r*, or *i*, so another pair of frequently recurring letters must be sought, in which none of the above letters occur. These are *ch*, *st*, and *au*.

Ch is improbable, because T in the cryptogram occurs more often than O, whereas, according to the scale of normal recurrences, *c* should occur much less frequently than *h*. The condition that TO represents *st* in clear is next considered, and it is found that on this assumption the recurrences of the individual letters agree better with the normal scale, while the result suits the group under consideration, which now reads :—

"*in seiner.*"

The next step is to consider the first group of letters of the cryptogram, which contain many of the letters of which equivalents have been assumed. If the latter are filled in, the following result is obtained :—

H W F A W Q K H T O W L O
. e r . e i n . s t e . t

With the help of the fact that the 1st and 8th letter of the above line are the same, and that the recurrences of " H " agree fairly well with the normal recurrences of "*d*," it is easy to guess that the first words are "*der Feind.*"

It is now clear that the third word must be *steht*, and that L represents *h* ; and in support of this we have the frequent recurrence of M L, which is probably *ch*. The key alphabet now stands thus :—

A B D F G H I J K L M O P Q R T U W X Z*
f . . r . d . . n h t . i . s . e . .

Another group of letters is now sought, containing a number of letters of which the equivalents are already known and the following letters, which come immediately after the group we have taken to mean "*in seiner,*" are taken :—

Z W T O F Q Z W K R J A T O W G G J K Z H R T
. e s t r i . e n f s t e . . . n . d s

N.B.—The thick letters denote those already determined.

---

* This alphabet contains only those letters which occur in the cryptogram.

The first word of the above, "*gestrigen*," is easily guessed, since the 1st and 7th letters are the same, which gives "*in seiner gestrigen.*" As an aid to making out the next word, the following letters are known :—

. . f s t e . . . n g d . s

It must next be decided what the double letters GG represent, and in the list of recurrences of double letters on page 44 are found—*ee*, *nn*, *ss*, *tt*, *ll*, *rr*, *mm*, *ff*, in this order. It is known that G does not represent *e*, *n*, *s*, *t*, *r*, or *f*, and the double letters must therefore be either *mm* or *ll*. From this it can be seen that the middle of the above group of letters must be the word "*stellung*," which fixes another of the three letters which precede this word. The result is *ufstellung*, of which the initial letter can be supplied, and "*aufstellung*" is written down.

The key alphabet is again written out, omitting as before letters which do not occur in the cryptogram.

A B D F G H I J K L M O P Q R T U W X Z
f . . r l d . u n h c t . i a s . e . g

There now remain only six letters in the cryptogram, which have not yet been determined, and the latter is written out in full, with the text letters beneath as far as these are known :—

H W F A W Q K H T O W L O Q P X W T W K O G Q M L W K K
d e r f e i n d s t e h t i . . e s e n t l i c h e n n

B M L Q K T W Q K W F Z W T O F Q Z W K R J A T O W G G
. c h i n s e i n e r g e s t r i g e n A u f s t e l l

J K Z H R T A F R K I B T Q T M L W G R Z W F D W
u n g d a s f r a n . . s i s c h e l a g e r . e

Q P B T M B J A W F P W J K H G W Q U I Q Z T O W
i . . s c . u f e r . e u n d l e i . . i g s t e

L O K B M L
h t n . c h

Of the unknown letters in the cryptogram B alone is of frequent recurrence. From the table of recurrences it is seen that among the unappropriated letters are o, b, m, f, or z, while in the message the letters *n* . *ch* twice follow the verb *steht*. The word is evidently *noch*, which gives us B = *o*.

There now remains only one group of any size which has not been read— . e i . o s c o u f e r . e, and so few letters are still undetermined, that the above are easily found after a few trials to read, "*bei Moscou Ferme.*"

The whole message is—"*Der Feind steht im wesentlichen noch in seiner gestrigen Aufstellung das französiche Lager bei Moscou Ferme und Leipzig steht noch,*" and the complete alphabet is :—

A B D F G H I J K L M O P Q R T U W X Z
f o b r l d z u n h c t m i a s p e w g

4. *Solution of a Substitution Cipher (Sliding Alphabet Cipher).*

The following cryptogram is in the English language, but the system on which it has been formed is not known. The message contains 94 letters, and the fact that the letter " e " occurs only three times and that " o " and " i " are found only once each proves clearly that it is a substitution cipher.

DDAYNH TXPAQ QB HNTOB CRTPY
SPWQJU UDDLZ XGUP NKAFLJ NTBX
LAGMQ CKCECINUUSYP WARMW CPJYJP
ZAMEMTR HZG QABKGEBM

It may be assumed that the groups of letters in the above cryptogram are conventional, for the help given by the knowledge of the length of each word is not usually afforded in a cipher message, that is to say, if the encipherer knows the first elements of his business. It may further be assumed that the whole of the message was not enciphered in one position of the sliding alphabet, for solution would in that case be a simple matter. It would only be necessary to try various positions of the sliding alphabet until a group of consecutive letters formed a word, and then the whole message could be at once read off. The fact that the cipher commences with a double letter confirms this point. If the position of the sliding alphabet were not changed at each letter, this would indicate that the message commenced with a repetition of the same letter, which is inadmissible in English.

It may be concluded, therefore, that the position of the alphabet is changed at each letter, and the length of the keyword must next be discovered, or, in other words, the number of alphabets employed.

As there are 94 letters in the cryptogram, the keyword is probably repeated many times, and each time that a certain letter in the text is enciphered in the same position of the sliding alphabet, the same cipher letter is obtained. This cipher letter may also be the result of a different letter of the text being enciphered in another position of the sliding alphabet, but it will be found that the length of the key word can usually be determined by counting the intervals, *i.e.*, the number of letters from one to another recurrence of the same cipher letter. If there are recurrences of the same pairs of letters, or o groups of three or more similar letters, the length of the keyword can be fixed with certainty. Having counted and compared these intervals, it will be found that, as a rule, there is only one factor which is common to the majority of them, and this factor indicates the length of the keyword.

The intervals between the recurrences of different letters in the above cryptogram are as follows :—

D D .....30.
A .....7, 31, 9, 17, 11, 10.
Y .....19, 41, 10.
N .....10, 24, 6, 15.
H .....8, 70.
T .....9, 5, 25, 36.

The recurrence of D D gives us $30 = 5 \times 6$.
" " " A " " $31 + 9 = 40 = 5 \times 8$, and $10 = 5 \times 2$.
" " " Y " " $19 + 41 = 60 = 5 \times 12$, and also 10.
" " " N " " 10, and 15, and $24 + 6 = 30 = 5 \times 6$.
" " " H " " $70 = 5 \times 14$.
" " " T " " 5 and 25.

In many cases two adjacent intervals between recurrences have been added together, for it is clear that the eventual position of the sliding alphabet will be the same if it is moved 25 times continuously, or 9 times and then 16 times. It will be at once seen from the foregoing table that the ruling factor is 5, and it may safely be assumed that the keyword contains 5 letters.

The letters of the cryptogram are now written out in 5 columns of letters.

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

The next step is to count the recurrences of the letters which occur most frequently in each column, and this gives the following result :—

In Column 1, G occurs 4 times, and T occurs 3 times.
In Column 2, Q occurs 3 times.
In Column 3, A and B both occur 3 times.
In Column 4, Y and M both occur 3 times.
In Column 5, N occurs 4 times, and K 3 times.

In addition to the above, various letters occur twice in the different columns, but these double occurrences do not afford sufficiently definite material on which to base preliminary deductions, and need not at present be considered.

Assuming that each of the letters which occur more than twice in any column represents *e*, equivalents are then written for the first 5 letters in each column, in the positions of the sliding alphabet in which the most frequently recurring letters represent *e*, thus :—

Column 1.—When G represents *e*, the first 5 letters obtained are *b f o r r*

„ T „ *e*, „ „ 5 letters obtained are *o s b e e*

Column 2.— „ Q „ *e*, „ „ 5 letters obtained are *r h e c d*

Column 3.— „ A „ *e*, „ „ 5 letters obtained are *e b f f c*

„ B „ *e*, „ „ 5 letters obtained are *d a e e b*

Column 4.— „ Y „ *e*, „ „ 5 letters obtained are *e v n i y*

„ M „ *e*, „ „ 5 letters obtained are *q h z u k*

Column 5.— „ N „ *e*, „ „ 5 letters obtained are *e r e i g*

„ K „ *e*, „ „ 5 letters obtained are *h u h l j*

A consideration of the above series points to the second series in columns 4 and 5 being probably incorrect, owing to the occurrence of so many unusual letters. If these are eliminated and the remainder written out, the following is obtained :—

b	*e*	*f*	*b*	*o*	*f*	*r*	*f*	*r*	*c*					
r	*ee*	*h*	*vr*	*e*	*ne*	*c*	*ii*	*d*	*yg*					
o	*d*	*s*	*a*	*b*	*e*	*e*	*e*	*e*	*b*					

If the upper alternative line of the above is discarded, and the remainder written out, the result is as follows :—

Ordees havr been eeceiied byg

It is evident that the fifth column requires re-adjustment, and that the first cipher letter, N, in this column must represent *r*.

With the sliding alphabet in this position, the equivalents for the first five letters of the fifth column are as follows :—*r e r v t*, and the beginning of the message now reads as follows :—

Orders have been received by t , &c.

The message can now be read off, each of the 5 columns being deciphered in the positions of the sliding alphabet, which give the above results, thus :—

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

Keyword.—If the sliding alphabet is placed successively in the positions in which the columns of letters have been read off, and the letter of the sliding alphabet which is under the A of the fixed alphabet in each of these positions is taken, the keyword *LODGE* is obtained.

It is to be noted, however, that the knowledge of the keyword is not necessary to the solution of a sliding alphabet cipher. It is, of course, necessary to know the keyword in order to encipher or decipher a message quickly, but it should be remembered that when solution has to be effected the determination of the keyword is the last step in the solution, and follows, not precedes, the reading of the message. Solution is invariably effected by counting the recurrences of certain letters in cipher, and by comparing these recurrences with the normal recurrences of certain letters in the language of the message.

Solution of Sliding Alphabet Cipher (in French).

The following is a solution of a message which was sent from London to the *Agence Havas* about the time of the British military operations in Egypt in 1882 :—

RBNBJ — JHGTS — PTABG — JXZBG — JICEM — QAMUW — IVGAG — NEIMW — REZKZ — SUABR — RBPBJ — CGYBG — JJMHE — NPMUZ — CHGWO — UDCKO — JKKBC — PVPMJ— NPGKW— PWADW— CPBVM — RBZBH — JWZDN — MEUAO— JFBMN— KEXHZ— AWMWK—AQMTG — JVGHC — QBMWL— ZEUKW — RETEW — CPBVM — CBAMN — RBJCZ — EAUUZ — KBCBX — RBJEJ — DTEDR — LKCEY — IFBHX — JHSBO— DFEHK — ZAAAK — SWMVZ — SKAUZ — IKCDR — UBAVL— NJSBJ — SBPAL — GDYFZ — GBAQK — NBAUZ — GDPVR— SAJEX — NDUBJ — GDUJX — LMXJL — SKKBO — HANMZ— IUGWO — RBJEJ — DTMKZ — SBSBE — DWZMJ — JQGJX— JZMKZ — JJYHG — DTXIJ — JUYPV — JVXWA — JLMHC— JJBSO — CEJTZ — IJBWX — EEXWX — JWGWX — JWSBE— JJMKX — LDXJH — DPOAJ — JJTDJ — CTMJZ — LQXPZ— HMJEH—UEUIG—DAAUW—IVGAG—NE.

The fact that Z occurs 22 times is alone sufficient to prove clearly that the cryptogram has been formed by some Letter Substitution system, and it may be assumed to be some variety of the Sliding Alphabet cipher, as this is by far the most common form of letter substitution. The next step is to ascertain the number of letters in the keyword, or, in other words, to find out the number of different alphabets used.

For this purpose repetitions of pairs of letters or groups of 3 or more similar letters are noted, and the letters from the beginning of one to the beginning of another of these repetitions are counted. If repetitions of groups of 3 or 4 letters are found, it may safely be assumed to result from the same group of letters in the message being enciphered in the same positions of the sliding alphabet, but if such groups are not available, the intervals between pairs of letters must be counted.

An examination of the cipher gives the following table :—

RB — ' R B '*	= 55	= 11	× 5
RB — " R B "	= 105	= 21	× 5
BJ — ' B J '	= 50	= 10	× 5
BJ — " B J "	= 225	= 45	× 5
BG — ' B G '	= 5	= 5	
BG — " B G "	= 40	= 8	× 5
RE — ' R E '	= 115	= 23	× 5

The above table includes less than half the repetitions which occur in the cryptogram, but shows clearly that the key must be a word of 5 letters. Indeed, this might have been guessed from the repetitions of *RB* alone, for 5 is the greatest common factor of 55 and 105 (*vide* table above). It is safer, however, to collect sufficient data to enable the length of the keyword to be determined with certainty.

The next step is to divide the cryptogram into 5 columns of letters, and to count the repetitions of different letters in each column.

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

* The single and double inverted commas denote the second and third recurrences of the pairs of letters respectively.

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

The number of times different letters occur in the above columns is as follows :—

1st column.—20J, 8R, 7D, 7N, 7S, 7C, 6I, 4L, 4G, 3P, 3U, 2H, 2K, 2Q, 2E, 2A, 2Z, 1M.

2nd column.—14B, 10E, 7W, 7J, 6A, 5P, 5T, 5V, 6D, 5K, 4F, 3U, 3H, 3Q, 2M, 1L, 1I, 1Z, 1G, 1X.

3rd column.—12M, 10A, 8G, 6X, 6J, 6U, 6B, 5C, 5Z, 4S, 4P, 4Y, 2K, 2N, 2E, 1Q, 1I, 1O, 1T.

4th column.—14B, 8W, 7E, 7H, 7K, 6U, 6A, 5M, 5V, 5D, 5J, 3T, 2P, 2I, 1S, 1C, 1F, 1Q.

5th column.—15Z, 11J, 9X, 8G, 7W, 7O, 3L, 4K, 4R, 3C, 3H, 3M, 3N, 3E, 1A, 1V, 1S.

As the cryptogram is of some length, the letter which occurs most often in each column may be taken to represent *e*, with the result that the second and fourth columns (in both of which *B* occurs most often) represent the same alphabet. A further proof that these 2 columns represent the same alphabet is to be found in the fact that in each of them the cipher letters E and W occur, with the exception of B, more frequently than any others.

The next step, which is of especial value to the solution of military cryptograms, is a consideration of the probable contents of the message, and of words and phrases, names of persons and places, &c., which may be expected to occur. It is known that the message was sent at the time military operations were being carried out in Lower Egypt, and consequently such words as *Arabi, Wolseley, Suez, Ismailia, Canal, général, soldat*, &c., may be expected to occur.

Of the first 10 letters in cipher, 3 have been already guessed, for the letter which occurs most frequently in each column has been taken to represent *e*.

R	B	N	B	J
	E*		**E**	
J	H	G	T	S
E				

Having reached this stage the manner in which a message of this nature generally begins must be considered, and in this as in almost all the steps towards solution, the method of elimination is employed. Instead of trying by a short cut to guess at a particular phrase or word, the various words and phrases which might possibly occur are considered, and those which do not fulfil the necessary conditions rejected.

It is improbable that the opening phrase of a message of considerable length is either interrogative or imperative; if, then, the first word is a verb, it will be either in the infinitive mood or in the form of the present participle. The simple style of communications of this nature to newspapers precludes the use of the infinitive; moreover, it is not a present participle, for, if so, it must be a verb

* Letters which have been already determined or guessed are printed in thick type.

of which the three first syllables of the present participle all contain the letter *e*. *Régénérant*, the present participle of the verb *régénérer*, is the only word which fulfils this condition, but it is unlikely to occur in a communication of this nature, and it may be assumed, therefore, that the first word of the cipher is not a verb.

It may here be explained that if one or more letters of a word as well as its length and position in a sentence be known, it will usually be found, by working with a small dictionary, that the number of words of the required length which comply with the necessary conditions is comparatively few, and it will generally be a matter of choice between only a few alternatives.

It having been decided that a verb is not the initial word of the cipher, substantives are next considered, and it is found that all but proper names are invariably preceded by some qualifying word, and can therefore be discarded ; this applies also to adjectives, with the exception of *divers*, *différent*, *maint* and *certain*, which alone could begin a sentence without being preceded by *de*, and these four words have not the letter *e* where required.

Among names of persons and places which might be exvected to occur in the despatch, there are none with an *e* in the required syllables ; and for the same reason adverbs, prepositions and conjunctions can be rejected.

The first letter, therefore, of the message cannot be either a verb, a substantive, an adjective, a proper name, an adverb, a preposition or a conjunction. It must therefore be either the article *le*, *les*, the pronouns *je*, *me*, *ce*, *cet*, *ces*, *mes*, *ses*, the negative *ne*, or the preposition *de*.

If the first word is the negative *ne*, a verb in the present participle must follow it, for the only other alternatives in the French language are not probable at the commencement of the message. It has already been stated that the opening phrase is not likely to be an interrogation or imperative ; it cannot be an infinitive in the negative for in that case *pas* must follow *me*, and this does not fall into line with the *e*'s already fixed. Another possible alternative is *ne* immediately followed by the infinitive and then by *que*, but this is an unlikely commencement to the message.

If, then, *ne* must be followed by a present participle, it must be some such word as *revenant* or *reçevant* (there are few words with an *e* in each of the first two syllables), and in both the above cases the cipher letters GTS would represent the termination *ant*. On reference to the table of recurrences, it is found that the cipher letter S only occurs once in the fifth column, and it is not likely, therefore, to represent *t*, which is a very common letter in French, and consequently *ne* followed by a present participle may be rejected.

The words *les*, *cet*, *ces*, *mes*, *ses*, may also be rejected, for the third cipher letter N only occurs twice in its column, and is not likely, therefore, to be the common letters *s* or *t*. Similarly, the first cipher letter R occurs 8 times in its column and cannot therefore represent *j* (*je*) ; the first word then must be *ce* or *le*, and it is more probably *le* than *ce*, because *l* is in French a more common letter than *c* and the cipher letter R occurs frequently, and also because *le* is extremely likely to be the first word of a message.

It may, therefore, be assumed that the first word is *le* or *ce*, preferably the former; it will probably be followed by a substantive, an adjective or an adverb of number, and it must be remembered that the word must have an *e* in each of the first two syllables. No adverb of number complies with this last condition; the adjectives *récent*, *décent* and *téméraire*, which have the two e's, must also be rejected, because the cipher letter H which would represent *n* occurs too seldom in the second column to stand for such a common letter as *n*; *détéstable* can also be rejected because the final letter *e* would be represented by T in the second column, whereas *e* in the second column has been assumed to be represented by the cipher letter B. It will be found on examination that *désert* and *télégraphe* must also be rejected, and the only word which complies with the necessary conditions is *général*, and in consequence the first word is taken to be *le* and not *ce*.

The next step is to fill in these two words, and to continue the same process :—

R	B	N	B	J
l	*e*	*g*	*e*	*n*
J	H	G	T	S
e	*r*	*a*	*l*	
P	T	A	B	G
			e	
J	X	Z	B	G
e			**e**	

The thick letters in the above table have been already fixed, and will help the deciphering of the next word.

It is probable that the despatch states to which general it refers; a proper name must, therefore, be looked for next. The cipher letter S which begins the word must represent an unusual letter of the alphabet, such as *k*, *w*, *y*, *z*, for it occurs only once in its column; moreover, there is an *e* in the fifth and seventh spaces, and this last *e* is followed by another unusual letter for the cipher letter occurs only once in its column; this all points to *Wolseley*.

It may be here remarked that, if the sliding alphabet had been employed with the normal order of the letters unchanged, the whole cryptogram could have been read off when the first words were guessed, but in this case it is obvious on trial with a " slider " that a conventional alphabet has been used, and so the process adopted must be repeated, until a sufficient number of letters have been fixed to enable the remainder to be guessed and the cryptogram read.

The solution has now reached the following point :—

R	B	N	B	J
l	*e*	*g*	*e*	*n*
J	H	G	T	S
e	*r*	*a*	*l*	*w*
P	T	A	B	G
o	*l*	*s*	*e*	*l*
J	X	Z	B	G
e	*y*		**e**	**l**
J	I	C	E	M
e				
Q	A	M	U	W

The data available for the determination of the next word are as follows :—

The 2nd, 3rd and 4th letters are known ; the letter M in the 3rd column probably represents *e*, and the first letter represented by the cipher letter Z occurs frequently, and must be one of the commonly used letters of the alphabet.

If Z represents the auxiliary verb *a*, the participle which follows must be *élevé* or *électrisé*, but the final *e* of these words does not in either case fit in with the conditions. The verb, therefore, must be in a simple tense. The only possible verbs are *dépend*, *dément*, *mène*, *retenu*, and *télégraphie*, and of these the last alone fulfils all the conditions. This word having been fixed, the solution is again written out as far as it has gone :—

R	B	N	B	J
l	*e*	*g*	*e*	*n*
J	H	G	T	S
e	*r*	*a*	*l*	*w*
P	T	A	B	G
o	*l*	*s*	*e*	*l*
J	X	Z	B	G
e	*y*	*t*	*e*	*l*
J	I	C	E	M
e	*g*	*r*	*a*	*p*
Q	A	M	U	W
h	*i*	*e*		
I	V	G	A	G
		a		l
N	E	I	M	W

It is known that G in the 3rd column represents *a*, and G in the 5th column *l*, and it may be assumed that *télégraphie* is followed either by *que* or *qu'il*, or by the name of a place, preceded by *de* or *d'*. It is not *que*, because *e* is not represented in the 1st column by I in cipher ; similarly it is not *qu'il*, because *l* is not represented in the 2nd column by V in cipher.

The name of a place preceded by *de* or *d'* must, therefore, be sought, and all the probable places in Egypt from which the telegram may have been despatched must be considered. There are few of these having the letters A and L in the required places, and *d'Ismailia* is easily guessed.

The solution as far as completed is again written out, and the letters immediately following, which are known, are again shown in thick type. To these letters may be added Z, as representing *e* in the 5th column, for Z occurs 16 times in this column.

R	B	N	B	J
l	*e*	*g*	*e*	*n*
J	H	G	T	S
e	*r*	*a*	*l*	*w*
P	T	A	B	G
o	*l*	*s*	*e*	*l*
J	X	Z	B	G
e	*y*	*t*	*e*	*l*
J	I	C	E	M
e	*g*	*r*	*a*	*p*
Q	A	M	U	W
h	*i*	*e*	*d'*	*i*
I	V	G	A	G
s	*m*	*a*	*i*	*l*
N	E	I	M	W
				i
R	E	Z	K	Z
l	a	t		e
S	U	A	B	R
i	*a*	s	e	
R	B	P	B	J
l	e		e	n
C	G	Y	B	G

The wording of the opening phrase and the letters *il* point to the next letters being *qu'il*. The verb must follow, and at first sight is not easy to guess; so the next group of letters is considered, and the word *Seulement* is easily recognized. Then, the 1st, 2nd, and 4th letters of the verb being known, as well as its length, a dictionary soon shows that the word sought for is *attend*.

The solution has now reached the following stage :—

R	B	N	B	J
l	*e*	*g*	*e*	*n*
J	H	G	T	S
e	*r*	*a*	*l*	*w*
P	T	A	B	G
o	*l*	*s*	*e*	*l*
J	X	Z	B	G
e	*y*	*t*	*e*	*l*
J	I	C	E	M
e	*g*	*r*	*a*	*p*
Q	A	M	U	W
h	*i*	*e*	*d*	*i*
I	V	G	A	G
s	*m*	*a*	*i*	*l*
N	E	I	M	W
i	*a*	*q*	*u*	*i*
R	E	Z	K	Z
l	*a*	*t*	*t*	*e*
S	U	A	B	R
n	*d*	*s*	*e*	*u*
R	B	P	B	J
l	*e*	*m*	*e*	*n*
C	G	Y	B	G
t			e	l
J	J	M	H	E
e		e		
N	P	M	U	Z
i		e	d	e

Of the letters immediately following the last word determined, if *le* is assumed to be a word, there are three letters, of which the last is *e*, for the first word. The first of these three cipher letters occurs only once in its column, which points to one of the letters *k*, *w*, *y*,

z, *q*, while the second letter also occurs seldom. From these data the word may be taken to be *que*, which gives :—

que le . e . . i . e de.

It is known that the first letter of the word sought is a consonant, if the assumption regarding *le* is correct, and that this consonant is represented by a cipher letter which occurs frequently. The letter should, therefore, be among the group E S A N T I R, the group of most frequently occurring letters in French, and this applies also to the 3rd letter of the word. In the 2nd column, of the group of letters E S A N T I R, *e*, *a*, and *i* have been fixed, and in the 4th column *e*, *a*, *t*, and *i*. This reduces considerably the number of possible alternatives, and a few trials will enable the blanks to be filled up thus :—

que le service de.

It will be seen from the following table that the next stage in the solution is easily arrived at :—

J	J	M	H	E
e	*s*	*e*	*r*	*v*
N	P	M	U	Z
i	*c*	*e*	*d*	*e*
C	H	G	W	O
t	r	a		
U	D	C	K	O
		r	t	
J	K	K	B	C
e			e	
P	V	P	M	J
o	m	m	u	n
N	P	G	K	W
i	c	a	t	i
P	W	A	D	W
o				
C	B	B	V	M

From the above *le service de transports et de communication* (*sic*) is easily read. It must be borne in mind that to fill in the blanks the table of recurrences of letters is always available. A comparison of the normal recurrences of various letters with the recurrences of these letters in the cipher generally points to one of a few letters

being that which is sought. The effect of this is to decrease the work of deciphering, for trials need only as a rule be made with a few letters.

The next passage to be deciphered is as follows :—

N	P	G	K	W
i	*c*	*a*	*t*	*i*
P	W	A	D	W
o	*n*	s		i
C	P	B	V	M
t	c			p
R	B	Z	B	H
l	e	t	e	
J	W	Z	D	N
e	n	t		
M	E	U	A	O
	a		i	s
J	F	B	M	N
e			u	
K	E	X	H	Z
	a		r	e
A	W	M	W	K
	n	e	n	
A	Q	M	T	G
		e	l	l
J	V	G	H	C
e	m	a	r	c
Q	B	M	W	L
h	e	e	n	
Z	E	U	K	W
	a		t	

If the recurrences of the cipher letters, of which the equivalents are not yet known, are again compared with the normal recurrences of these letters, it will be seen from the above table that the sentence reads : *soit complètement organisé pour faire une nouvelle marche en avant.*

It is not necessary to follow the solution in detail beyond the above point ; the complete message can now be read as follows :—

Le général Wolseley télégraphie d'Ismailia qu'il attend seulement que le service de transports et de communication (sic) soit complétement organisé pour faire une nouvelle marche en avant, il a fait compte sur le chemin de fer et le canal pour transporter les approvisionnements des troupes mais l'ennemi a coupé ces voies de communication en construisant des digues dans le canal et en élevant une vaste jetée sur la ligne du chemin de fer. Ces obstacles sont maintenant enlevés et trois machines font le service du camp anglais d'Ismailia.

The following table shows the complete cipher and decipher. The capital letters represent the cipher letters, and the small letters those of the text :—

R	B	N	B	J
l	*e*	*g*	*e*	*n*
J	H	G	T	S
e	*r*	*a*	*l*	*w*
P	T	A	B	G
o	*l*	*s*	*e*	*l*
J	X	Z	B	G
e	*y*	*t*	*e*	*l*
J	I	C	E	M
e	*g*	*r*	*a*	*p*
Q	A	M	U	W
h	*i*	*e*	*d*	*i*
I	V	G	A	G
s	*m*	*a*	*i*	*l*
N	E	I	M	W
i	*a*	*q*	*u*	*i*
R	E	Z	K	Z
l	*a*	*t*	*t*	*e*
S	U	A	B	R
n	*d*	*s*	*e*	*u*
R	B	P	B	J
l	*e*	*m*	*e*	*n*

C	G	Y	B	G
t	*q*	*u*	*e*	*l*
J	J	M	H	E
e	*s*	*e*	*r*	*v*
N	P	M	U	Z
i	*c*	*e*	*d*	*e*
C	H	G	W	O
t	*r*	*a*	*n*	*s*
U	D	C	K	O
p	*o*	*r*	*t*	*s*
J	K	K	B	C
e	*t*	*d*	*e*	*c*
P	V	P	M	J
o	*m*	*m*	*u*	*n*
N	P	G	K	W
i	*c*	*a*	*t*	*i*
P	W	A	D	W
o	*n*	*s*	*o*	*i*
C	P	B	V	M
t	*c*	*o*	*m*	*p*
R	B	Z	B	H
l	*e*	*t*	*e*	*m*
J	W	Z	D	N
e	*n*	*t*	*o*	*r*
M	E	U	A	O
g	*a*	*n*	*i*	*s*
J	F	B	M	N
e	*p*	*o*	*u*	*r*
K	E	X	H	Z
f	*a*	*i*	*r*	*e*
A	W	M	W	K
u	*n*	*e*	*n*	*o*

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

Z	A	A	A	K
v	*i*	*s*	*i*	*o*
S	W	M	V	Z
n	*n*	*e*	*m*	*e*
S	K	A	U	Z
n	*t*	*s*	*d*	*e*
I	K	C	D	R
s	*t*	*r*	*o*	*u*
U	B	A	V	L
p	*e*	*s*	*m*	*a*
N	J	S	B	J
i	*s*	*l*	*e*	*n*
S	B	P	A	L
n	*e*	*m*	*i*	*a*
G	D	Y	F	Z
c	*o*	*u*	*p*	*e*
G	B	A	Q	K
c	*e*	*s*	*v*	*o*
N	B	A	U	Z
i	*e*	*s*	*d*	*e*
G	D	P	V	R
c	*o*	*m*	*m*	*u*
S	A	J	E	X
n	*i*	*c*	*a*	*t*
N	D	U	B	J
i	*o*	*n*	*e*	*n*
G	D	U	J	X
c	*o*	*n*	*s*	*t*
L	M	X	J	L
r	*u*	*i*	*s*	*a*
S	K	K	B	O
n	*t*	*d*	*e*	*s*

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

E	E	X	W	X
m	*a*	*i*	*n*	*t*
J	W	G	W	X
e	*n*	*a*	*n*	*t*
J	W	S	B	E
e	*n*	*l*	*e*	*v*
J	J	M	K	X
e	*s*	*e*	*t*	*t*
L	D	X	J	H
r	*o*	*i*	*s*	*m*
D	P	O	A	J
a	*c*	*h*	*i*	*n*
J	J	T	D	J
e	*s*	*f*	*o*	*n*
C	T	M	J	Z
t	*l*	*e*	*s*	*e*
L	Q	X	P	Z
r	*v*	*i*	*c*	*e*
H	M	J	E	H
d	*u*	*c*	*a*	*m*
U	E	U	I	G
p	*a*	*n*	*g*	*l*
D	A	A	U	W
a	*i*	*s*	*d*	*i*
I	V	G	A	G
s	*m*	*a*	*i*	*l*
N	E			
i	*a*			

Alternative solution, by employing the "Law of Symmetry of Position."

When solving a cipher message of this class, a point will be reached when several letters have been determined in one alphabet and one at least of those letters in one of the remaining alphabets.

Thus at the stage shown at the bottom of page 66, a table may be drawn up as under. The alphabet at the top of the table represents the equivalents *in clear* of the 15 cipher letters (spread over

the 5 conventional alphabets used), of which the meanings have been already determined. These cipher letters are represented by capital letters, shown under the top 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
Equivalents in clear																											
Conventional alphabets	1st						J						R				P										
	2nd						B						T							H						X	
	3rd	G						N												A							
	4th						B						T														
	5th												G		J									S			

The following procedure is then adopted :—

J is common to the 1st and 5th alphabets ; in the 1st alphabet R follows in the 7th space after J and can therefore be located in the same relative position to the letter J in the 5th alphabet, *see* table below. Similarly P, which is in the 3rd space after R in the 1st alphabet, must occupy the 3rd space after R in the 5th alphabet. In the same way G and S may be transferred from the 5th to the 1st alphabet. The same procedure can be continued and H and X from the 2nd can be located in the 4th alphabet, which is the same as the second alphabet, and the table will now appear as follows :—

		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
Equivalents in clear																											
Conventional alphabets	1st			*G*		J			*N*				R		*S*	P						*A*					
	2nd					B							T							H						X	
	3rd	G		*J*			N			*R*			*S*	*P*						A							
	4th					B							T							*H*						*X*	
	5th				*A*								G		J								*R*		S	*P*	

The equivalents of 29 cipher letters are now known, and by the use of another group of letters taken from the cryptogram it will be found possible rapidly to increase the number of such equivalents. In fact, once the equivalent of any cipher letter has been obtained in any *one* of the Conventional Alphabets, that cipher letter may be considered determined for *all* the alphabets.

From the above it will be seen that a Conventional Alphabet gives little more security than an ordinary alphabet if a long message is enciphered.

Certain systems have been devised which make the above method of solution impossible. In these systems a different conventional alphabet is used for each different position of the sliding alphabet. The use of such systems in the field would cause considerable delay and probably lead to frequent mistakes, and they are therefore not suitable for military purposes.

CHAPTER V.

Cipher Systems not described in Chapter III.

Letter Transpositions—Word Transpositions—Substitution ciphers—Miscellaneous ciphers.

Diagonal Transposition Cipher.

In this cipher the letters of the text are written in diagonal lines, the first letter being written in one of the corners of the diagram used. The size of the square or rectangle, or the number of letters in each column must be agreed upon beforehand by the correspondents.

Supposing each column were to contain 8 letters and the message "A reconnaissance made yesterday across the river found no traces of the enemy" were to be sent, it would first be written out as follows :—

a	e	n	s	e	e	y	h	o
r	o	i	c	y	a	t	f	r
c	a	n	e	d	s	r	t	f
n	a	d	r	s	e	o	o	n
s	a	e	o	v	n	s	e	f
m	t	r	i	d	e	e	y	t
s	c	r	n	c	h	m	l	t
a	e	u	a	t	e	u	s	o

The following figures show the order in which the letters are written out :—

1	3	6	10	15,	&c.
2	5	9	14		
4	8	13			
7	12				
11					&c.

The cryptogram is then formed by writing out the lines of letters :—

A E N S E E Y H O R O I C Y A T F R C A N E D S, &c.

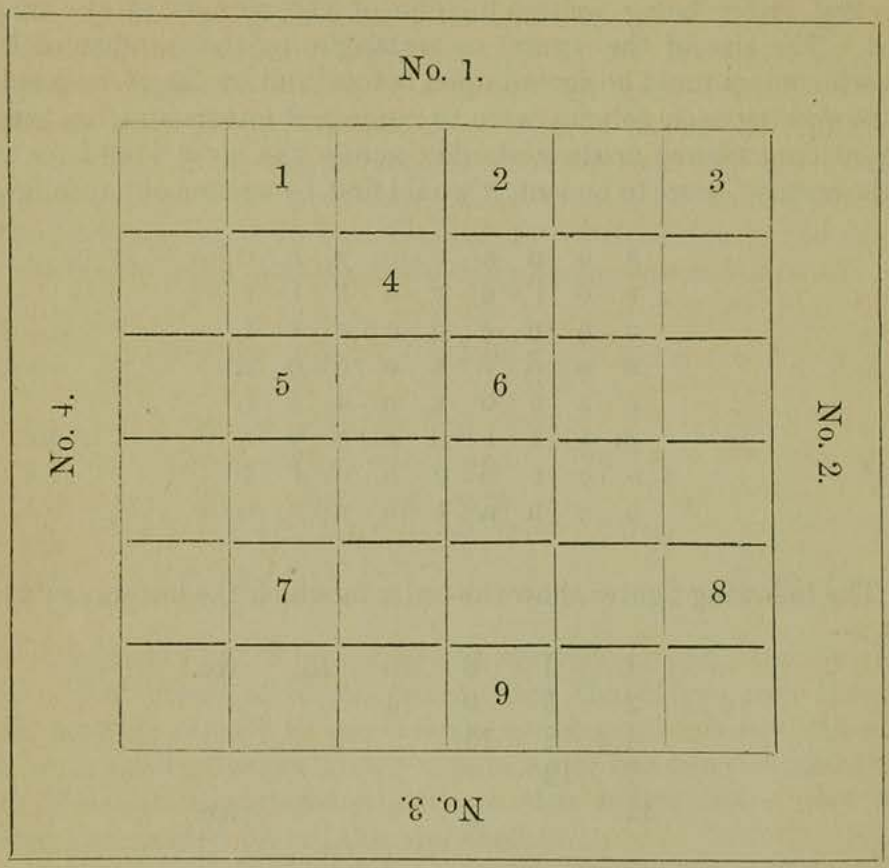
The above method could be varied by commencing at any other corner of the rectangle.

In order to decipher such a cryptogram, the receiver divides the total number of letters by the number in each column which in this case is 8. The quotient represents the number of lines, and the cryptogram is then written out in lines containing this number of letters and the text read off in diagonal lines as above.

Stencil Cipher.

This is a form of transposition cipher which has the advantage of being easy to work, equally well suited to the transposition either of words or letters, and of affording great security provided that the key is not lost or captured. The capture of the key by the enemy would destroy all security, while if the key were lost or temporarily mislaid, messages could neither be read nor enciphered. Consequently the system is unsuited to use in the field.

In order to use this system each correspondent must have a key consisting of a square card or paper, from which certain spaces have been cut out according to a pattern agreed upon. The card may be divided into any number of spaces, the security of the system being in proportion to the number of such spaces. If six spaces in each side were agreed upon, the card might have the following pattern :—



The numbers indicate spaces which are cut out of the card.

In order to encipher a message, the stencil card is laid on a piece of paper with the edge marked No. 1 uppermost, and the letters* of the text are written through the holes in the lines from top to bottom and from left to right. When all the holes have thus had a letter written in them, the card is moved and replaced with the edge marked No. 2 uppermost. The holes will now cover blank spaces in which the writing of the letters of the text is continued in the same manner as before till the spaces are filled up ; the same process is

* In word transpositions, words are written through the holes, instead of letters.

repeated with No. 3 and No. 4 edges uppermost. If the message does not contain as many letters as there are spaces in the card, the spaces which are unoccupied after the message is completed should be filled up with dummy letters. If there are more letters in the message than there are spaces in the card, a second table of letters can be constructed using exactly the same method.

If the following message—"The headquarters of the first army corps will be at York"—were to be enciphered with the card already described, the following result would be obtained :—

a	t	h	h	r	e
e	m	h	y	f	e
t	e	e	a	o	r
r	s	i	p	r	s
o	d	f	s	t	q
t	w	a	u	r	i

The remainder of the message would then be enciphered in the same manner, and would form a second table. The cryptogram would then be written out as follows :—

ATHHR EEMHY FCTEE, &c.

The construction of the card presents no difficulties, but care must be taken not to cut out a square which, in some new position of the card, will expose a space which has already been occupied. This can be avoided as follows :—When any space is selected to be cut, mark the three other spaces which would occupy the same position when the card is moved round, so that none of these spaces may be cut out. For instance, the space marked 3 having been selected, the remaining corner spaces would be marked, as, if any of these spaces were cut out, the movement of the card would show the letter already written in No. 3.

To render cryptograms formed on this system more difficult to solve, one or other of the following plans may be adopted :—

1. Before beginning to write out the text, lay the card face downwards on the paper with the edge No. 3 (or any other agreed on) uppermost, and with the card in this position write down arbitrary letters till each space has been occupied ; then turn the card face upwards and write the text as before, avoiding any spaces which are found to be already occupied.

2. The order of the positions of the card may be changed by agreement. For instance, instead of taking the order 1, 2, 3, 4, the arrangement might be 3, 1, 4, 2, &c.

It should be remembered that this cipher, in common with all transposition systems, affords no security in the case of a short message. For instance, if the words "Mobilization completed" had to be sent, it would be impossible, by any system of transposition, to mix up the letters so as to prevent the text being easily obtained by a series of trials.

Federal Army Cipher (B).

This is a development of the Federal Army Cipher (A), *see* page 27. In this cipher there were two alternative code words for each general or prominent officer in both armies, and for prominent civilians. A portion of the code was as follows :—

Adam ..	President of U.S. ..	Asia.
Abel.. ..	Secretary of State..	Austria.

Generals.

Archery ..	G. B. McClellan ..	Ark.
Bangor ..	U. S. Grant ..	Bengal.

Naval Officers.

Bethune ..	Faragut ..	..	Blanchard.
Bonner ..	Wilkes ..	..	Bishop.

Rivers.

Gem.. ..	Potomac ..	..	Ginseng.
Girdle ..	Rapidan ..	..	Granada.

There were also code words to indicate the time of day, places, Governors of States, Confederate Generals, and miscellaneous expressions in common use, each with two equivalents, the total number of entries being no less than 400.* Similarly, there were several words to indicate various combinations of lines and columns, thus :—

Message of five lines ; commencement words :

Cairo ..	Four columns.	Congress	Five columns.	Calhoun ..	Six columns.
Curtin ..		Coldburn		Church ..	
Cavalry		Childs ..		Cobb ..	

The following routes for the different number of columns were agreed upon :—

Six column route.—Up the 6th, down the 5th, up the 4th, down the 3rd, up the 2nd, down the 1st.

Five column route.—Down the 5th, up the 1st, down the 4th, up the 3rd, up the 2nd.

Four column route.—Down the 4th, down the 2nd, down the 1st, down the 3rd.

Routes were also agreed upon for each of the remaining number of columns from 3 to 10.

---

* It is evident that such a long list of code words could not be remembered, and consequently the system has the disadvantage of all codes.

In this cipher the following "route" was also introduced, the true sequence of the words being indicated by the figures :—

Six Column Route.

6*	17	27	36*	26*	16*
7	5	28	35	25	15
8	18	4	34	24	14
9	19	29	3	23	13
10	20	30	33	2	12
11*	21*	31*	32	22	1

In this "route" a blind word without meaning was introduced after each number marked with an asterisk.

In later ciphers used during the war the same principle was observed, but the code portion of the key was increased in size. In order to increase the security of the cipher, in case of a copy of the key being captured, the instructions as to the route were conveyed by tables like the following :—

	3		7		4		2
8		10		14		12	
	13		11		9		
6		5		1			

In this table the two centre lines are introduced to deceive the uninitiated. The upper line indicates the columns that are to be read from top to bottom, and the lower line those that are to be read upwards. The above route would be up the 6th, down the 3rd, up the 5th, down the 7th, up the 1st, down the 4th, and down the 2nd. The number of columns is shown by the highest figure in the top or bottom line.

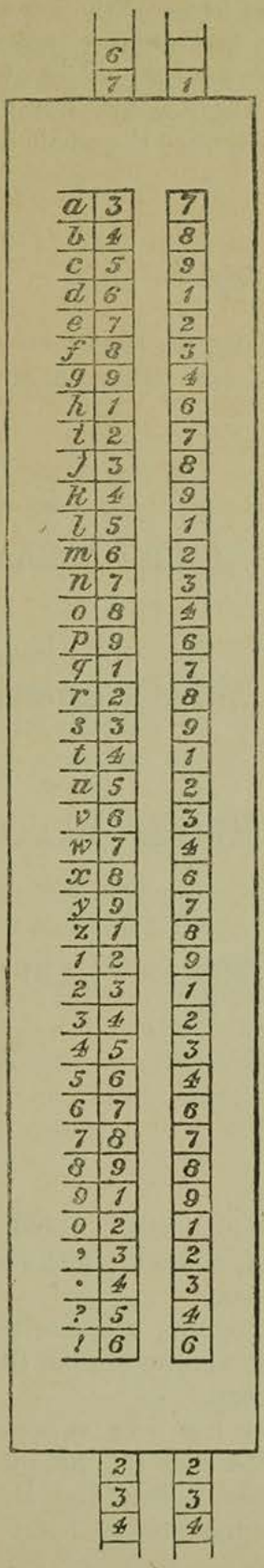
Double Slide Figure Cipher or Code.

The principle of this cipher is similar to that of the Sliding Alphabet cipher (*see* page 32). In this case, however, the apparatus consists of a fixed alphabet (with figures, &c., added, if required) and two slides. On one of the latter the figures 1 to 9 are repeated as often as necessary, and on the other the same figures omitting the 5. In order to use this cipher each correspondent must be in possession of the diagram below, but as no effort of memory is required it can be reconstructed without difficulty, if lost or mislaid.

A keyword must be agreed upon between the correspondents, say the word "gold." Then a number consisting of two figures is chosen by the sender, *e.g.*, 94. This is written at the beginning of the cryptogram in order to inform the recipient how to set the slides to commence deciphering. In order to encipher the message the slides are arranged so that the first letter of the keyword "g" and the figures 9 and 4 are opposite one another, and in this position the equivalent numbers for each letter of the text are obtained. When the sender considers a change advisable he introduces one of the change numbers, followed by the new number. He then sets the slides so that the new figures are opposite to the second letter of the keyword. This process is repeated until the message is completed.

If the message "Blow up bridge" were to be sent with the keyword "gold," and if the first number 94 were changed to 26 at the beginning of the last word of the text, the cryptogram would be :—

94485184745296402679595892361 3



Numbers used to indicate the introduction of new key number.

Dummy numbers. There being no 5 in the right hand slide, these numbers can easily be recognized

The recipient, in order to read the cryptogram, divides the figures into pairs and strikes out any dummies. He then sets the slides to the first key number and the first letter of the keyword, and reads off the letters of the text until the first number indicating a change of key number is reached. He then sets the slides afresh, using the second letter of the keyword and the new key number next in the cryptogram, and continues the process until the whole text is obtained.

Bacon's Cipher.

In this cipher, designed by Lord Bacon, the letters of the alphabet are represented by permutations of two letters, A and B, in groups of five, as shown below :—

a.	b.	c.	d.	e.	f.
AAAAA	AAAAB	AAABA	AAABB	AABAA	AABAB
g.	h.	i.	k.	l.	m.
AABBA	AABBB	ABAAA	ABAAB	ABABA	ABABB
n.	o.	p.	q.	r.	s.
ABBAA	ABBAB	ABBBA	ABBBB	BAAAA	BAAAB
t.	u.	v.	w.	x.	y.
BAABA	BAABB	BABAA	BABAB	BABBA	BABBB

z.

BBABB.

According to this cipher the word " halt " would be represented by AABBBAAAAAABABABAABA, a result which shows the system to be unsuitable for military purposes.

In order to decipher the cryptogram, the receiver divides it, if necessary, into groups of 5 letters, and ascertains from the key the letter which corresponds to each group.

A method by which this cipher has been varied is to use other letters of the alphabet instead of A and B ; for instance, A might sometimes be represented by other vowels and B by consonants. Thus the word " halt " might be represented by :—

EARTHAEIOUEDUCAKEATS.

The Vowel Cipher.

For this cipher a diagram must be prepared as below. The vowels are arranged along two adjoining sides, and the letters of the alphabet are inscribed in the diagram, a conventional alphabet being formed by means of a keyword (*see* page 19) :—

*	A	E	I	O	U
U	*o*	*h*	*e*	*r*	*l*
O	*f*	*a*	*u*	*y*	*g*
I	*q*	*k*	*x*	*b*	*t*
E	*c*	*z*	*n*	*w*	*m*
A	*s*	*v*	*d*	*i*	*p*

In this cipher each letter of the text is represented by the two vowels which stand respectively in the same column and the same line, *e.g.*, b is represented by IO, a by OE, t by IU, &c., and the message " Send up tents " would be enciphered thus :—

AEUIEIAIOIAUIUUIEIIUAE.

To decipher the crytogram, the receiver divides the letters into pairs, and by means of his key table finds the letters corresponding to each pair. It is hardly necessary to point out that this cipher is quite unsuited to military purposes.

A variation of the above system is known as the " Shield of Polybius." In this case the vowels are represented by figures, and each letter of the text is represented in a precisely similar manner by two figures instead of two vowels.

Napoleon's Cipher or "Tableau de Porta."

This system is merely a variation of the Sliding Alphabet cipher, and has no advantage over the forms of this cipher already described. It is, however, of military interest, for it was used by Napoleon during the operations in the Peninsula, and is consequently known by his name, though it was employed practically in this form by an Italian doctor, named Porta, in the 16th century.

In order to use the cipher the following table is constructed. The letters of the alphabet are written out in pairs of lines each of 12 letters and repeated 12 times, the order of the letters in the second line being altered in each alphabet. Two key alphabets are then written out vertically as shown in the table :—

Key Alphabet No. 1.													Key Alphabet No. 2.
a	A	B	C	D	E	F	G	H	I	K	L	M	z
b	N	O	P	Q	R	S	T	U	V	X	Y	Z	y
c	A	B	C	D	E	F	G	H	I	K	L	M	x
d	O	P	Q	R	S	T	U	V	X	Y	Z	N	v
e	A	B	C	D	E	F	G	H	I	K	L	M	u
f	P	Q	R	S	T	U	V	X	Y	Z	N	O	t
g	A	B	C	D	E	F	G	H	I	K	L	M	s
h	Q	R	S	T	U	V	X	Y	Z	N	O	P	r
i	A	B	C	D	E	F	G	H	I	K	L	M	q
k	R	S	T	U	V	X	Y	Z	N	O	P	Q	p
l	A	B	C	D	E	F	G	H	I	K	L	M	o
m	S	T	U	V	X	Y	Z	N	O	P	Q	R	n
n	A	B	C	D	E	F	G	H	I	K	L	M	m
o	T	U	V	X	Y	Z	N	O	P	Q	R	S	l
p	A	B	C	D	E	F	G	H	I	K	L	M	k
q	U	V	X	Y	Z	N	O	P	Q	R	S	T	i
r	A	B	C	D	E	F	G	H	I	K	L	M	h
s	V	X	Y	Z	N	O	P	Q	R	S	T	U	g
t	A	B	C	D	E	F	G	H	I	K	L	M	f
u	X	Y	Z	N	O	P	Q	R	S	T	U	V	e
v	A	B	C	D	E	F	G	H	I	K	L	M	d
x	Y	Z	N	O	P	Q	R	S	T	U	V	X	c
y	A	B	C	D	E	F	G	H	I	K	L	M	b
z	Z	N	O	P	Q	R	S	T	U	V	X	Y	a

* This table is constructed for the French language. For enciphering messages in English, a complete alphabet of 26 letters would generally be used.

In order to encipher a message by this system, a keyword is first chosen and is written letter for letter under the message, being repeated as often as necessary. The letter of the keyword which stands below any letter of the text indicates which alphabet is to be used.

Supposing the words " Bridge blown up " are to be enciphered with the keyword " Practice," key alphabet No. 1 being used, the message is enciphered thus :—

Text ..	B	R	I	D	G	E	B	L	O	W	N	U	P
Key letters	p	r	a	c	t	i	c	e	p	r	a	c	t
Cipher	V	I	V	R	Q	V	P	N	G	A	A	G	F

The method of enciphering is as follows :—The first letter of the text " B " has the key letter " p " below it, so alphabet " p " (or " p q," for it will be noted that each alphabet is indicated by a pair of letters) is to be used.

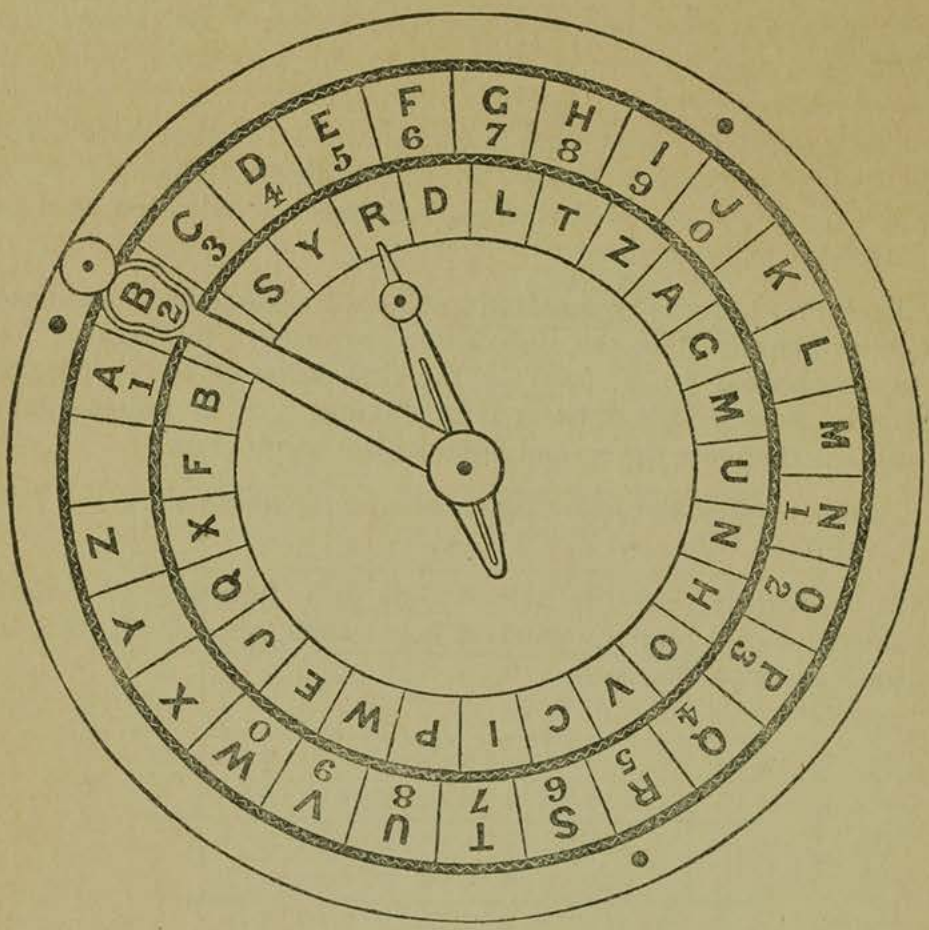
Each text letter is represented in cipher by the letter immediately above or beneath it in the alphabet to be used. In alphabet " p," B is represented by V, so V is the first letter of the cryptogram. Similarly the second text letter R in alphabet " r " is represented by I, and I is therefore the second letter of the cryptogram.

In this manner the following cryptogram is obtained :—V I V R Q V P N G A A G F.

It is evident that the above table only furnishes 12 different alphabets, as the various pairs of key letters, ab, cd, ef, &c., only indicate one alphabet each.

Wheatstone's Cryptograph.

This instrument, designed by the late Sir Charles Wheatstone, is above 4 inches in diameter, and consists of a dial with two hands, as shown here.



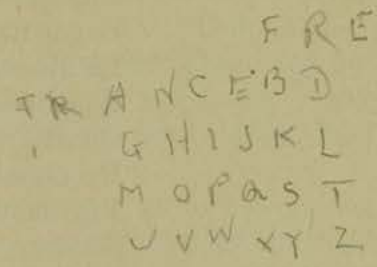
In the outer alphabet the letters are in their natural order, with a blank space between the A and the Z, but on the inner circle the letters are arranged in an arbitrary order. The inner alphabet is inscribed on a circle of card, which can be detached from the instrument and replaced by another circle and alphabet when required. Th s arbitrary alphabet can be formed in several ways, with or without the use of a keyword. The inner circle of card bearing the arbitrary alphabet is always set so that the first letter of this alphabet stands immed ately below the blank space in the outer alphabet. As there is no blank in the inner circ e, it has one space less than the outer circle, and by a simple mechanical contrivance each complete revolution of the long hand causes the short hand to point to one place in advance. Thus, when the long hand points to B and the short to R if the long hand is moved round so that it again points to B, the short hand will point to D.

To use the instrument, the sender, having set the long hand to the blank space and brought the short hand directly under it,* moves the long hand forward so that it points to the first letter of the text on the outer circle, and writes down as the cipher letter the letter on the inner circle to which the short hand is directed. The long hand is then moved forward to the next letter of the text, and the next cipher letter is obtained; at the end of each word a dummy letter is introduced, this being the letter to which the short hand points when the long hand is moved opposite the blank space.

The receiver, after setting both hands to the blank space, moves the long hand round till the short hand points to the first letter of the cryptogram. The long hand then indicates the corresponding letter of the text, and the other letters are obtained in a similar manner.

Marmont's Figure Code.

This code has special military interest, for the original fell into the hands of an English Staff Officer in the Peninsula. It was found among the papers of the late Sir George Scovell, by whose relatives it was kindly lent to the War Office.



*The short hand is free to move independently of the long one, though the motion of the latter affects the former.

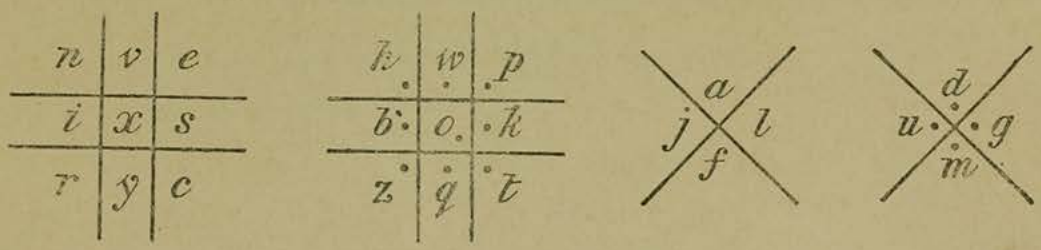
a	2, 3, 10, 29.
b	38, 56.
c	6, 39.
d	40, 57.
e	8, 14, 27, 37, 41.
f	42, 58.
g	32, 43.
h	26, 44.
i, j	4, 16, 22, 35.
k	45.
l	17, 33, 46.
m	24, 47.
n	5, 11, 19.
o	18, 23, 34.
p	13, 25.
q	48, 59.
r	7, 15, 21, 36.
s	9, 12, 28, 31.
t	20, 50, 60.
u	51, 61, 62.
v, w	1, 52.
x	53.
y	54.
z	55.
&	63.

Alcantara	91
Avila	85
Agueda	100
Alagon	98
Arrondissement	105
Artillerie	121
Badajoz	90
Bataillon	117
Brigade	115
Cinquième	81
Ciudad Rodrigo	92
Col de Banos	95
Col de Miravete	94
Cavalerie	119
Commandant	112
Convoi-s	109
Chevaux	123
Deuxième	78
Droit-e	83
Division-s	114
Estramadure	102
Ennemi-s	128
Evacuation	106
Gauche	84
Guadiana	97
Garnison	129
Général	113
Génie..	122
Guerillas	130
Hommes	132
Infanterie	120
Lugar nuevo	93
La Manche	103
Quatrième	80
Quartier G^{al}.	111
Reconnaissance	126
Régiment	116
Sixième	82
Salamanque	96
Subsistance-s	107
Talavera	87
Tolède	88
Truxillo	89
Tage	101
Tietar	99
Troupes	118
Troisième	79
Un point	30
Un point & virgule ..	49

For the purpose of economising time when deciphering, a corresponding table with the figures in numerical order and their equivalents written opposite them was made out.

The Masonic Cipher.

In order to use this the following diagrams must be in possession of both correspondents :—



The letters are then represented as follows :—*n* by ⌋, *x* by ⊏, *k* by ⊑, *q* ⊓, *a* by ∨, &c. The word "cipher" would thus appear as ⌜ ⌋ ⊑ ⌋ ⌊ ⌝.

The above diagrams admit of many variations ; they can be filled in by the aid of any conventional alphabet.

The disadvantage of this cipher is that the cryptogram shows unmistakably the system employed.

Schotti's Dot Cipher.

For this cipher the correspondents must each have a key alphabet the letters of which are arbitrarily numbered,* thus :—

a	b	c	d	e	f	g	h	i	j	k	l
21	9	16	5	25	10	20	1	15	12	26	2
m	n	o	p	q	r	s	t	u	v	w	x
24	11	19	7	23	3	18	14	22	8	4	17
					y	z					
					13	6					

Then, if the message to be sent were "send reinforcements," a dot would be put under the 18th letter of the newspaper or book (as the first letter of the text is represented by 18), the next dot under the 25th from the letter previously marked (as e, the next letter, is represented by 25,) the next under the 11th after that, and so on.

When a book or newspaper expected to contain a cryptogram of this form arrives, the receiver counts the number of letters from the beginning to the first dot, and then the number to each succeeding dot. The number thus obtained, when referred to the key alphabet, give the letters of the text. Sometimes the dots are written in sympathetic ink, in which case the receiver must first treat the book or paper so as to make the dots visible.

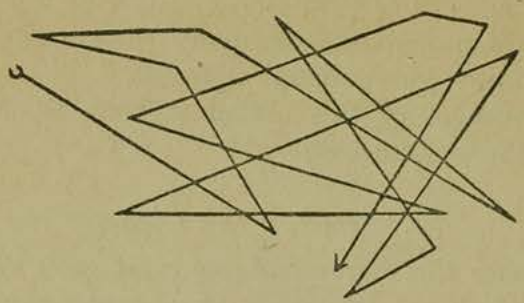
The Line Cipher.

In order to use this cipher each correspondent has an arbitrary alphabet written either on squared paper as shown below, or inscribed in some other figure. The sender lays a piece of tracing paper over

* A conventional alphabet could of course be formed by the aid of a key-word, and the letters then numbered consecutively from 1 to 26, thus doing away with the necessity of the correspondent keeping a key alphabet.

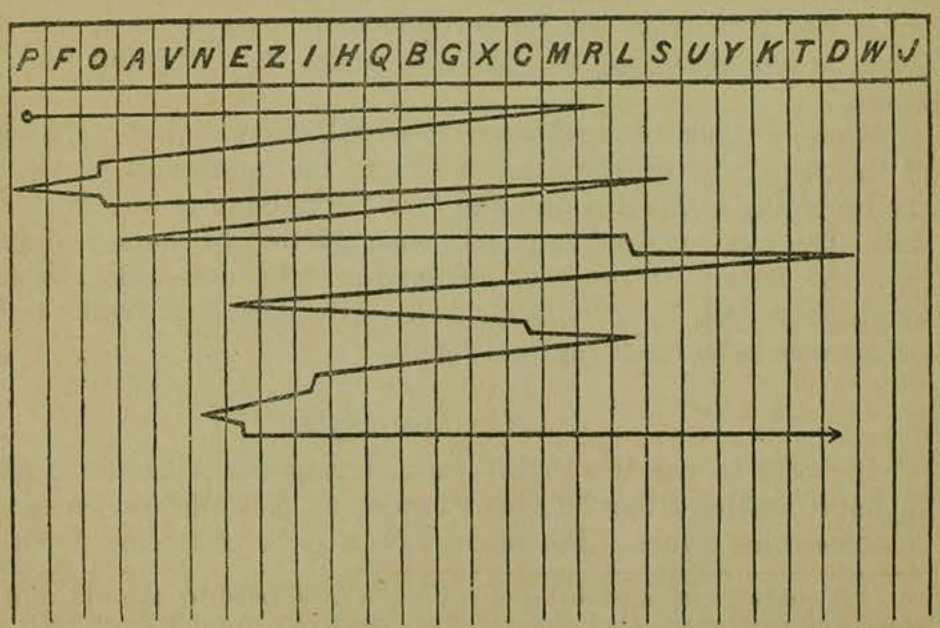
his key alphabet and connects the letters in succession by straight lines. The pattern thus formed constitutes the cryptogram. For instance, the message "Proposal declined," if enciphered with the following key alphabet, would have the form given below :—

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



The receiver, having made a tracing of the cryptogram on transparent paper, lays it over his key alphabet and reads off the message.

For a long message sent on this system very large squares would be necessary in order to avoid confusion, and, consequently, it is more convenient to arrange the letters of the alphabet at the top of 26 vertical columns and form the pattern regularly downwards, marking by a sharp bend in the line each letter which cannot be indicated by an angle. With this arrangement the pattern would be as follows for the message given above :—



INDEX.