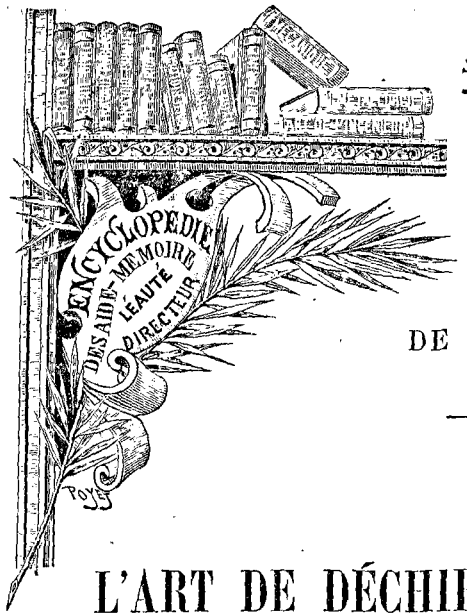


Section de l'Ingénieur

DE VIARIS

L'ART DE DÉCHIFFRER

LES DÉPÊCHES SECRÈTES

GAUTHIER-VILLARS ET FILS

G. MASSON

ENCYCLOPÉDIE SCIENTIFIQUE DES AIDE-MÉMOIRE

COLLABORATEURS

Section de l'Ingénieur

MM.

Alain-Abadie.
Alheilig.
Armengaud jeune.
Arnaud.
Bassot (Colonel).
Baume Pluvinel (de la).
Bérard (A.).
Bergeron (J.).
Berthelot.
Bertin.
Billy (Ed. de).
Bloch (Fr.).
Blondel.
Boire (Em.).
Boucheron (H.).
Candlot.
Caspari.
Charpy (G.).
Clugnet.
Croneau.
Damour.
Defforges (Comm^{t}).
Delafond.
Dudebout.
Duquesnay.
Durin.
Dwelshauvers-Dery.
Etard.
Fabre (C.).
Fourment.
Fribourg (Comm^{t}).
Frouin.
Garnier.
Gassaud.

MM.

Gautier (Armand).
Gautier (Henri).
Godard.
Gouilly.
Grouvelle (Jules).
Guenez.
Guillaume (Ch.-Ed.).
Guye (Ph.-A.).
Guyou (Comm^{t}).
Hatt.
Hérisson.
Hospitalier (E.).
Hubert (H.).
Hutin.
Jacométy.
Jean (Ferdinand).
Labouret (de).
Launay (de).
Laurent (H.).
Lavergne (Gérard).
Léauté (H.).
Le Chatelier (H.).
Lecomte.
Leloutre.
Lenicque.
Le Verrier
Lindet (L.).
Lippmann (G.).
Lumière (A. et L.).
Madamet (A.).
Magnier de la Source.
Margerie.
Matignon.
Meyer (Ernest).

MM.

Michel-Lévy.
Minel (Pol).
Minet (Ad.).
Moëssard (Comm^{t}).
Moissan.
Monnier.
Moreau (Aug.).
Naudin (Laurent).
Ouvrard.
Perrin.
Perrotin.
Picou (R.-V.).
Poulet (J.).
Prudhomme.
Rateau.
Resal (J.).
Ricaud.
Rocques-Desvallées.
Rouché.
Sarrau.
Sauvage.
Schlœsing fils (Th.).
Schützenberger.
Seyrig (T.).
Sinigaglia.
Sorel.
Trillat.
Urbain.
Vermand.
Viaris (de).
Wallon.
Widmann.
Witz (Aimé).

ENCYCLOPÉDIE SCIENTIFIQUE

DES

AIDE-MÉMOIRE

PUBLIÉE

SOUS LA DIRECTION DE M. LÉAUTÉ, MEMBRE DE L'INSTITUT

DE VIARIS — L'Art de chiffrer et déchiffrer les dépêches. 1

Ce volume est une publication de l'Encyclopédie scientifique des Aide-Mémoire ; F. Lafargue, ancien élève de l'École Polytechnique, Secrétaire général, 46, rue Jouffroy (boulevard Malesherbes), Paris.

N° 38 A.

ENCYCLOPÉDIE SCIENTIFIQUE DES AIDE-MÉMOIRE

PUBLIÉE SOUS LA DIRECTION

DE M. LÉAUTÉ, MEMBRE DE L'INSTITUT.

L'ART

DE

CHIFFRER ET DÉCHIFFRER

LES DÉPÊCHES SECRÈTES

PAR

LE MARQUIS DE VIARIS

Ancien élève de l'École Polytechnique
Ancien officier de Marine

PARIS

GAUTHIER-VILLARS ET FILS,
IMPRIMEURS-ÉDITEURS
Quai des Grands-Augustins, 55

G. MASSON, ÉDITEUR,
LIBRAIRE DE L'ACADÉMIE DE MÉDECINE
Boulevard Saint-Germain, 120

PREMIÈRE PARTIE

—

NOTIONS PRÉLIMINAIRES

—

CHAPITRE PREMIER

—

GÉNÉRALITÉS

1. Usage des dépêches chiffrées. — Les correspondances secrètes, c'est-à-dire ne présentant aucun sens apparent et destinées à être comprises, au moyen de conventions antérieures, par les seuls initiés, étaient autrefois l'apanage presque exclusif de la diplomatie. Aujourd'hui leur usage est général. Non seulement la diplomatie, mais l'armée, le commerce, la presse en font un usage quotidien, et comme la très

grande partie de ces correspondances sont transmises par le télégraphe, nous les appellerons indistinctement : *dépêches chiffrées*, qu'elles soient composées de groupes de chiffres, de groupes de lettres ou d'un assemblage de mots en apparence incohérents.

2. Eléments constitutifs de la langue. — Pour chiffrer une dépêche, c'est-à-dire pour rendre incompréhensible chacune des phrases qui la composent, il faut modifier les éléments constitutifs de cette phrase. Une phrase est constituée par des mots se suivant dans un ordre donné, nécessaire au sens de la phrase :

Pierre a tué Paul *Paul a tué Pierre*

sont deux phrases composées des mêmes mots et leur signification diffère absolument. Les mots eux-mêmes se composent de lettres assemblées dans un certain ordre : *crâne, écran, rançe, nacre, ancre, Nérac*, sont six mots différents composés des mêmes lettres.

3. Trois familles de méthodes. — Pour constituer une phrase, les lettres et les mots ont donc deux valeurs, valeur absolue et valeur relative ou de position. Pour chiffrer une phrase,

on aura donc à modifier un ou plusieurs de ses éléments, c'est-à-dire :

1° la valeur absolue des lettres,
ou : 2° leur valeur relative,
ou bien : 3° la valeur absolue des mots,
ou encore : 4° leur valeur relative.

Ecartons tout d'abord cette dernière hypothèse, car brouiller simplement les mots d'une phrase ne présenterait aucune sécurité. Restent trois catégories que nous étudierons successivement.

Nous désignerons sous le nom de méthodes à *alphabets* les méthodes de chiffrement où l'on modifie la valeur absolue des lettres ; par méthodes à *anagramme*, celles où on modifie leur valeur relative. Enfin pour remplacer les mots par d'autres mots ou des groupes de chiffres ou de lettres, il a fallu établir par convention préliminaire des tableaux, répertoires ou dictionnaires. Nous donnerons, à ces méthodes, le nom de méthodes à *répertoire*.

4. Ordre des études. — Ces dernières sont usitées surtout par les négociants, les journaux et la diplomatie. Elles sont en effet d'un usage plus rapide que toutes les autres méthodes et ont le grand avantage de permettre la réalisation d'économies très notables dans la transmission

des télégrammes. Toutefois comme elles sont moins intéressantes et variées au point de vue théorique, nous ne nous occuperons d'elles qu'en dernier lieu. Avant même d'étudier les autres, il convient de savoir :

1° De quelle nature sont habituellement les conventions permettant aux correspondants de traduire leurs dépêches ;

2° A quelles conditions générales doit satisfaire une méthode de cryptographie usitée dans un service régulier pour donner aux correspondants la sécurité dont ils ont besoin au point de vue du secret des dépêches.

CHAPITRE II

DES CLEFS

5. Mots de convention. — La convention à établir entre correspondants doit être aussi simple que possible et facile à retenir de mémoire.Ce sera donc en général un mot, c'est le *mot clef.*

6. Clefs numériques ou littérales. — Mais ce mot unique peut, suivant les besoins des procédés auxquels on aura recours, être trop long, ou au contraire trop court, nous devons donc montrer comment d'un mot clef convenu, on peut déduire une *clef* d'une certaine longueur. clef numérique ou littérale.

Admettons que le mot clef soit RÉPUBLIQUE et que nous ayons justement besoin d'une clef numérique de *dix*. La méthode à suivre est de numéroter les lettres du mot suivant leur valeur relative dans l'alphabet ordinaire. Ainsi dans RÉPUBLIQUE on mettra le chiffre 1 au-dessous du B, le chiffre 2 au-dessous du premier E et le chiffre 3 au-dessous du second E, le 4 sous l'I, etc., en sorte que ces chiffres se présenteront ainsi :

R	É	P	U	B	L	I	Q	U	E
8	2	6	9	1	5	4	7	10	3

et la clef numérique de dix sera :

8.2.6.9.1.5.4.7.10.3.

Une clef numérique plus courte que le mot clef s'obtiendra en n'écrivant que les lettres nécessaires pour obtenir le nombre voulu :

Clef de sept :

R	É	P	U	B	L	I
6	2	5	7	1	4	3

6.2.5.7.1.4.3.

Au contraire, une clef plus longue se fera en

répétant le mot clef autant de fois qu'il sera nécessaire.

Clef de quinze :

R É P U B L I Q U E R É P U B
11 3 8 13 1 7 6 10 14 4 12 5 9 15 2

11.3.8.13.1.7.6.10.14.4.12.5.9.15.2.

Ce procédé est très élastique et peut servir dans la plupart des cas.

7. Clef de 25 lettres. — Dans quelques systèmes on a besoin d'une clef numérique ou littérale de 25. Ce nombre étant celui des lettres de l'alphabet, voici un procédé qui met cette coïncidence à profit. Écrivez les lettres du mot clef en supprimant les répétitions qui peuvent s'y trouver et au-dessous de chacune d'elles, écrivez les lettres de l'alphabet non encore employées, dans leur ordre naturel, puis relevez de haut en bas chaque colonne verticale :

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

La clef littérale de 25 est :

RAMZE CNPDO UFSBG TLHVI JXQKY

Comme les précédentes, on transformera cette clef littérale en clef numérique en attribuant à chaque lettre la valeur absolue de son rang dans l'alphabet normal.

Clef numérique de 25 :

18.1.13.25.5.3.14.16.4.15.21.6.19.2.7.20.12.8.
22.9.10.23.17.11.24.

8. Inconvénients et variantes. — Ce procédé, une fois bien compris, est très simple, mais il peut avoir des inconvénients pour certaines méthodes. Il m'est arrivé de déchiffrer des dépêches où l'on avait employé ce système de clef, en cherchant les places que pouvaient occuper les lettres A, B ou Z, places qui sont presque toujours les mêmes. Ainsi si A ou B ne font pas partie du mot *clef*, l'une d'elles se trouve forcément la deuxième lettre de la clef. Si l'on a déterminé la place de Z, il y a des chances pour que l'emplacement d'Y et de X soit facilement retrouvé.

Une variante très simple consisterait à écrire de droite à gauche les lignes paires du tableau générateur de la clef, en suivant l'ordre des flèches.

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

La clef littérale devient en ce cas :

RKMEJ NPHOU GSBFT LDVIC XQAYZ

et cette clef ne présente pas les mêmes inconvénients que la précédente au point de vue des emplacements probables de A,B,Z.

Une autre variante peut-être encore plus avantageuse, mais un peu moins simple, est la suivante :

Ecrire le tableau générateur de gauche à droite, comme dans le premier procédé, mais le prolonger sur la droite d'autant de lettres qu'en contient réellement le mot clef. Ainsi avec

RÉPUBLIQUE, dix lettres, on écrirait le tableau générateur ainsi :

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

et on obtient la clef de 25 en supprimant les dix premières lettres qui se trouvent reportées à la fin :

UFSBG TLHVI JXQKY RAMZE CNPDO

9. Clef de longueur indéfinie. — Il y a encore, bien entendu, beaucoup d'autres systèmes de clefs possibles. Deux correspondants peuvent convenir de prendre comme clef indéfinie les mots contenus dans telle page d'un livre désigné. On peut aussi former une clef indéfinie par le procédé suivant : convenir qu'avec le mot clef pris tout seul, et supposé de dix lettres par exemple, on chiffrera les dix premières lettres de la dépêche, puis que ces lettres seront une nouvelle clef pour traduire les dix lettres suivantes et ainsi de suite.

Exemple : dépêche à chiffrer :
Le ministre partira ce soir pour Aix.

R É P U B L I Q U E
L E M I N I S T R E
P A R T I R A C E S
O I R P O U R A I X

Avec le mot clef on chiffrera les dix premières lettres ; avec ces dix lettres, les dix suivantes et enfin avec celles-ci le reste.

Le correspondant déchiffrera la dépêche par tranches successives de dix lettres et n'aura aucune difficulté pour connaître ainsi les clefs successives. Ces derniers procédés ne sont pas jusqu'ici d'un usage courant.

10. Recherche du mot de convention. — Lorsqu'on se trouve en présence d'une dépêche dont on ne connaît pas la clef et qu'on est parvenu à déchiffrer, il résulte en général immédiatement de ce déchiffrement la connaissance de la clef numérique ou littérale, mais il est intéressant de rechercher quel a pu être le mot clef qui a servi à établir la clef elle-même. En général cette recherche ne présente pas de très grandes difficultés, un peu de sagacité est pourtant nécessaire.

Il faut d'abord se rendre compte du système de transformation employé. Si la clef a 25 lettres, les emplacements de X,Y,Z permettent de reconnaître l'emploi de la deuxième méthode et la séparation en tranches convenables fait apparaître le mot clef employé. Pour une clef de moins de 25 lettres, l'emploi de la première méthode est presque certain, et la reconstitution plus difficile si la clef est courte et le mot clef long. Pour exemple de la méthode à suivre prenons un cas simple. On a trouvé la clef numérique suivante :

15.3.11.17.1.9.7.13.18.4.16.5.12.19.2.10.8.14.
20.6.

On voit immédiatement un groupe 1.9.7.13. qui se trouve répété plus loin sous la forme 2.10.8.14. On peut donc affirmer que le mot clef n'a pas suffi pour former cette clef de 20 et qu'il a fallu le répéter en tout ou en partie. La dernière lettre 6 correspond à une lettre antérieure qui ne peut être que 5 ou 4. D'autre part la 1re lettre 15 a dû être répétée avec le n° 16 ou 17, mais 17 se trouvant avant 16, il en ressort que 16 est l'unique répétition de 15 et que par suite le mot clef était terminé

après 4. Donc le mot clef a *dix* lettres et se réduit à :

15.3.11.17.1.9.7.13.18.4.

que pour plus de simplicité on peut écrire :

8.2.6.9.1.5.4.7.10.3.

Est-il probable que ce mot renferme des lettres pareilles ? 3 pourrait être la répétition de 2 ; 6 et 7 pourraient être les mêmes lettres ainsi que 8, 9 et 10. La lettre finale est une des premières de l'alphabet, c'est probablement un E, surtout si l'on suppose 2 et 3 pareilles ; 1 sera donc A,B,C ou D. En écrivant sous chaque chiffre quelques lettres hypothétiques placées dans l'ordre où elles peuvent l'être, en supposant la présence des autres voyelles I,O,U, on arrivera par quelques tâtonnements à trouver le mot clef. C'est d'ailleurs évidemment une question de sagacité.

11. Importance de cette recherche. — Cette recherche a une certaine importance au point de vue du déchiffrement des dépêches ultérieures écrites avec le même mot clef. Aucune, toutefois si le mot clef et sa transformation en

clef restent absolument invariables? Mais il peut en être autrement; tout élément invariable est mauvais en cryptographie. Un officier, cryptographe distingué, m'a soumis à déchiffrer des dépêches. Les clefs de ces dépêches étaient ainsi composées : le mot clef primitif était suivi de la date du jour où la dépêche était écrite; par exemple le mot de convention RÉPUBLIQUE, pour une dépêche écrite le cinq Mars, 5/3, aurait donné comme mot clef :

RÉPUBLIQUE CINQ TROIS

ou encore :

RÉPUBLIQUE DIMANCHE

Il y a là un procédé intéressant pour ajouter un élément variable à un mot de convention invariable par lui-même.

CHAPITRE III

—

DE LA SÉCURITÉ AU POINT DE VUE DU SECRET

12. Dépêche isolée ou service régulier. — Il peut se faire qu'une dépêche isolée, très courte, chiffrée d'une certaine façon, soit indéchiffrable. Il n'en résulte pas que la méthode employée soit bonne, donne la même sécurité pour un service régulier, celui de l'armée, par exemple, où il s'agit de milliers de dépêches écrites avec un même système et peut-être un même mot clef.

Quelles sont donc les conditions que doit remplir une méthode pour être considérée comme

bonne et donnant des dépêches indéchiffrables ?

13. Conventions admises. — La première de toutes est qu'elle n'exige pas le mystère. Il est nécessaire de supposer l'*ennemi*, c'est-à-dire toute personne étrangère pour qui la correspondance doit rester secrète, dans les conditions les plus favorables. Si la méthode exige un tableau d'alphabets, un appareil, il faut que l'ennemi puisse les posséder, il doit pouvoir connaître dans les moindres détails la méthode employée, avoir sous les yeux vingt, cinquante dépêches écrites avec le même mot clef, car dans la pratique toutes ces hypothèses peuvent être des réalités. Au point de vue spécial de l'armée, l'ennemi peut en effet intercepter cinquante dépêches, il peut s'approprier d'une façon ou d'une autre tous les détails de la méthode de chiffrement.

14. Conditions requises. — Le seul élément qui doit rester inconnu, c'est le mot clef assimilable au mot d'ordre. L'ignorance de ce seul mot doit rendre le cryptographe le plus habile impuissant à déchiffrer les nombreuses dépêches qu'il a entre les mains.

15. Desiderata. — Mais il y aurait plus à souhaiter encore. Il faudrait que chaque dépêche présentât par elle-même un certain caractère individuel, en sorte que la possession par l'ennemi d'une dépêche chiffrée et de sa traduction en clair, n'entraînât pas forcément le déchiffrement de toutes les autres dépêches.

Dans les méthodes à répertoires, ce desideratum est partiellement satisfait, sous la réserve que le répertoire ne soit pas un de ceux qu'on trouve dans le commerce et qu'il soit d'ailleurs rigoureusement tenu secret. Dans les méthodes actuellement connues des deux premières catégories, aucune ne remplit cette condition. Pour toutes sans exception, si l'on connaît le mode de chiffrement dans ses détails, la possession simultanée du texte chiffré et de sa traduction en clair donne immédiatement la clef; c'est-à-dire le déchiffrement de toutes les autres dépêches écrites avec la même clef. Il serait très désirable qu'il en fût autrement, mais la chose paraît fort difficile; nous avons cependant signalé, au chapitre précédent, une manière de modifier quotidiennement la clef qui donnerait aux dépêches un caractère journalier, sinon individuel.

Dans les méthodes à anagramme, nous aurons

à expliquer une manière d'opérer qui dépend de la longueur de la dépêche expédiée. Ici le caractère est nettement individuel, malheureusement la méthode visée ne présente en elle-même guère de sécurité.

DEUXIÈME PARTIE

—

MÉTHODES A ALPHABETS

—

CHAPITRE PREMIER

—

GÉNÉRALITÉS

16. Définition. — Les méthodes à alphabets sont celles où une lettre du texte clair est remplacée par une autre lettre, par des chiffres ou par des signes conventionnels quelconques ; dans ce dernier cas, les dépêches chiffrées ne seraient pas transmissibles par télégraphe.

17. Trois catégories. — Il peut se faire que dans le courant d'une dépêche le même signe représente toujours la même lettre, la méthode

employée est alors dite à simple clef ou à alphabet unique. Si, au contraire, l'alphabet conventionnel change à chaque lettre du texte clair, la méthode est à double clef ou à alphabets multiples. J'ai constaté dernièrement dans certaines dépêches l'emploi d'une méthode intermédiaire: le même alphabet servait pour une série de lettres, puis changeait subitement. Dans ces dépêches, on changeait d'alphabet après avoir cryptographié une lettre déterminée A, E ou S et convenue d'avance entre les correspondants. Il est facile d'imaginer des variantes à ce procédé, j'ai moi-même dans un ouvrage précédent (1) proposé deux dispositifs de la clef en regard du texte clair, qui s'appliquent immédiatement à ces changements d'alphabets. L'un des dispositifs est dit : « à arrêts convenus d'avance », la période de changement étant déterminée par la valeur numérique attribuée aux lettres de la clef. Le second dispositif : « à la volonté de l'expéditeur », consiste à introduire dans le texte une lettre convenue, le W, et à changer d'alphabet immédiatement après avoir cryptographié cette lettre.

(1) *Cryptographie*, étude publiée dans le *Génie Civil*, 1888. Brochure, p. 11 et 12.

CHAPITRE II

—

MÉTHODES A ALPHABET UNIQUE

18. Exemple simple. — L'exemple le plus simple que nous puissions indiquer est celui-ci : écrire l'alphabet comme ci-dessous et substituer à la lettre du texte clair, celle qui se trouve immédiatement au-dessus ou au-dessous :

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

Le mot RÉPUBLIQUE serait traduit par IVKFYORJFV.

19. Autre exemple. — Mais pour étudier les défauts de cette méthode, il est nécessaire de

prendre un exemple moins simple. Soit comme dépêche à traduire : *le Général de division réunira les Officiers de son État-Major;* le mot de convention est : RÉPUBLIQUE. Au-dessous de l'alphabet normal, écrivons une des clefs littérales de 25 déjà indiquées (1re partie, Chap. II, § 7).

Alphabet normal :

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

Alphabet conventionnel :

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

La dépêche chiffrée, en cherchant le texte clair dans l'alphabet normal et le texte chiffré dans l'alphabet conventionnel, sera :

FENEBEIIRFZEZDXDVDGBIIEJBDIIRFEVGC

CDMDEIIVZEVGBEIRISROGII

20. Remarques sur la langue Française. — Dans l'alphabet ci-dessus, le hasard fait que l'E clair se chiffre par un E et que par suite la prédominance dans la phrase choisie de la lettre E apparaît plus clairement, mais on sait que cette prédominance est la règle absolument

générale et que dans toute phrase française, sur cinq lettres environ on rencontre un E. Or comme la même lettre du chiffre représente toujours la même lettre du clair, il sera d'une facilité extrême de reconnaître quel est le signe qui représente la lettre E ; après l'E, les lettres les plus fréquentes sont A,S,R,I, etc. (1). En général, si l'on affaire à un cryptogramme supposé écrit en langue française et que l'on y remarque un signe, une lettre dont la fréquence dépasse notablement celle des autres, on peut affirmer que ce cryptogramme est écrit avec un alphabet unique et que le signe le plus fréquent représente la lettre E. Une fois cette lettre connue, les particularités de la langue et la fréquence des autres lettres donnent bien vite des indications suffisantes pour former des lambeaux de mots et déchiffrer toute la dépêche.

21. Remarques sur l'exemple. — Mais avec ces méthodes, la présence réitérée de l'E n'est pas le seul indice précieux pour le déchiffrement. Dans le texte chiffré ci-dessus, on remarque le groupe ZDXDVD. Ce groupe appelle l'attention, et le champ des hypothèses à faire pour sa

(1) Voyez 5e partie, Chap. II, § 73.

traduction est restreint. Si l'on n'a pas encore la certitude de l'E, on pourrait supposer que ce groupe doit se traduire par LE DECE, comme par exemple « le décès » mais si l'on connaît déjà l'E et que l'on sache avoir affaire à une dépêche militaire, le mot vrai « *divisi...on* » sautera infailliblement aux yeux du déchiffreur ignorant de la clef, de celui que nous appelons l'ennemi.

22. Appréciation de la valeur de ces méthodes. — Notre conclusion est que les méthodes à alphabet unique ne présentent aucune sécurité, et plus tard, dans la suite de ces études, nous considérerons comme théoriquement déchiffré tout cryptogramme que nous parviendrons à ramener à un alphabet unique.

CHAPITRE III

—

MÉTHODE MIXTE

23. Définition et exemple. — On change l'alphabet conventionnel après l'avoir employé pendant le chiffrement d'une série de lettres. Pour donner un exemple pratique de cette méthode nous supposerons l'alphabet conventionnel déjà cité :

RAMZECNPDOUFSBGTLHVIJXQKY

écrit sur une bandelette de papier, cette bandelette glissant en regard de l'alphabet normal, répété s'il est nécessaire. Pour le début de la dépêche, la bandelette est placée de telle sorte

que l'R corresponde à l'A de l'alphabet normal ; la convention à établir est celle-ci : chaque fois que l'on aura cryptographié un E du texte clair, on avancera la bandelette d'un cran, c'est-à-dire d'une lettre, ce qui revient à changer l'alphabet conventionnel. Dans le texte chiffré qui suit, les séries de lettres cryptographiées avec le même alphabet se trouvent séparées par une barre verticale :

Texte clair : *l e g e n e r a l d e d i v*
Texte chiffré : F E | C Z | F M | C Q D R A | Y E H

Texte clair : *i s i o n r e u n i r a l e s*
Texte chiffré : E G E U O B R | T D Z S J N Y | S

Texte clair : *o f f i c i e r s d e s o n*
Texte chiffré : D Y Y M X M K | U F X Q U N C

Texte clair : *e t a t m a j o r.*
Texte chiffré : X | U L U Z L R C D.

24. Remarques sur l'exemple.— Ici ce n'est évidemment pas la fréquence des répétitions de l'E qui permettra de déchiffrer la dépêche, mais on peut néanmoins voir que cette méthode a un grand défaut, elle ne dissimule pas du tout la contexture des mots que l'ennemi peut penser à rechercher. Nous signalions tout à l'heure le

mot : *division*, il apparaît encore ici clairement dans les lettres YEIIEGE... ; le mot *officier* est aussi facile à conjecturer dans DYYMXM...

25. Appréciation de la valeur de la méthode et des variantes. — Cette méthode mixte ne présente pas beaucoup plus de sécurité qu'une méthode ordinaire à alphabet unique. Il est évident qu'on pourrait la compliquer un peu : 1°, en choisissant une clef d'un des modèles que j'ai indiqués au Chap. II, § 8 ; 2°, en commençant le chiffrement à une lettre variable de l'alphabet normal ; 3°, en faisant avancer la bandelette d'un nombre de lettres variable, etc., mais les observations précédentes sur la contexture non altérée des mots connus subsistent entières.

26. Observation aux inventeurs. — A ce propos, je signalerai aux inventeurs de procédés cryptographiques un écueil à éviter. Lorsqu'ils ont reconnu que leur procédé primitif ne présentait pas une sécurité suffisante, ils cherchent des modifications à y apporter. Bien souvent ces changements constituent une difficulté nouvelle pour les correspondants. La dépêche est bien plus pénible à chiffrer et à traduire, mais,

au point de vue de l'ennemi, la sécurité n'en est pas augmentée ; en somme l'inventeur doit faire la plus grande attention à ce que les modifications apportées constituent des améliorations réelles et non de simples complications.

CHAPITRE IV

—

ALPHABETS MULTIPLES RÉGULIERS

27. Définition. — Les méthodes à alphabets multiples prêtent à de nombreuses et intéressantes combinaisons. Les alphabets multiples sont réguliers lorsque les lettres des alphabets conventionnels sont placées dans leur ordre normal; lorsqu'il en est autrement, les alphabets multiples sont dits : intervertis, et seront étudiés au chapitre suivant.

28. Leur ancienneté. — Blaise de Vigenère (1586) et le père Kircher (1663) ont indiqué dans leurs ouvrages le principe de ces méthodes, mais la forme la plus connue, celle qu'on ap-

pelle le « chiffre carré » est due à Dlandol (1794).

29. — Tableau carré.

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

CHIFFRE CARRÉ

30. Fonctionnement. — Pour chiffrer une lettre de la dépêche, on écrit le mot clef en le répétant, autant de fois qu'il est nécessaire, en regard du texte clair. Puis, cherchant l'alphabet vertical commençant par la lettre de la dépêche et l'alphabet horizontal commençant par la lettre correspondante de la clef (ou réciproquement, vu la symétrie du tableau), on prend comme chiffre la lettre située à l'intersection des alphabets.

Pour traduire le cryptogramme le correspondant fera l'opération inverse. Il écrira le mot clef en regard du texte chiffré, cherchera l'alphabet horizontal commençant par la lettre clef, le suivra jusqu'à la rencontre de la lettre chiffre et remontera jusqu'à la lettre initiale de l'alphabet vertical ainsi obtenu.

31. Exemple. — Il va de soi que l'on pourrait utiliser ce tableau de beaucoup d'autres manières, mais toutes ces manières peuvent être ramenées à une formule générale.

Soit à chiffrer avec le mot clef : RÉPUBLIQUE la dépêche suivante : *Le général de brigade préviendra les colonels de se tenir prêts à partir.*

Texte clair : *l e g e n e r a l d e b r i g a*
Mot clef : r e p u b l i q u e r e p u b l
Texte chiffré : D I V Z O P A Q G H V F H D H L

Texte clair : *d e p r e v i e n d r a l e s c*
Mot clef : i q u e r e p u b l i q u e r e
Texte chiffré : L U K V V A Y Z O O A Q G I K G

Texte clair : *o l o n e l s d e s e t e n i r*
Mot clef : p u b l i q u e r e p u b l i q
Texte chiffré : E G P Z M C N H V X T O F Z Q I

Texte clair : *p r e t s a p a r t i r.*
Mot clef : u e r e p u b l i q u e.
Texte chiffré : K V V Y I U Q L A K D V.

32. Valeur numérique des lettres. — Si l'on donne à chaque lettre de l'alphabet, comme valeur numérique, le numéro de son rang dans l'alphabet normal, les lettres du

texte clair seront :	12	5	7	5	14	5	18	1	12	etc.
celles de la clef :	18	5	16	21	2	12	9	17	21	//
celles du texte chiffré :	4	9	22	25	15	16	1	17	7	//

33. Formule algébrique. — Désignons par c la lettre du texte clair, par γ celle de la clef et par χ la lettre chiffrée, il est facile de voir que la lettre chiffrée est obtenue par la relation simple $c + \gamma - 1 = \chi$ ou $\chi + 25$. Mais ajouter 25 à la valeur numérique de la lettre, revient à sup-

poser les alphabets prolongés indéfiniment, (ou placés en rond). Remarquons encore que, si au lieu de partir de la lettre A comme unité, nous avions numéroté les lettres par rapport à leurs distances respectives de A compté pour zéro, B aurait pour valeur numérique 1, C vaudrait 2, etc., en sorte que les lettres des textes prendraient toutes des valeurs inférieures d'une unité et deviendraient :

$c = 11$		4	6	4	13	4	17	0	11
$\gamma = 17$		4	15	20	1	11	8	16	20
$\chi = 28$	(3)	8	21	24	14	15	25	(0) 16	31 (6)

et la relation algébrique s'écrit encore plus simplement :

$$\chi = c + \gamma$$

Si l'on veut chercher d'autres manières de se servir du chiffre carré, on les trouvera dans la formule plus générale :

$$\chi = 25 + c + \gamma$$

Pour l'étude complète de cette formule nous prions le lecteur de se reporter à notre ouvrage antérieur déjà cité (1). Nous nous contenterons

(1) *Cryptographie*, p. 13 et suivantes.

de dire qu'on peut encore la généraliser en y introduisant un élément variable λ, tiré du mot clef, et changeant avec chaque dépêche. La formule devient alors :

$$c + \gamma + \chi = \lambda$$

Dans la pratique on peut se convaincre par expérience que l'usage du tableau est pénible et lent, et qu'il y aurait avantage à se servir de la formule algébrique, si l'on avait appris par cœur les valeurs numériques des 25 lettres de l'alphabet.

34. Sécurité. — Quelle est, au point de vue de la sécurité du secret la valeur des méthodes ayant pour base le chiffre carré ? Pendant fort longtemps, elles ont été considérées comme indéchiffrables. Mais depuis quelques années, les études cryptographiques étant en faveur, on a donné des procédés de déchiffrement absolument certains.

35. Méthode de déchiffrement. — Quelle que soit la façon dont on s'est servi du tableau des alphabets, si l'on possède plusieurs dépêches écrites avec la même clef, les premières

lettres de chaque dépêche se trouvent écrites avec le même alphabet, les secondes lettres également et ainsi de suite; les lettres de même rang dans chaque dépêche dépendent du même alphabet conventionnel, et par suite peuvent être considérées dans leur ensemble comme un cryptogramme chiffré avec un alphabet unique c'est-à-dire théoriquement déchiffré.

Cette première remarque était facile à faire, la suivante est beaucoup plus ingénieuse, elle est due à M. Kerckhoffs (1883). Dans une phrase française il y a des séries de lettres (des polygrammes), qui se trouvent fréquemment à côté les unes des autres ; *les*, *ou*, *et*, *ment*, *ront*, en sont des exemples. D'un autre côté le mot clef étant de longueur limitée, les lettres qui le composent se trouvent indéfiniment répétées. Dans la longueur d'une dépêche, il arrivera presque forcément qu'un groupe de lettres du texte clair, deux, trois ou quatre se trouveront plusieurs fois en regard des mêmes lettres de la clef. Dans ce cas elles seront chiffrées avec les mêmes alphabets conventionnels ; il y aura donc dans le texte chiffré des groupes de lettres, bigrammes, trigrammes etc., qui se trouveront répétés et *le nombre de lettres qui séparera ces répétitions sera un multiple du nombre de lettres*

de la clef. Réciproquement, si le déchiffreur aperçoit dans le cryptogramme des groupes de lettres répétés, il pourra supposer s'il s'agit de bigrammes, affirmer s'il trouve des trigrammes que ces groupes proviennent de la rencontre des mêmes lettres du texte clair et des mêmes lettres de la clef.

36. Exemple. — Prenons pour exemple la dépêche chiffrée précédemment :

DIVZO PAQGH VFHDH LLUKV VAYZO OAQGI
KGEGP ZMCNH VXTOF ZQIKV VYIUQ LAKDV

Nous y remarquons le bigramme ZO, 4e et 5e lettres, répété aux 24e et 25e lettres ; le bigramme IIV, 10-11 et 40-41 ; le trigramme AQG, 7-8-9 et 27-28-29 et le trigramme KVV, 19-20-21 et 49-50-51. Le nombre des lettres qui sépare ces répétitions étant 20 ou 30, nous en concluons que leur sous-multiple commun 10 est le nombre des lettres de la clef (ou à la rigueur l'un de ses multiples).

Une fois le nombre de lettres de la clef trouvé, il suffit de séparer le cryptogramme en tranches de la longueur de la clef ; écrivant ces tranches les unes sous les autres, chaque colonne verticale dépend d'un alphabet unique et le problème

'est ramené au précédent. Le cryptogramme s'écrira :

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

Cette dépêche est évidemment trop courte pour qu'on puisse établir des conjectures suffisamment probables sur la composition de chaque colonne verticale, mais deux autres dépêches de même longueur suffiraient certainement.

37. Analyse d'un déchiffrement. — Voici d'ailleurs comment l'on procéderait. Le déchiffreur remarquant quatre V dans la première colonne supposerait que le V peut bien représenter un E du texte clair. Cherchant dans le tableau carré l'alphabet commençant par E, le suivant jusqu'au V et remontant, il conjecturerait que la première lettre de la clef est un R. Avec cette hypothèse la première lettre D correspond à un L, lettre fort probable pour représenter un début de dépêche.

Mais l'R de la clef ne peut être suivi que d'un H ou mieux d'une voyelle, de même l'L du début doit aussi précéder une voyelle; le tableau carré montre immédiatement que la 2e lettre I

ne peut se trouver à l'intersection de colonnes horizontales ou verticales commençant toutes deux par des voyelles que pour A, E, I. Il en résulte trois hypothèses pour la 2e lettre de la clef et trois traductions correspondantes pour les lettres de la 2e colonne verticale.

1re colonne	R	1re lettre de la clef
D		*l*
V		*e*
V		*e*
K		*s*
V		*e*
V		*e*

2e colonne	Trois hypothèses pour la 2e lettre de la clef :		
	A	E	I
I	*i*	*e*	*a*
F	*f*	*b*	*x*
A	*a*	*v*	*r*
G	*g*	*c*	*y*
X	*x*	*s*	*o*
Y	*y*	*t*	*p*

Les traductions possibles des lettres des deux premières colonnes verticales sont donc :

li...	*le...*	*la...*
ef...	*eb...*	*ex...*
ea...	*ev...*	*er...*
sg...	*sc...*	*sy...*
ex...	*es...*	*eo...*
ey...	*et...*	*ep...*

Il faut maintenant choisir entre ces trois hypothèses; à bien examiner, la 2e colonne présente les associations de lettres les plus probables, et nous sommes amené à préférer l'hypothèse de E comme 2e lettre de la clef.

La 3e colonne verticale ne présente aucune indication, mais à la 4e on remarque deux Z, on peut essayer si par hasard le Z ne chiffrerait pas l'E. Dans cette hypothèse la 4e lettre de la clef serait un U, et la clef débuterait par RE.U...

Les lettres de la 4e colonne seraient E, I, E, L, T, A, et nos débuts de traduction se présenteraient ainsi :

le. e...
eb. i...
ev. e...
sc. l...
es. t...
et. a...

On pourrait encore continuer, mais un déchiffreur expérimenté sachant qu'il a affaire à une dépêche militaire pourra parfaitement conjecturer que *b.i* est peut-être le début du mot *brigade*, que *c.l* peut aussi commencer le mot *colonel*. S'il essaye l'une de ces deux suppositions, il sera amené à voir qu'elles peuvent être exactes simultanément et qu'en ce cas la troisième lettre du

mot clef serait P. Dès lors ce mot commençant par RÉPU... et ayant 10 lettres ne peut être que *réputation* ou *république*, le déchiffrement est dès lors complètement résolu.

38. Observations. — Evidemment dans cet exemple, la première colonne verticale a présenté une circonstance exceptionnellement favorable, le V en majorité représentant réellement un E; dans la 10e colonne où le V domine aussi, il ne représente pas un E du texte clair. En général, il faudrait un plus grand nombre de lettres pour agir avec certitude, mais nous pouvons affirmer que toutes les hypothèses que nous avons émises dans cet exemple ne dépassent pas celles que fait couramment un déchiffreur quelque peu expérimenté.

39. Longueur de la clef, clef indéfinie. — La longueur de la clef étant l'élément de déchiffrement, on est amené à penser qu'une clef indéfinie donnerait de la sécurité à la méthode. Un auteur a, dans une brochure parue dernièrement (1), proposé une méthode reposant sur l'emploi des phrases d'un livre comme clef indéfinie.

(1) M. Hermann, auteur et éditeur, à Paris, 1891.

Les lettres de ces phrases sont combinées avec celles du texte clair d'une façon équivalente à l'équation entre c, χ et γ (§ **33**).

40. Difficultés théoriques et pratiques. — Mais cet auteur ne semble pas prévoir le cas de plusieurs dépêches écrites à différents correspondants ; il n'indique pas le moyen d'empêcher que les lettres de même rang de ces dépêches soient écrites avec le même alphabet (§ **35**). Il n'indique pas non plus comment après avoir chiffré une 1re dépêche, on doit chiffrer les suivantes. Continue-t-on à partir de la lettre précise du livre où l'on s'est arrêté dans le chiffrement précédent? Telle est probablement l'intention de l'auteur, mais, alors si une dépêche n'est pas arrivée à destination, comment le correspondant est-il informé du nombre de lettres qu'elle contenait? Si dix correspondants ont reçu chacun une 1re dépêche de longueur différente, il faudra noter soigneusement à quelle lettre du livre on en est resté pour chaque correspondant! Outre qu'il n'est pas prouvé que cette méthode soit indéchiffrable, elle est bien incomplète au point de vue de la pratique journalière.

Nous avons donné une clef indéfinie (1re partie, chap. II, § **9**) où la clef se forme au fur et à

mesure de la dépêche, nous avons même indiqué dans un autre ouvrage un procédé empêchant les lettres de même rang de dépêches de dépendre du même alphabet. Mais malgré ces précautions deux officiers de nos amis ont déchiffré nos dépêches de ce système.

41. Conclusion. — En somme, la parfaite régularité du tableau carré, ou de l'équation équivalente entre c, γ et χ rend bien difficile la recherche d'une méthode indéchiffrable.

CHAPITRE V

—

ALPHABETS MULTIPLES INTERVERTIS

42. Deux principes d'interversion. — On a cherché à éviter cette régularité en substituant dans le tableau des alphabets intervertis aux alphabets normaux. L'interversion peut être régulière ou irrégulière. Elle est régulière lorsque les alphabets dépendent d'une base commune, d'un mot convenu, *cryptogame*, par exemple :

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

TABLEAU D'ALPHABETS INTERVERTIS RÉGULIÈREMENT

L'interversion est irrégulière lorsque chacun des alphabets est indépendant des autres.

43. Interversion régulière. — Le chiffrement et la traduction d'une dépêche se font exactement de la même manière qu'avec le chiffre carré, il faut cependant remarquer que les correspondants ne peuvent se passer du tableau, car le procédé qui consistait à donner des valeurs numériques aux lettres n'est pas applicable ici, au moins d'une façon pratique.

Toutes les méthodes de déchiffrement indiquées pour le tableau carré s'appliquent également au tableau des alphabets intervertis, seulement avec les alphabets normaux, aussitôt qu'on avait l'emplacement de la lettre E dans un alphabet, on connaissait immédiatement tout l'alphabet correspondant; avec les alphabets intervertis régulièrement, il n'en est plus de même; on peut cependant voir dans le tableau ci-dessus que si l'on arrive à placer dans sa case une seule lettre, on peut par symétrie reconstituer tout une diagonale.

44. Interversion irrégulière. — Cette facilité ne se retrouve pas dans les alphabets intervertis irrégulièrement. Ceux-ci paraissent donc avoir de ce chef une supériorité réelle sur

les alphabets normaux puisque l'ennemi sera obligé par tâtonnements de rechercher les lettres une par une au lieu de les trouver par séries. Malheureusement ces alphabets présentent d'autres difficultés dans la pratique usuelle.

45. Difficultés pratiques. — Ou le tableau des alphabets reste écrit en permanence chez les correspondants, on peut supposer alors qu'il arrivera à la connaissance de l'ennemi et le déchiffrement des dépêches sera ramené au cas des alphabets normaux ; ou le tableau doit ne rester écrit qu'au moment précis où l'on s'en sert et il y a là un travail supplémentaire et pénible pour les correspondants. Pour le réaliser il faut que chaque alphabet ait une base qui puisse se graver facilement dans la mémoire. Nous avons eu sous les yeux des alphabets intervertis dont la base était une série de phrases connues telles que : *Allons enfants de la patrie*, *Bienheureux les pauvres d'esprit*, *Cherchez et vous trouverez*, *Dans le royaume des aveugles*, *Esprit saint descendez en nous*, etc., etc. On ne prenait dans chacune de ces phrases que les lettres non répétées bien entendu : ALONSEFTDPRI et l'on complétait l'alphabet par les lettres non encore employées dans leur ordre normal.

Reconstituer les alphabets chaque fois est donc possible, mais nécessite un travail long et pénible. Nous avons dit plus haut que les conserver écrits en permanence permettait à l'ennemi de les connaître et ramenait pour lui le problème du déchiffrement à celui des alphabets normaux ; ceci bien entendu à condition que le chiffreur se serve du tableau interverti comme du tableau carré.

46. Appareil Bazeries. — Mais on peut combiner d'autres méthodes qui utilisent mieux la supériorité réelle des alphabets intervertis. La plus intéressante que nous connaissions a été inventée en 1891 par M. le capitaine Bazeries (1). Elle exige un appareil auquel il a donné le nom de « cryptographe cylindrique ». Cet appareil se compose d'un cylindre sur lequel on enfile un certain nombre de rondelles portant chacune un alphabet conventionnel gravé. Ces rondelles peuvent être maintenues en place au moyen d'une broche et l'appareil est tout à fait analogue aux cadenas à lettres usités anciennement. L'ensemble de ces rondelles représente donc un

(1) Actuellement chef d'Escadron au train des Equipages.

tableau d'alphabets intervertis irrégulièrement. Mais dans l'opinion de l'inventeur, ce tableau peut impunément être connu de l'ennemi, l'appareil peut lui être livré. En effet, cet appareil représente un tableau essentiellement variable ; chaque rondelle porte un numéro d'ordre et le tableau se trouve modifié par l'ordre dans lequel on enfile les rondelles ; chaque alphabet conventionnel peut occuper n'importe quelle place et l'ensemble de ces positions est facilement déterminé par une clef numérique égale au nombre des rondelles.

Le fonctionnement de l'appareil est simple et ingénieux. Une fois les rondelles enfilées dans l'ordre désigné par la clef, on les fait tourner, pour amener devant un zéro gravé sur le cylindre, chacune des premières lettres du texte clair. S'il y a vingt rondelles on compose ainsi vingt lettres de la dépêche suivant une génératrice du cylindre et l'on immobilise les rondelles au moyen de la broche. Chaque rondelle portant gravées les 25 lettres de l'alphabet, le cylindre présente des numéros de 0 à 24 qui correspondent à 25 génératrices. Celle qui est numérotée 0 forme le texte clair, et l'on prend pour texte chiffré la suite des lettres situées sur une quelconque des 24 autres génératrices, c'est-à-dire qu'à un

texte clair correspondront 24 textes chiffrés au choix.

Malgré cette extrême variété de combinaisons, nous sommes parvenu à déchiffrer des dépêches écrites avec cet ingénieux appareil. Ce système étant le plus intéressant qui ait paru depuis quelques années nous reviendrons sur son fonctionnement et la méthode appliquée à son déchiffrement (5e Partie, Chap. v).

TROISIÈME PARTIE

MÉTHODES A ANAGRAMME

CHAPITRE PREMIER

MÉTHODES SANS APPAREILS

47. Préliminaires. — Les chapitres précédents montrent combien il est difficile d'empêcher le déchiffreur ennemi de ramener un cryptogramme à une série de dépêches écrites avec un alphabet unique et la prédominance de la lettre E suffit pour faire considérer comme théoriquement déchiffrée toute dépêche de ce dernier genre. Ces difficultés que l'on rencontre pour cacher *l'identité* des lettres ont amené à conserver cette identité et à rechercher la sécurité dans la dissimulation de leurs valeurs relatives, en intervertissant l'ordre naturel des lettres de la dépêche.

48. Méthode des diviseurs. — Si cette interversion, cet anagramme portait exclusivement sur chaque mot pris individuellement, le déchiffrement ne serait qu'un jeu d'enfants ; il en serait de même si l'anagramme ne portait que sur des groupes d'une dizaine de lettres. Citons comme exemple de ce procédé la méthode appliquée quelquefois et citée partout, des diviseurs avec transposition simple ou double. Supposons une dépêche, réduite à 35 lettres par une orthographe télégraphique : *Impossible exécuter les ordres reçus hier*. Le nombre 35 ayant deux diviseurs 5 et 7, on disposera le texte sur cinq rangées horizontales de sept lettres chacune :

	1	2	3	4	5	6	7
1	*i*	*m*	*p*	*o*	*s*	*s*	*i*
2	*b*	*l*	*e*	*e*	*x*	*e*	*c*
3	*u*	*t*	*e*	*r*	*l*	*e*	*s*
4	*o*	*r*	*d*	*r*	*e*	*s*	*r*
5	*e*	*c*	*u*	*h*	*i*	*e*	*r*

49. Transposition simple ou double. — La dépêche pourrait être transcrite en relevant simplement les colonnes de bas en haut ou de haut en bas. Mais on a trouvé plus prudent de transposer d'abord l'ordre des colonnes verticales,

puis l'ordre des rangées horizontales, ou réciproquement et de ne transcrire la dépêche qu'après ces opérations. Ces transpositions peuvent-elles donner un résultat sérieux ? Analysons ce qui s'y passe et pour cela suivons le sort des lettres d'une colonne et d'une rangée. Toutes les autres lettres seront figurées par des points :

TEXTE CLAIR

	1	2	3	4	5	6	7
1	.	.	.	.	*b*	.	.
2	.	.	.	.	*b*	.	.
3	.	.	.	.	*b*	.	.
4	*a*	*a*	*a*	*a*	*x*	*a*	*a*
5	.	.	.	.	*b*	.	.

TRANSPOSITION SIMPLE

	3	2	1	5	7	6	4
1	.	.	.	*b*	.	.	.
2	.	.	.	*b*	.	.	.
3	.	.	.	*b*	.	.	.
4	*a*	*a*	*a*	*x*	*a*	*a*	*a*
5	.	.	.	*b*	.	.	.

TRANSPOSITION DOUBLE

	3	2	1	5	7	6	4
4	*a*	*a*	*a*	*x*	*a*	*a*	*a*
3	.	.	.	*b*	.	.	.
5	.	.	.	*b*	.	.	.
1	.	.	.	*b*	.	.	.
2	.	.	.	*b*	.	.	.

Quelles que soient les transpositions, l'anagramme ne portera que sur un petit nombre de lettres, qui s'intervertiront entre elles sans

jamais se mélanger avec les autres. Appliquons ces transpositions à la dépêche en question.

TEXTE CLAIR

	1	2	3	4	5	6	7
1	*i*	*m*	*p*	*o*	*s*	*s*	*i*
2	*b*	*l*	*e*	*e*	*x*	*e*	*c*
3	*u*	*t*	*e*	*r*	*l*	*e*	*s*
4	*o*	*r*	*d*	*r*	*e*	*s*	*r*
5	*e*	*c*	*u*	*h*	*i*	*e*	*r*

TRANSPOSITION SIMPLE

	3	2	1	5	7	6	4
1	*p*	*m*	*i*	*s*	*i*	*s*	*o*
2	*e*	*l*	*b*	*x*	*c*	*e*	*e*
3	*e*	*t*	*u*	*l*	*s*	*e*	*r*
4	*d*	*r*	*o*	*e*	*r*	*s*	*r*
5	*u*	*c*	*e*	*i*	*r*	*e*	*h*

TRANSPOSITION DOUBLE

	3	2	1	5	7	6	4
4	*d*	*r*	*o*	*e*	*r*	*s*	*r*
3	*e*	*t*	*u*	*l*	*s*	*e*	*r*
5	*u*	*c*	*e*	*i*	*r*	*e*	*h*
1	*p*	*m*	*i*	*s*	*i*	*s*	*o*
2	*e*	*l*	*b*	*x*	*c*	*e*	*e*

Supposons le relevé fait par colonnes et de bas en haut, les trois textes chiffrés sont :

1° EOUBI CRTLM UDEEP HRREO IELXS ESEES RRSCI

2° UDEEP CRTLM EOUBI IELXS RRSCI ESEES HRREO

3° EPUED LMCTR BIEUO XSILE CIRSR ESEES EOHRR

et ces trois textes chiffrés présentent à peu près les mêmes difficultés (ou facilités) de déchiffrement pour l'ennemi, ignorant s'il y a eu ou non transposition. Tous les groupes se retrouvent sans mélange intime.

50. Relevé par colonnes paires ou impaires. — Il est facile de voir par l'examen des trois textes que le relevé de bas en haut crée plus de difficultés à l'ennemi que le relevé par rangées horizontales, on pourrait d'ailleurs également convenir que le relevé se fera de bas en haut pour certaines colonnes, les impaires par exemple et de haut en bas pour les colonnes paires. Dans ce cas, le texte n° 3 deviendrait :

3 bis EPUED RTCML BIEUO XSILE CIRSR SEESE RRHOE

51. Choix des diviseurs. — Il arrivera le plus souvent que le nombre des lettres de la dépêche ne se divisera pas en deux diviseurs nombres premiers comme 5 et 7. Il faudra donc établir des conventions supplémentaires pour permettre au correspondant de savoir tout de suite quels sont les diviseurs choisis : si par exemple la dépêche avait 70 lettres, on aurait le choix entre 7×10 ou 5×14. Si l'on étudie la façon dont se fait l'anagramme des lettres, on voit que

plus les groupes seront nombreux, plus intime sera le mélange. Il y a donc avantage à prendre le plus grand diviseur pour les rangées et le plus petit pour les colonnes, en admettant que le relevé se fasse par colonnes comme plus haut. Mais si le nombre des lettres au lieu d'être 70 était 71 ou 73 on ajouterait à la fin de la dépêche un certain nombre de lettres nulles de façon à trouver des diviseurs commodes. A 71 une lettre ajoutée donnerait 3 rangées de 24 lettres, à 73 une lettre de plus fournirait 2 rangées de 37 lettres, mais il serait plus commode d'ajouter deux lettres nulles et de chiffrer 75 se décomposant en 3 fois 25.

52. Les transpositions sont données par un mot clef. — Notons en passant que les différents ordres de transposition sont donnés par un mot de convention transformé en clefs numériques de longueurs nécessaires suivant le mode d'opérer indiqué précédemment.

53. Diviseur constant avec reste variable. — Nous venons de citer deux dépêches de longueur moyenne 72, 75 lettres où l'on est amené à partager la dépêche en rangées de 24 ou 25 lettres. Le chiffreur a eu la préoccupation de choisir ses diviseurs, de rajouter des lettres nulles

en quantité convenable. Son correspondant aura eu des préoccupations analogues. Aussi est-on amené à prendre un nombre fixe convenu d'avance pour le nombre de lettres de chaque rangée, 20 ou 25, et à écrire la dépêche sans se préoccuper autrement de savoir si le nombre des lettres est un multiple ou non du nombre choisi. La façon de former une clef numérique ou littérale de 25 étant souvent adoptée amènera à choisir 25 comme diviseur constant à reste variable, mais l'exemple que nous allons donner aura comme base le diviseur 20.

1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 17 18 19 20
i m p o s s i b l e d e x e c u t e r l
e s o r d r e s r e c u s h i e r

Le mot clef RÉPUBLIQUE comme clef numérique de 20 donne :

15.3.11.17.1.9.7.13.18.4.16.5.12.19.2.10.8.14.20.6.

Convenons de relever les colonnes paires de haut en bas et les impaires de bas en haut, le texte chiffré sera :

I C O P C D R T E I R L E I S X E O R
U E D S E U R M S E E B S E H L S R

54. Variantes. — Il est évident que l'on peut

compliquer cette méthode de bien des manières, ainsi la dépêche au lieu d'être écrite comme plus haut, pourrait l'être de cette façon :

1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20
i	*m*	*p*	*o*	*s*	*s*	*i*	*b*	*l*	*e*	*d*	*e*	*x*	*e*	*c*	*u*	*t*	*e*	*r*	*l*
.	.	.	*r*	*e*	*i*	*h*	*s*	*u*	*c*	*e*	*r*	*s*	*è*	*r*	*d*	*r*	*o*	*s*	*e*

La 1re rangée est écrite de gauche à droite comme d'habitude, mais la 2e rangée l'est en sens inverse, de droite à gauche ; puis si la dépêche est plus longue, la 3e rangée se retrouve dans l'ordre naturel, la 4e à l'envers et ainsi de suite. Mais l'ennemi, supposé au courant du procédé employé pourrait avec le nombre de lettres de la dépêche connaître les cases pleines, il est bon de créer de ce chef une incertitude. Le moyen est simple : au lieu de mettre la première lettre du texte clair dans la case 1, on la mettra dans une case variable, dépendant de la longueur du mot clef, ou de la longueur de la dépêche (*caractère individuel*, voir 1re partie, Chap. III, p. 15). Par exemple le mot clef ayant dix lettres, on commencera la dépêche à la case 11, laissant vides les dix premières :

1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20
										i	*m*	*p*	*o*	*s*	*s*	*i*	*b*	*l*	*e*
e	*r*	*s*	*e*	*r*	*d*	*r*	*o*	*s*	*e*	*l*	*r*	*e*	*t*	*u*	*c*	*e*	*x*	*e*	*d*
c	*u*	*s*	*h*	*i*	*e*	*r*	.	.	.	.	.	.	.	.	.	.	.	.	.

Ou bien la dépêche ayant 35 lettres, c'est-à-dire 7 groupes de 5 lettres, on laissera les sept premières cases vacantes, en commençant à la case 8.

On pourra imaginer bien d'autres conventions analogues, mais en somme toutes donneront des résultats sensiblement équivalents.

CHAPITRE II

—

MÉTHODES AVEC APPAREILS

55. But des appareils. — Dans les méthodes précédentes on a toujours commencé par écrire le texte clair en mettant à côté les unes des autres les lettres dans leur suite naturelle, et cherchant surtout leur mélange dans la façon de relever les groupes. Dans un autre ordre d'idées, on peut chercher une plus grande dispersion des lettres dès le début du travail. Il suffit pour cela de disposer des cases suivant une figure géométrique convenue, carré, rectangle, parallélogramme, etc., de semer les lettres dans ces différentes cases, puis de les relever par rangées ou colonnes après leur avoir fait subir

au besoin des transpositions comme précédemment.

56. Ordre dû au hasard ou au raisonnement. — La convention qui présidera à cette dispersion des lettres dans la figure convenue peut être due au hasard, par exemple les cases recevront des numéros suivant un tirage au sort. On peut aussi se proposer de rechercher si un numérotage rationnel ne donnerait pas un mélange aussi intime.

57. Ordre dû au hasard. — *a*). *Carré de cent cases.* — On a donné à chacune des cases d'un carré de cent, un numéro d'ordre et on écrit chacune des lettres du texte clair à la case qui lui correspond, la 1re lettre à la case numérotée 1, la 2e à la case 2 et ainsi de suite : la case 2 se trouve d'ailleurs loin ou près de la case 1, suivant les hasards du numérotage. Puis on relève les lettres par rangées et leur mélange est très complet.

b). *Nécessité d'une convention supplémentaire.* — Si nous avons en vue un système applicable à un service régulier comme celui de l'armée, nous devons supposer que le carré peut tomber entre les mains de l'ennemi avec son

numérotage, il serait donc nécessaire avant de procéder au relevé des rangées ou colonnes de leur faire subir une transposition simple ou double commandée par une clef quelconque.

c). *Bandelettes ou réglettes.* — Mais ces transpositions deviennent pénibles lorsque le nombre des cases augmente, aussi a-t-on pensé à substituer au carré de cent cases dix bandelettes de papier portant chacune dix numéros et représentant ainsi dix rangées faciles à transposer. Dans la pratique, cent cases sont insuffisantes, le carré devrait en avoir 400, le nombre des bandelettes deviendrait trop grand, on a pensé à leur substituer des réglettes carrées. Dix de ces réglettes portant sur chaque face dix des nombres de 1 à 400 remplacent le carré de 400 cases. Chaque face des réglettes et chaque réglette elle-même est désignée par un numéro d'ordre. On comprend qu'au moyen d'une convention fournie par un mot clef, on puisse placer les réglettes dans un ordre donné et leur faire présenter une face déterminée. Supposons donc les réglettes ainsi rangées et une dépêche de 250 lettres à chiffrer. Sur la 1re réglette, on cherchera s'il y a un nombre inférieur à 250, admettons que 77 s'y trouve. On placera la 1re lettre du texte clair à la 77e case d'un carré de 400 tracé sur du papier

quadrillé. Sur la réglette rangée la 2e se trouvent les nombres 247 et 26, la 2e lettre du texte clair ira à la 247e case et la 3e à le case 26. Lorsqu'on aura fait cette recherche pour les dix réglettes, on les fera toutes tourner d'un quart de tour, de façon à leur faire présenter une face nouvelle et on recommencera les recherches dans le même ordre que précédemment. On arrivera à placer ainsi les 250 lettres du texte clair dans les 250 premières cases du carré figuré. Cet appareil constitue en somme un tableau à numérotage variable. Remarquons que l'on pourrait procéder d'une façon inverse et mettre la 77e lettre du texte clair à la 1re case du carré, la 247e à la 2e case, la 26e à la 3e et ainsi de suite. Nous n'insistons pas ici sur la valeur relative de ces manières de procéder (1), on verra plus loin que cette méthode ne donne pas un secret suffisant pour compenser ses nombreux inconvénients : difficultés dans le maniement régulier de ces réglettes, et fatigue de la recherche des numéros à choisir sur chacune.

58. Transposition raisonnée. — *a*). *Grilles.* — Si l'on présente devant un carré de cent cases

(1) V. *Cryptographie*, p. 27 et 28.

une feuille de carton percée de 25 trous laissant apercevoir 25 des cases, on peut imaginer une disposition de ces 25 trous telle que si l'on présente à nouveau le carton perforé après l'avoir fait tourner d'un quart de tour, 25 nouvelles cases deviennent visibles ; telle enfin que les cent cases aient été successivement visibles dans les quatre positions successives que peut occuper la feuille de carton. Cette feuille de carton ou de métal perforée de trous ainsi disposés s'appelle une *grille* et a été autrefois d'un très grand usage. Nous avons longuement étudié dans un précédent ouvrage (1) les nombreuses dispositions que peuvent présenter les grilles, nous n'y reviendrons pas ici.

b) Autres appareils. — On peut imaginer bien d'autres systèmes que les grilles pour opérer le mélange intime des lettres ; on peut affirmer que tous ceux de ces appareils qui seront dignes d'attention auront à peu près la même valeur théorique. Les différences consisteront surtout dans leur plus ou moins grande facilité d'application pratique. Dans notre ouvrage déjà cité (2) nous décrivons une plaquette d'ivoire

(1) *Cryptographie.* pages 30 à 38.
(2) *Cryptographie,* pages 39 à 42.

portant gravées les lettres de l'alphabet. Cette plaquette permet de se servir du mot de convention directement sans passer par l'intermédiaire d'une clef numérique ou littérale et correspond théoriquement à un rectangle où les lettres seraient disposées par rangées de longueur variable avec transposition double.

CHAPITRE III

DU DÉCHIFFREMENT DE CES MÉTHODES

59. Méthodes à double diviseur. — Ces méthodes ne peuvent pas supporter l'épreuve qu'on doit leur imposer par hypothèse, c'est-à-dire la connaissance par l'ennemi du mode d'opérer. En effet, si nous prenons le texte chiffré n° 3, transposition double, de la dépêche de 35 lettres citée plus haut, l'ennemi saura immédiatement comment partager le texte chiffré en tranches ; en prenant les lettres de même rang dans chaque groupe, il reconstituera une rangée horizontale. Le texte cité est :

EPUED LMCTR BIEUO XSILE CIRSR ESEES EOHRR

Les deuxièmes lettres de chaque groupe sont PMISISO, dans lesquelles tout déchiffreur reconnaîtra le commencement du mot : IMPOSSI(BLE). Le texte 3 bis, présenterait peut-être quelques difficultés de plus, mais en somme il ne saurait résister sérieusement aux recherches.

60. Méthode à réglettes. — Cette méthode, au point de vue des difficultés qu'elle offre au déchiffrement est bien supérieure aux autres, néanmoins comme elles, elle donne trop de prise aux tâtonnements. Les recherches porteront sur le voisinage obligatoire des lettres Q et U, sur la reconstitution d'un mot probable : général, division, régiment, etc. Nous croyons savoir qu'un officier a soumis le système aux épreuves suivantes : on lui a remis deux dépêches de même longueur écrite avec la même clef, puis une dépêche contenant un mot connu, *officier*, par exemple, et enfin une dépêche quelconque. Ce cryptographe expérimenté a pu déchiffrer toutes ces dépêches successivement et par conséquent reconstituer tout le système.

61. Conclusion. — Du moment que cette méthode ne présentait pas une sécurité absolue,

les difficultés de son application pratique étaient telles qu'on a dû l'abandonner, et qu'on semble devoir renoncer également à toutes les méthodes à anagramme.

QUATRIÈME PARTIE

—

MÉTHODES A RÉPERTOIRE

—

CHAPITRE PREMIER

—

DES DIVERS RÉPERTOIRES

62. Préliminaires. — Nous avons jusqu'ici étudié les procédés employés pour dissimuler l'identité des lettres formant les mots d'une dépêche ou leur suite naturelle, nous devons maintenant montrer comment on dissimule les mots eux-mêmes. La langue française comprend de 8000 à 8500 mots usuels, on peut les réunir dans un dictionnaire et représenter chacun

d'eux par des signes convenus. Pour le choix des signes, qui doivent être transmissibles par télégraphe, on consultera les conventions internationales (1). Celles-ci admettent la transmission de groupes de lettres, de groupes de chiffres et de mots dits *de convention*. Ces mots qui doivent avoir une signification individuelle et qui peuvent être pris dans une ou plusieurs langues désignées, sont dits « de convention » lorsque leur suite ne présente aucun sens apparent aux employés du télégraphe. La diplomatie se sert en général des groupes de chiffres, mais les commerçants préoccupés surtout de l'économie pécuniaire, ont recours aux mots de convention.

63. Tableaux chiffrants et déchiffrants. — La diplomatie de presque tous les pays emploie ou a employé des tableaux chiffrants et déchiffrants. Dans un tableau ou répertoire se trouvent rangés, par ordre alphabétique, les mots, noms propres ou locutions au nombre de dix mille (en général) dont on peut avoir besoin. En face de chacun, est placé un numéro d'ordre

(1) 5e partie, chapitre III.

donné par un tirage au sort, c'est le tableau chiffrant. Il a comme corrélatif un second tableau où les nombres se suivent dans leur ordre naturel ayant en face de chacun d'eux la locution correspondante, c'est le tableau déchiffrant. On voit que changer le numérotage de ces tableaux entraîne un travail assez considérable et nous aurons à revenir sur ce fait lorsque nous traiterons de la sécurité due à leur usage.

64. Répertoire Sittler. — Avoir deux tableaux par correspondant et être tenu de les refaire entièrement, lorsque pour un motif quelconque on est obligé de les modifier, a paru aux particuliers une obligation pénible et M. Sittler a inventé un répertoire destiné à obvier à ces deux inconvénients. Le répertoire Sittler se compose de cent pages contenant chacune cent mots ou locutions, soit dix mille en tout. Donc chacune de ces lignes peut être représentée par un groupe de quatre chiffres de 0000 à 9999. A chaque page les lignes sont numérotées d'une façon fixe de 00 à 99. Mais les pages elles-mêmes ne sont pas numérotées. Les correspondants conviennent entre eux de la pagination et de cet élément variable dépend le secret. Remarquons, au point de vue du déchiffrement, que pour éviter au

destinataire, des recherches assez longues, la pagination doit être régulière, c'est-à-dire que la page qui se présente la première peut bien être numérotée 56, mais que la 2e sera, en ce cas, numérotée 57 et ainsi de suite. D'ailleurs rien de plus simple que de changer la pagination au besoin. Les journaux usent beaucoup du répertoire Sittler dans leurs relations avec leurs correspondants à l'étranger.

65. Mots de convention. — Les négociants semblent préférer les répertoires à mots de convention. Le Sittler permettait cependant une économie. Les tarifs télégraphiques comptent comme un mot, un groupe de cinq chiffres. Une locution du Sittler n'en employant que quatre, il en résultait une économie de 20 p. %; par contre le Sittler limite à 10000 le nombre de ses lignes. Un répertoire à mots de convention est en quelque sorte illimité, et on peut y introduire une quantité considérable des phrases dont le négociant peut avoir besoin. Citons l'*ABC télégraphic Cod*, répertoire anglais de 15000 lignes. Ces répertoires conçus exclusivement en vue de l'économie, ne fournissent jusqu'ici aucun élément de secret, car étant vendus dans le commerce, tout le monde peut savoir que tel

mot de convention correspond à telle phrase (1). Il est vrai que chaque négociant peut se faire pour lui-même un code qu'il gardera secret.

---

(1) L'auteur avait annoncé dans son précédent ouvrage : *Cryptographie*, page 60, la préparation d'un répertoire qui devait paraître sous le titre de :

ABC

Répertoire économique

pour la correspondance télégraphique secrète.

Cet ouvrage n'a pas encore paru, l'auteur ayant dû le refondre entièrement à la suite des modifications des règlements internationaux. Tout en étant vendu publiquement, ce répertoire permettra, par un procédé particulier, le secret de la correspondance, un seul exemplaire étant à la fois chiffrant et déchiffrant.

CHAPITRE II

—

DU DÉCHIFFREMENT DES DÉPÊCHES CHIFFRÉES AVEC LES RÉPERTOIRES

66. Evaluation numériqne du secret dans les divers répertoires — Au point de vue du secret, les tableaux chiffrants et déchiffrants tiennent la première place, aucune relation n'existant en effet entre l'ordre alphabétique des locutions et l'ordre numérique. Il en résulte que la connaissance du nombre correspondant à une locution demeure isolée, elle n'entraîne celle d'aucune autre locution. Il n'en est pas de même du répertoire Sittler, tel qu'on l'emploie actuellement, la connaissance du numérotage *d'une seule* locution entraîne celle de toutes les lignes

du répertoire. Supposons en effet que l'on ait la certitude que 7692 correspond à.... : 1° On saura le numérotage des 99 autres lignes de la même page 76 ; 2° comme pour la facilité du déchiffrement la pagination est régulière, on est certain que la page précédente est paginée 75 et la suivante 77. Donc tout le répertoire s'en suit. Si la pagination était irrégulière, la connaissance d'une locution entraînerait seulement celle des 99 autres de la même page. Nous savons qu'un cryptographe pense à séparer les lignes d'une page d'un répertoire, genre Sittler, en dizaines, se réservant de changer à volonté le chiffre des dizaines, les unités seules restant fixes ; dans ce cas l'ennemi apprenant le numérotage d'une ligne connaît dix numéros, de plus il sait le numéro de la page et même de toutes les pages, si la pagination est régulière. Avec cette pagination il n'aura d'hésitation qu'entre dix locutions pour chaque nombre qu'il trouvera dans la dépêche.

67. Surveillance exercée sur les dépêches chiffrées. — Quelle que soit une dépêche chiffrée, par cela seul que les correspondants ne veulent pas être compris, la dépêche devient suspecte, et les gouvernements, tout en autorisant sa transmission, exercent sur elle une certaine

surveillance. C'est le plus souvent aux ministères chargés de la sécurité nationale, Affaires étrangères, Guerre, Intérieur, que l'Administration des télégraphes transmet copie de toute dépêche chiffrée, qu'elle provienne de l'étranger ou de l'intérieur, ou même qu'elle transite seulement sur le territoire.

68. Des procédés de déchiffrement. — La plus grande partie des journaux se servent du répertoire Sittler, aussi le procédé employé pour connaître leur pagination est des plus simples. Le fonctionnaire chargé de cette besogne n'a pas beaucoup de peine à se donner. Il reçoit la copie d'une dépêche transmise au journal par son correspondant étranger et cherche le lendemain, dans le corps du journal, la dépêche traduite émanant du correspondant en question. Quelles que soient les modifications apportées dans la traduction, sachant en somme de quoi il est question dans la dépêche, il n'est pas difficile, avec un Sittler sous les yeux, de trouver le numérotage d'un des mots. Le fonctionnaire prend en note que tel journal se sert d'un répertoire Sittler paginé de telle façon. Dorénavant il pourra donner à son gouvernement la traduction de toute dépêche adressée au journal avant

même que le journal lui-même ne l'ait traduite. Les diplomates usent surtout de tableaux chiffrants et déchiffrants, et nous avons vu que la connaissance d'une ligne n'entraînait aucunement celle des autres, aussi le procédé est-il moins simple, mais il a néanmoins une certaine analogie. Tous les gouvernements publient de temps à autre des Livres, bleus, jaunes, blancs, pour communiquer à leurs Parlements l'historique de certaines négociations. Le gouvernement voisin, par le territoire duquel les dépêches ont transité, a conservé précieusement le texte chiffré de ces dépêches. Le fonctionnaire spécial compare ce texte chiffré avec le texte clair qui lui est ainsi bénévolement livré, et recueille facilement des notions sur un grand nombre de lignes du tableau employé. Il en prend note soigneusement, s'efforçant de reconstituer l'ensemble du tableau. Le sens général d'une phrase dont il connaît cinq ou six mots lui en découvre forcément d'autres, et lorsqu'il possède quelques locutions usuelles, temps des verbes *être* ou *avoir*, désignation de personnages importants, il lui devient facile de déchiffrer de nouvelles dépêches et d'enrichir son répertoire. Son travail reste utile tant que le gouvernement visé n'a pas changé le numérotage de ses tableaux.

Pour éviter ce déchiffrement facile de son répertoire, M. Sittler propose différents artifices, par exemple modifier, d'une façon convenue, les nombres régulièrement obtenus; le mot situé page 96, ligne 72 qui devrait s'écrire 9672, deviendrait 7296 ou 9762 ou 9267, etc. Ce procédé qui serait percé à jour par la connaissance d'un seul mot, a de plus l'inconvénient d'obliger à une attention soutenue les correspondants qui ont en général assez de travail avec le déchiffrement lui-même.

Pour les tableaux chiffrants, on propose d'ajouter un nombre convenu, mais souvent variable, aux nombres réguliers. Supposons qu'aux groupes 7742, 8536, 0279 on ajoute le quantième du mois 17, par exemple, on expédiera la dépêche chiffrée 7759, 8553, 0276. Mais cet artifice ne tromperait pas longtemps un déchiffreur un peu sagace qui aurait déjà formé une partie de son tableau. En somme, il est dangereux de conserver le même tableau après la publication d'un de ces livres diplomatiques dont nous venons de parler, il n'est même pas prudent, d'une manière générale, de conserver sans changement, le même tableau chiffrant plus de deux ou trois mois.

CINQUIÈME PARTIE

OBSERVATIONS ET NOTIONS GÉNÉRALES

CHAPITRE PREMIER

OBSERVATIONS SUR L'ENSEMBLE DES MÉTHODES PRÉCÉDENTES

69. Critiques faites. — On a pu remarquer que les nombreux systèmes exposés dans les chapitres précédents ont tous prêté le flanc à des critiques, que nous nous sommes efforcé de justifier en indiquant des méthodes de déchiffrement qui doivent réussir presque toujours. Mais il est bien entendu aussi que nos critiques concernent exclusivement les systèmes en tant que devant être appliqués à un service régulier et

permanent. Il est parfaitement possible qu'une dépêche isolée reste indéchiffrable dans certaines conditions.

70. Combinaisons de méthodes. — Mais il y a encore un moyen de rendre excellents la plupart des systèmes exposés, même les médiocres, c'est de combiner entre eux deux systèmes de familles différentes. Si l'on modifie par une méthode à anagramme la suite naturelle des lettres d'un texte chiffré avec des alphabets ou la suite des chiffres obtenus par un répertoire, les nouveaux textes chiffrés seront peut-être indéchiffrables, mais en général la longueur de cette double opération de chiffrement fait rejeter cet artifice.

71. Conclusion. — Aussi notre conclusion est-elle, qu'en dépit des inventeurs qui proposent journellement des méthodes indéchiffrables, rien n'est plus difficile que d'en combiner une, présentant même des qualités sérieuses.

CHAPITRE II

—

DE LA FRÉQUENCE DES LETTRES DANS LA LANGUE FRANÇAISE

72. Choix des textes à analyser. — M. Kerckhoffs a donné des nombres représentant la fréquence relative des lettres en français, mais il n'a pas indiqué le nombre de lettres analysées qui lui avait fourni ces résultats. Dans certaines études, les chiffres admis ne nous ont pas donné pleine satisfaction, aussi avons-nous tenu à refaire ce travail sur des bases absolument nouvelles. Nous avons d'abord pensé que cent mille lettres étaient nécessaires pour donner des moyennes

se rapprochant autant que possible de la vérité. De plus, il nous restait à choisir un texte satisfaisant. Un ouvrage quelconque d'une certaine longueur ne traitant qu'un seul sujet peut parfaitement ne pas représenter une moyenne, car les exigences du sujet ou le style de l'auteur peuvent faire prédominer certaines tournures de phrases. Nous avons donc voulu que le plus grand nombre de sujets possibles fussent traités et par des écrivains différents. Un numéro de journal se trouvait ainsi désigné et nous avons choisi *le Temps*, numéro du 2 mars 1891. L'analyse des trois premières pages nous a donné 80000 lettres, nombre suffisant à cause de la constance des résultats obtenus.

73. Résultats. Tableaux. — Le tableau A donne les chiffres trouvés par fractions de dix mille lettres environ.

Le tableau B présente les lettres par ordre de fréquence EASINTRULO, il indique leur proportion sur mille et donne aussi à titre de renseignements le nombre de redoublement de lettres relevés. On voit qu'en français L, S sont les deux lettres qui se redoublent le plus fréquemment. Ajoutons encore que sur les 13884 E relevés, les E muets se trouvent au

nombre de 6599, soit un peu moins de la moitié. Nous avons compté comme E muet : *que*, *je*, *le*, *ville*, etc.

TABLEAU A

A	878	761	859	775	801	797	914	787
B	79	90	95	100	75	99	88	90
C	326	356	342	340	345	281	406	341
D	399	383	422	463	315	336	454	412
E	1696	1710	1702	1674	1739	1916	1672	1775
F	103	110	121	80	89	117	88	93
G	92	107	121	100	77	71	98	93
H	74	67	81	51	73	81	68	71
I	817	739	735	769	733	734	750	719
J	35	38	35	43	51	61	46	48
K	7	5	7	5	1	//	//	4
L	612	515	577	563	618	663	502	605
M	271	254	233	275	306	324	250	284
N	728	715	731	707	729	641	780	739
O	528	592	530	611	547	501	514	517
P	305	336	266	296	249	258	270	283
Q	126	130	91	84	118	116	104	120
R	751	723	719	789	610	640	696	742
S	769	772	769	876	814	743	840	819
T	694	754	706	714	667	724	748	671
U	579	651	595	574	662	657	582	670
V	137	157	144	117	147	159	192	122
W	//	1	10	1	2	//	//	//
X	29	36	46	58	36	43	48	44
Y	15	12	18	27	24	23	24	26
Z	12	2	13	2	35	10	10	6
	10062	10016	9968	10094	9863	9995	10144	10081

TABLEAU B

	Nombre total	Redoublements	Proportion pour 1000
E	13884		174
A	6572		82
S	6402	342	80
I	5996		75
N	5770	179	72
T	5678	198	71
R	5670	128	71
U	4970		62
L	4655	386	58
O	4340		54
D	3184	2	40
C	2737	48	34
P	2263	98	28
M	2197	176	27
V	1175		15
Q	889		11
F	801	99	10
G	759	3	9
B	716		9
H	566		7
J	357		4
X	340		4
Y	169		2
Z	90		1
K	29		//
W	14		//
	80223		1000

En consultant le tableau C le lecteur verra qu'une phrase contient en moyenne 21,5 mots,

mais les moyennes partielles varient de 18 à 27, écart trop grand pour que l'on puisse faire un fonds sérieux sur ces chiffres. Au contraire, le même tableau C montre qu'un mot contient 4,5 lettres en moyenne générale avec des écarts de 4,06 à 4,72. Ces chiffres sont très sensiblement constants et bien inférieurs au nombre généralement admis de six lettres par mot.

TABLEAU C

Phrases	Moyennes des mots contenus dans une phrase	Mots	Moyennes des lettres contenues dans un mot	Lettres
103	21,07	2171	4,6347	10062
80	27	2167	4,6220	10016
100	21,25	2125	4,691	9968
106	20,17	2138	4,721	10094
132	18,4	2428	4,062	9863
121	19,88	2406	4,154	9995
96	22,52	2162	4,692	10144
93	24,47	2276	4,429	10081
831	**21,5**	**17873**	**4,4967**	**80223**

CHAPITRE III

—

RENSEIGNEMENTS SUR LES TRANSMISSIONS TÉLÉGRAPHIQUES DES DÉPÊCHES SECRÈTES

74. Instruction T. — Les règlements pour la transmission télégraphique des dépêches secrètes, se trouvent dans un manuel désigné sous le nom de « Instruction T ». On peut le consulter dans tous les bureaux télégraphiques. Ce manuel doit être tenu à jour par les employés.

75. Résumé des règlements. — L'article 29 de cette instruction spécifie que le texte d'un télégramme privé peut être rédigé en langage secret convenu ou chiffré, ou en un mélange de

ces deux langages, s'ils sont admis par l'office de destination. Le texte des télégrammes d'État ou officiels peut être rédigé dans les mêmes formes que les télégrammes privés, mais le mélange de chiffres et de lettres n'est pas admis.

L'article 31 donne la définition du langage secret, qu'il distingue en langage convenu et langage chiffré. On entend par télégrammes en *langage convenu* ceux où il est fait emploi de mots, qui, tout en présentant un sens intrinsèque, ne forment pas de phrases compréhensibles pour les bureaux des offices en correspondance. Ces mots doivent être empruntés à l'une ou plusieurs des langues française, latine, allemande, anglaise, espagnole, hollandaise, italienne et portugaise, et ne pas contenir plus de dix lettres pour les relations extérieures. Le bureau d'origine peut demander la production du vocabulaire, afin de vérifier l'authenticité des mots employés. Mais il résulte d'une lettre de M. le Directeur Général des Postes et Télégraphes du 7 avril 1892 (annexée) que cette production du vocabulaire est strictement bornée à permettre de déterminer la langue à laquelle appartiendrait un mot litigieux. Elle ne peut entraîner la recherche du sens attaché par l'expéditeur aux mots convenus qu'il emploie.

On entend par télégrammes en *langage chiffré* ceux dont le texte est intégralement ou partiellement formé de groupes ou bien de séries de chiffres ayant une signification secrète. Le texte chiffré des télégrammes privés doit être composé exclusivement de chiffres arabes. L'emploi de lettres ayant une signification secrète est *toléré* dans les relations du service intérieur, mais il est *interdit* dans les relations internationales.

76. Observations. — Ces derniers règlements modifient essentiellement les précédents qui admettaient le langage chiffré en groupes de lettres. D'après la lettre déjà visée de M. le Directeur des Postes et Télégraphes cette modification a été introduite le premier juillet 1891, dans les relations internationales, et elle est motivée par l'impossibilité de transmettre avec exactitude des groupes de lettres, n'offrant ni sens ni cohésion. Il est à croire que la même modification sera introduite prochainement aussi dans les relations du service intérieur. Il en résulte que la plupart des systèmes que nous avons étudiés dans les précédents chapitres seraient inapplicables pour la télégraphie privée. Mais ils pourraient néanmoins être utilisés dans

les correspondances postales ou pour les télégrammes d'État, officiels. Remarquons que les gouvernements eux-mêmes se sont privés d'un moyen de correspondre qui aurait pu leur être utile dans des circonstances spéciales. Supposons en effet un officier en mission secrète à l'étranger; pour correspondre télégraphiquement avec lui, le Ministre de la Guerre devra employer une autre méthode de chiffre que celle dont l'officier a l'habitude, ou alors il sera tenu de lui faire parvenir un télégramme officiel qui dévoilera son identité.

77. Répertoire de lettres. — Il y a, du reste, un moyen de tourner la difficulté. A la suite du dictionnaire ABC, que nous nous proposons de faire paraître sera annexé un répertoire contenant uniquement les 15 625 combinaisons possibles des 25 lettres prises trois à trois, et à chaque combinaison correspondra un mot de convention satisfaisant aux règlements internationaux. Il en résultera que si l'on a adopté, en général, une méthode de chiffrement produisant des groupes de lettres, on ne sera pas tenu d'y renoncer pour des télégrammes internationaux. En traduisant chaque groupe de trois lettres par le mot convenu correspondant, le télégramme

secret prendra une tournure commerciale qui le rendra admissible sur toutes les lignes télégraphiques, et cet avantage pourra compenser l'excédent de travail qui en résultera pour les correspondants.

78. Erreurs dans les transmissions. — D'ailleurs, cette traduction de groupes de lettres en mots convenus aurait aussi un grand avantage dans quelques circonstances. Il est certain que, malgré les collationnements, la transmission fidèle des groupes de lettres est difficile, et cette difficulté pourrait servir de prétexte à certains gouvernements étrangers, dont les employés altéreraient, plus ou moins sciemment, les dépêches d'un autre gouvernement, dépêches supposées d'une extrême urgence. La traduction préalable des groupes de lettres en mots convenus ôterait tout prétexte à de pareilles manœuvres, et d'ailleurs localiserait l'erreur, s'il s'en commettait une, un mot étant transmis pour un autre; on verrait immédiatement dans la traduction quel est le groupe de lettres altéré, et une erreur localisée est toujours facile à réparer.

79. Lettre du Directeur des postes et Télégraphes.

MINISTÈRE
Du Commerce,
et de l'Industrie

DIRECTION GÉNÉRALE
Des Postes
et des Télégraphes

Exploitation électrique

1er BUREAU

Correspondances télégraphiques

RÉPUBLIQUE FRANÇAISE

Paris, le 7 avril 1892

Monsieur,

N° 229-0

J'ai l'honneur de vous donner ci-après les renseignements que vous m'avez demandés par votre lettre du 29 mars dernier :

1° Depuis le 1er juillet 1891, date de la mise en vigueur du nouveau règlement télégraphique international, révisé à Paris en 1890, l'emploi de lettres ayant une signification secrète est interdit dans les relations internationales

Cette suppression a été motivée par l'impossibilité de transmettre, avec une entière sécurité et une parfaite exactitude, des groupes de lettres n'offrant par elles-mêmes

Monsieur de Viaris, 8, rue Appert, à Paris.

ni sens ni cohésion et représentées par des signaux entre lesquels se produisent fréquemment d'inévitables confusions.

L'usage des lettres est par exception admis pour la reproduction des marques de commerce ainsi que dans les télégrammes d'Etat et dans les télégrammes sémaphoriques provenant d'un navire en mer quand l'expéditeur a demandé la transmission du texte en signaux du code commercial.

L'usage en France du langage en lettres secrètes est interdit dans les relations internationales et provisoirement toléré dans les relations intérieures, aucun acte législatif n'étant encore intervenu pour en étendre l'interdiction à la correspondance du régime intérieur.

2° Dans le langage convenu, les mots doivent appartenir à l'une ou à plusieurs des huit langues admises pour la correspondance télégraphique. Dans le régime intérieur, ces mots ne doivent pas avoir plus de 15 caractères et dans le régime international plus de 10 caractères. Le bureau d'origine a le droit de demander communication du code de l'expéditeur s'il suppose que les mots présentés ne sont pas réguliers et ne sont que des assemblages arbitraires de lettres. Comme on ne se préoccupe pas de connaître le sens attaché par l'expéditeur aux mots convenus qu'il emploie, on s'attache surtout à faire déterminer la langue à laquelle appartiennent les mots litigieux.

Les noms propres ne sont admis dans les télégrammes en langage convenu qu'avec leur signification en langage clair.

3° Par application de l'article XIX, § 3 du décret du

16 avril 1881 qui régit la correspondance télégraphique intérieure, les télégrammes privés en langage secret sont soumis à la formalité de la recommandation (Collationnement et accusé de réception). La taxe du collationnement est égale à la moitié de celle d'un télégramme ordinaire de même longueur. La taxe de l'accusé de réception est égale à celle d'un télégramme ordinaire de dix mots.

Dans le régime international cette obligation n'existe pas.

Recevez, Monsieur, l'assurance de ma considération distinguée.

Le Directeur général des Postes et des Télégraphes

POUR LE DIRECTEUR GÉNÉRAL :

Le Directeur du Matériel et de l'Exploitation Electrique,

Signature illisible.

CHAPITRE IV

—

DE DEUX MÉTHODES A ALPHABETS N'EMPLOYANT QUE DES CHIFFRES ARABES

80. Méthode anglaise. — La suppression des dépêches chiffrées en groupes de lettres nous amène à dire quelques mots de deux méthodes employant exclusivement des chiffres. L'une est usitée en Angleterre. Son principe est simple. Elle emploie les nombres de 00 à 99, et attribue à chaque lettre de l'alphabet, pour la représenter, une quantité de ces nombres proportionnelle à la fréquence de la lettre dans la langue. Appliquée au français, il faudrait attribuer à l'E 18 nombres, à l'A 8, à l'S 8, etc. Il suffit alors dans le chiffrement d'une lettre, de prendre

alternativement les différents nombres qui peuvent représenter cette lettre. Cette méthode a l'inconvénient de doubler le nombre des caractères à transmettre, puisque chaque lettre est représentée par deux chiffres. Si le tableau de répartition est fixe, il constitue un répertoire dont la connaissance annule le secret des dépêches. Nous n'avons pas pu savoir si le tableau varie avec un mot de convention et comment se fait cette variation.

81. Autre méthode. — Nous avons soumis en 1890 au Ministre de la Guerre, qui n'a pas cru devoir l'adopter, une autre méthode à chiffres arabes reposant sur un principe tout-à-fait différent. Les lettres étaient partagées en trois séries de fréquence et leur nombre était porté à 29 par la distinction faite entre trois espèces d'E, l'E muet, l'E s'écrivant avec accent, et l'E qui n'est ni muet ni accentué, le mot *pensée* renferme un échantillon de ces trois espèces d'E; d'ailleurs cette distinction était théorique et les espèces d'E pouvaient impunément être confondues dans la pratique; il y avait aussi deux sortes d'A. La 1re série de fréquence comprenait une sorte d'A, deux E, puis I, N, O, R, S, T, U. Les lettres de la 2e et de la 3e série étaient placées

sous celles-ci dans un ordre fixe; et l'on établissait la convention suivante. Si au moyen d'une clef numérique de dix, l'A était représenté par 8, l'N par 2 etc., les lettres correspondantes de la 2e série devaient être représentées par 88, 22, et celles de la 3e série par 888,222. Il est certain que le nombre des caractères à transmettre était encore notablement augmenté, mais cette augmentation ne dépassait pas 33 pour cent, au lieu d'atteindre 100 % comme dans la méthode précédente. Pour mettre en pratique cette méthode, il fallait, dans le texte clair, supprimer les lettres redoublées; de plus cette transformation par un alphabet unique n'aurait pas donné à elle seule une sécurité suffisante; une fois le texte chiffré, il était nécessaire de transposer les chiffres obtenus par une méthode à anagramme aussi simple que possible. Néanmoins ces difficultés de pratique pouvaient effrayer au point de vue d'un service régulier.

CHAPITRE V

APPAREIL DU CAPITAINE BAZERIES

82. Son fonctionnement. — Nous avons déjà donné quelques détails sur le cryptographe cylindrique du capitaine Bazeries (2e partie, chap. v, § **48**), qui par son aspect général rappelle les anciens cadenas à lettres. L'appareil que nous avons vu se composait de 20 rondelles numérotées ; sur chacune était gravé un alphabet quelconque, chaque alphabet étant d'ailleurs indépendant du suivant. Nous avons dit qu'après avoir enfilé les rondelles sur le cylindre dans un ordre déterminé par une clef numérique de 20, on faisait tourner convenablement les rondelles pour aligner les 20 premières lettres du texte clair suivant une génératrice du cylindre marquée zéro ; une fois les rondelles assujetties dans cette position, on prend comme texte chiffré la suite des lettres donnée par l'une quelconque des 24 autres génératrices.

83. Remarques. — Nous croyons qu'il peut être utile de faire connaître comment nous sommes parvenu à déchiffrer ces dépêches ; les inventeurs pourront ainsi voir que le plus faible indice suffit pour donner une base sérieuse à toute une méthode de déchiffrement.

En maniant le cryptographe cylindrique, voici la remarque que nous avons faite. Si l'on suppose le texte clair uniquement composé de lettres E, chaque génératrice présente une composition essentiellement différente de sa voisine ; ainsi la première génératrice est composée de 1 A, 1 B, 2 C, 3 D, 1 G, 2 H, 1 L, 1 O, 1 R, 2 S, 2 T, 2 U, et 1 X ; la 2e de 2 A, 3 F, 1 G, 1 H, 1 I, 1 J, 3 N, 1 O, 2 P, 1 R, 1 T, 1 V, 1 Y, 1 Z et ainsi de suite, il n'y a pas deux génératrices dont la composition soit la même. Cette composition est indépendante de l'ordre des rondelles, en sorte que si l'on suppose le texte clair formé d'une suite de lettres E, la composition en lettres d'une génératrice indiquera son *numéro*, quelque soit l'ordre des rondelles. La remarque faite pour la lettre E s'applique à toutes les autres lettres. Il en résulte donc aussi qu'à une génératrice donnée une lettre ne sera jamais représentée que par *douze* ou *treize* des 24 autres lettres. Telles sont les bases sur lesquelles nous nous sommes appuyé.

84. Déchiffrement connaissant les numéros des génératrices employées. — Nous avons demandé au capitaine Bazeries de nous remettre une dépêche en nous indiquant les numéros des génératrices qu'il aurait employées. Auparavant nous avions formé d'après l'appareil le tableau des génératrices de E, c'est-à-dire un tableau synoptique indiquant que pour la rondelle n° 1 l'E est représenté par un H à la 1re génératrice, par un I à la 2e, par un J à la 3e etc. ; qu'à la rondelle n° 2, l'E est représenté par U à la 1re génératrice, par Y à la 2e et ainsi de suite. L'appareil ayant 20 rondelles, si l'on sépare la dépêche chiffrée en tranches de 20 lettres, les lettres de même rang dépendent de la même rondelle. Voici la dépêche reçue :

Génératrice employée	
5	N D G I R S F N N F K O H J C M G C L J
7	C E U Q M J K T M B X H J C L I G F S K
11	Q I K Y M R J K Q P M J D Y Q I K V F V
1	Q X D D Z N M L J B Y S Q N T S A I P U
20	Z L T E Y Q H B R E A E Q F Y H X Q T Y
13	M N Q O Q L A Y F V D Y I A F S H R U D
10	P F J C T L C T Z C X H G K N G H X D J
14	P F S U Y X Q B I D V Y K O G Y P Y R Z
19	R N Y F F G O Q M U J H N Y G M S X Z Y
7	P K N J P D V O Q S X J X J M L Z S F X
6	D D D D B Q F S N H N Z I N J V J I H U
15	Q G V A V O U F O P J D H E X Y Q O R Q
17	U N S B U S Y O Q V E A Y U I T A B X G
//	U V

J'ai supposé que le texte chiffré était composé uniquement de lettres E et j'ai cherché dans le tableau synoptique quelles rondelles pouvaient donner, pour E texte clair, la lettre correspondante du texte chiffré, en admettant que l'on ait employé les génératrices désignées. Voici les premiers résultats.

1re ligne verticale	Numéros de rondelles	2e ligne verticale	Numéros de rondelles	etc.
N	//	D	2, 15	
C	//	E	//	
Q	4, 9	I	//	
Q	//	X	6	
Z	8, 10	L	//	
M	7, 8, 14	N	2, 12	
P	9	F	//	
P	2, 12	F	//	
R	9	N	5	
P	6	K	//	
D	17, 19	D	17, 19	
Q	2, 3, 10, 12	G	//	
U	//	N	//	

En réalité le texte chiffré n'est pas composé exclusivement de E, mais la lettre E représente environ 18 % de ce texte. On peut donc supposer que la rondelle dont le numéro se représente le plus fréquemment dans chaque colonne est celle qui correspond réellement à des E et par suite est celle que l'on a véritablement employée. En appliquant cette supposition à l'exemple,

j'ai trouvé désignées les rondelles 9, 2, 19, 3, 17, ″, 18, 8 etc.; la 6e colonne et les 9e, 10e, 11e ne donnaient plus de résultats bien appréciables. En enfilant sur le cryptographe les rondelles dans l'ordre ci-dessus, le texte chiffré se traduisait par :

l	*e*	*c*	*e*	*t*	.	*t*	*j*	. . . *n* . .	etc.
m	*p*	*t*	*o*	*n*	.	*d*	*u*	. . . *s* . .	″
e	*l*	*e*	*d*	*e*	.	*e*	*s*		″
n	*s*	*v*	*e*	*u*	.	*l*	*u*		″
a	*p*	*a*	*d*	*e*	.	*e*	*n*		″

Au début de la dépêche on voit immédiatement apparaître les mots : *le Petit Journal*, ce qui indique que la 3e rondelle est mauvaise. Pour avoir un *p* en clair à la 5e génératrice avec la lettre G du texte chiffrré, il faut la rondelle 14 et la traduction complète de la dépêche est : « *Le Petit Journal et le Temps ont dû vous apprendre le décès de ce pauvre Monsieur Lucas enlevé si rapidement, c'est bien malheureux. Il laisse inachevé(e) une œuvre très remarquable sur la théorie des nombres* ; *le premier volume a paru, quant aux deux autres il est à présumer qu'ils ne sont pas prêts à voir le jour de longtemps.* » Ajoutons que la clef numérique employée était :

9. 2. 14. 3. 17. 6. 18. 8. 13. 20. 16. 12. 1. 10. 11. 4. 15. 5. 19. 7.

et que d'après les principes énoncés dans l'étude des clefs, j'en ai déduit que le mot clef était

LE PETIT JOURNAL.

85. Déchiffrement connaissant un mot. A la suite de ce résultat le capitaine Bazeries m'a remis une dépêche, dans laquelle se trouvait le mot « *officier* ». Les numéros des génératrices employées n'étaient pas connus. Voici le texte de cette dépêche :

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

J'ai fait observer précédemment qu'à une génératrice donnée une lettre déterminée ne pouvait être représentée que par douze ou treize des autres lettres. Si donc je suppose que le mot connu « officier » a été chiffré avec la 1re génératrice, le polygramme inconnu du texte de la dépêche correspondant ne pourra commencer que par l'une des lettres susceptibles de chiffrer la lettre O à la 1re génératrice, ces lettres sont ABCEFLPRTUV; tout polygramme commen-

çant par une autre lettre ne pourra être celui que je cherche; mais le même raisonnement s'appliquant aux lettres suivantes du polygramme, je suis amené à former le tableau :

1re *génératrice*

O peut être représenté par		A B C E F L P R T U V
F	//	B C G H I J K M P
F	//	B C G H I J K M P
I	//	B D F G H K L M N P S T X Y Z
etc.		etc.

Sous chaque ligne du texte chiffré je fais glisser un papier où le mot OFFICIER est écrit à intervalles égaux à ceux des caractères de la dépêche et je présente ce mot devant les polygrammes pouvant commencer par un O (en texte clair). J'examine si la 2e lettre de ce polygramme peut représenter un F, si la 3e peut aussi être un F, la 4e un I etc., le procédé est plus long à expliquer qu'à appliquer. La dépêche étant assez courte, l'essai d'une génératrice m'a pris de 10 à 15 minutes. Notons en passant que ce travail d'essai pourrait être fait par 20 secrétaires examinant chacun l'hypothèse d'une des 20 génératrices du cylindre (M. Bazeries recommande de n'employer qu'exceptionnellement les quatre génératrices immédiatement voisines du zéro, elles ne sont d'ailleurs pas numérotées sur l'appareil).

Revenons à la traduction de notre dépêche.

En essayant la 2e génératrice, le polygramme AIIUCKUAB était indiqué comme pouvant représenter OFFICIER, avec certaines rondelles. Ces rondelles immédiatemment essayées ne donnaient aucun résultat possible pour la traduction des lignes précédentes, la combinaison n'était donc pas la vraie. Auparavant à la 1re génératrice j'avais trouvé que la fin de la 6e ligne XBJ pouvait correspondre à OFF et que, les cinq lettres du commencement de la 7e ligne KFSSU pouvaient se traduire par ICIER. Je devais donc supposer la 6e ligne chiffrée avec la 1re génératrice, la 7e également et le mot *off | icier* coupé en deux par la fin de la 6e ligne, mais les numéros des rondelles pour OFF et pour ICIER étaient les mêmes, la combinaison n'était donc pas encore bonne, toutefois il y avait à la noter, d'autres génératrices pouvant mieux convenir. En effet, à la 3e génératrice XBJ pouvait encore donner OFF et voici les numéros des rondelles :

3e génératrice XBJ : 6 ou 9, 16, 3 ou 10 ;

1re // KFSSU : 3, 1, 17, 12 ou 18, 1,7 ou 16.

En éliminant les rondelles communes, 1, 3, 16, les quatre combinaisons à étudier étaient 6. 16. 10 avec 3. 1. 17. 12. 7 ou 3. 1. 17. 18. 7 ; ou bien 9. 16. 10 avec les mêmes.

Il a été très rapide de voir que la seule bonne était :

3. 1. 17. 18. 7 avec 6. 16. 10

car ces groupes de rondelles donnaient seuls des fragments de phrases très acceptables. D'ailleurs ces cinq premières rondelles indiquaient comme début de la dépêche LEGEN qui permettait d'essayer *le génie* ou *le général*, cette dernière hypothèse apparaissait comme la bonne et le reste de la dépêche se traduisait en quelques minutes ; le texte clair était :

Le général de division défile à la tête de sa division ayant à huit mètres derrière lui son chef d'état-major et à KKBOFAKK *derrière celui-ci les* officiers *de son état-major.*

D'après les conventions de l'auteur de la dépêche KKBOFAKK veut dire 1,5o.

Clef numérique :

3. 1. 17. 18. 7. 11. 3. 5. 15. 8. 4. 2. 19. 20. 9. 12. 14. 6. 16. 10.

On peut y remarquer immédiatement la combinaison 3. 1. 17. 18 répétée en 4. 2. 19. 20 qui fixe à *dix* le nombre des lettres du mot clef et permet de conjecturer que ce mot était :

« BASSE INDRE »

86. Déchiffrement d'une dépêche quelconque. — Après le déchiffrement de ces deux dépêches, M. Bazeries m'en a communiqué trois autres dont je ne savais rien, si ce n'est qu'elles étaient écrites toutes trois avec la même clef ; il serait fastidieux d'en indiquer intégralement le texte, disons seulement que l'une commençait par ZAEMX, la 2e par ZGJZZ et la dernière par CPGQK.

Des essais infructueux me firent voir qu'aucune d'elles ne contenait le mot « officier ». Ne sachant rien sur leur contenu, j'allais essayer des vocables communs comme *ement*, *eraient*, lorsque je fis d'abord l'hypothèse que l'une des dépêches pouvait bien commencer par LES. Après quelques nouveaux essais, très rapides ceux-là, je trouvai que si la 2e dépêche commençait par LES, les rondelles convenables donnaient DES pour début de la 1re ZAE, et LAV pour début de la 3e CPG. *Les* et *des* ne m'indiquaient pas la suite, mais *lav* ne pouvait commencer que LA VUE, LA VITESSE etc. Les rondelles convenables pour faire *la vitesse* me donnaient à la 2e dépêche 2e *les approv...* et pour la 1re *des parcs a...*

Le début de la 2e dépêche désignait clairement *les approvisionnements* dont les rondelles

formaient à la 1re dépêche : *des parcs aérostatiques* et à la 3e : *la vitesse d'une colonne...* Dès lors, toutes les rondelles étaient mises en place, c'est-à-dire les dépêches déchiffrées. Si j'avais essayé le vocable *ement* je l'aurais trouvé trois fois dans les dépêches qui contenaient les mots : approvisionnements, renseignements et gonflement. J'étais donc certain de réussir, si l'essai des débuts de dépêches ne m'avait rien donné. La clef numérique employée était :

8. 11. 1. 14. 5. 16. 2. 9. 19. 15. 6. 13. 17. 3. 7. 18. 20. 10. 12. 4.

Cette fois la découverte du mot clef fut moins facile, j'arrivai cependant à déterminer

INDRET DIX SEPT DEUX

ce qui, je l'ai appris depuis, voulait dire : Indret, 17 — 2, c'est-à-dire : *dix-sept février*. Au chapitre des clefs nous avons indiqué cette modification assez heureuse du mot clef, ici : *Indret*.

CHAPITRE VI

—

REPRÉSENTATION DES SIGNES NUMÉRIQUES ET ORTHOGRAPHIQUES

87. Nécessité d'une convention. — Il peut arriver que dans le courant d'une dépêche on ait absolument besoin d'indiquer la ponctuation ou l'orthographe exacte d'un nom propre ; à coup sûr il arrivera que l'on ait à parler de nombres qu'il serait trop long de traduire en toutes lettres ; quel que soit le système employé une convention s'impose.

88. Représentation des chiffres arabes et des nombres. — Voici celle que nous

proposons. Les dix chiffres arabes seront représentés par les dix premières lettres de l'alphabet :

A	B	C	D	E	F	G	H	I	J
1	2	3	4	5	6	7	8	9	0

et pour avertir de leur signification numérique, on les encadrera entre deux K ; ainsi KCK signifiera 3, et KCFIJAK, 36 901.

89. Les signes orthographiques. — Toutes les autres lettres de l'alphabet placées comme les dix premières entre deux K auront une signification de signes orthographiques :

L	M	N	O	P
virgule	*un point*	*alinéa*	*exclamation*	*interrogation*
,	.		!	?

P	R	S	T
guillemets	*parenthèse*	*trait d'union*	*apostrophe*
"	()	-	'

U	V	X	Y
cédille	*tréma*	*accent aigu*	*accent grave*
¸	¨	´	`

Z
accent circonflexe
^

90. Les signes relatifs aux nombres. — Mais on peut aussi sans crainte de confusion placer l'une de ces lettres entre deux des dix premières ou entre l'une d'elles et un K et alors lui donner une signification différente et ayant rapport aux signes numériques. L signifierait « virgule » comme ci-dessus et 25, 33 se traduirait par KBELCCK. Les autres letttres voudraient dire :

Q	R	S	T
numéro	*terminaison iéme*	*séparation de deux nombres*	*terminaison iémement*

U	V	X	Y
exposant ou puissance	*plus* +	*moins* −	*multiplié par* ×

Z
divisé par ou barre de fraction

Les lettres MNOP restent disponibles si l'on avait à établir d'autres conventions relatives aux nombres.

Donnons quelques exemples :

Numéro 27 : KQBGK ;
Vingt-septième : KBGRK ;
27 — 32 — 14 : KBGSCBSADK ;
Vingt-septièmement : KBGTK ;

27^4 : KBGUDK ;
27 plus 32 : KBGVCBK ;
32 moins 27 : KCBXBGK ;
32 multiplié par 27 ; KCBYBGK ;
32 divisé par 27 : KCBZBGK etc.

Dans les conventions précédentes nous n'avons pas parlé du point et virgule (;) qui se chiffrera KMLK, ni des deux points (:) que l'on traduira par KMMK.

SIXIÈME PARTIE

—

MÉTHODE NOUVELLE

CHAPITRE PREMIER

—

GENESE DE LA METHODE

91. Remarques sur les systèmes exposés précédemment. — Le lecteur a pu observer qu'au cours des études précédentes, aucun système n'a échappé à nos critiques. Nous avons proscrit les méthodes à anagramme, exposé les difficultés pratiques (pour l'Armée) des répertoires, enfin nous avons donné des marches certaines à suivre pour obtenir le déchiffrement des méthodes connues à base d'alphabets multiples.

92. Les tableaux carrés.— L'infériorité des tableaux carrés, tableau de Vigenère ou alphabets intervertis régulièrement, provient de leur trop grande symétrie. Leurs 25 alphabets peuvent tous s'obtenir au moyen d'un seul d'entre eux, dont on écrirait les lettres sur une circonférence. Aussi dans tous, une lettre donnée est toujours suivie et précédée des mêmes lettres, par exemple dans le tableau basé sur le mot CRYPTOGAME (2e partie, chap. v, § 42) la lettre Y sera constamment précédée de R et suivie de P.

93. Le cryptographe cylindrique. — Le cryptographe cylindrique dont les alphabets sont intervertis irrégulièrement, ne présente pas ce défaut, mais cependant nous avons obtenu le déchiffrement en remarquant qu'une lettre donnée n'est jamais suivie à une certaine distance, que de douze ou treize des vingt quatre autres lettres.

94. Desideratum. — On est donc amené à penser qu'on obtiendrait des résultats supérieurs en employant des alphabets composés de telle sorte, que dans leur ensemble, une lettre quelconque soit suivie alternativement de chacune des 24 autres.

CHAPITRE II

—

CRÉATION DES ALPHABETS

95. Recherches préliminaires. — Est-il possible de créer 24 alphabets satisfaisant au précédent desideratum, c'est-à-dire tels que A soit suivi dans un alphabet de B, dans un autre de C, dans le 3e de D ; que B soit suivi alternativement de A, C, D et ainsi de suite. Nous n'avons pu réussir ni à combiner 24 alphabets satisfaisant à cette condition, ni à démontrer mathématiquement que cette combinaison était impossible. Mais nous avons trouvé une méthode qui permet de créer 120 (5×24) alphabets qui dans leur ensemble satisfont à la condition désirée, c'est-à-dire que dans l'ensemble de ces 120

alphabets A sera suivi de B cinq fois, de C cinq fois également, et aussi de D, E, F, etc. ; B sera suivi cinq fois de A, C, D et ainsi de toutes les lettres.

96. Mode d'opérer. — Considérons la série des 25 premiers nombres rangés dans leur ordre naturel :

1. 2. 3. 4. 5. 6. 7. 8. 9. . . . 24. 25

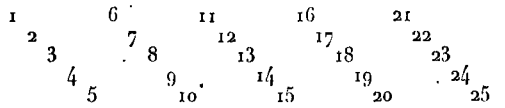
Si maintenant on prend ces nombres de deux en deux, de trois en trois et ainsi de suite, on obtient un certain nombre de combinaisons toutes différentes, dans lesquels 1 ne sera jamais à côté du même nombre :

1. 3. 5. 7. . . 1. 4. 8. 12. . . 1. 5. 9. 13. . .
. . . 1. 7. 13. 19. . .

Remarquons l'absence de la série qui commencerait par 1. 6. 11. 16. . ; celle-ci ne peut pas, en conservant la régularité de la marche adoptée, employer tous les nombres parce que la période est de 5, et que 5 est le diviseur de 25 ; il en est de même des séries de 10 en 10, de 15 en 15, de 20 en 20. On ne peut obtenir que 20 séries complètes, symétriques deux à deux et dans

lesquelles 1 sera suivi de 20 nombres différents. Les nombres absents sont 6, 11, 16, 21. De même dans ces séries 2 ne sera pas suivi de 7, 12, 17, 22 ; 3 de 8, 13, 18, 23, etc. Si l'on forme le tableau :

TABLEAU I



les nombres placés sur la même horizontale ne se trouvent pas voisins les uns des autres dans les 20 séries formées comme nous venons de le dire. On peut écrire les cinq tableaux suivants dont le mode de dérivation du premier est évident.

TABLEAU II

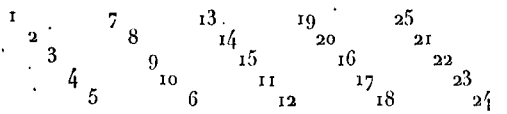


TABLEAU III

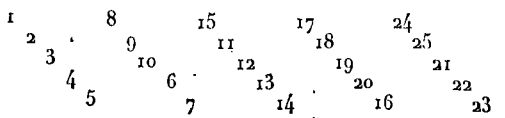


TABLEAU IV

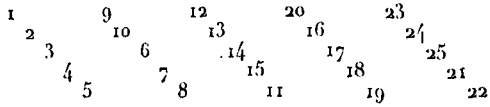


TABLEAU V

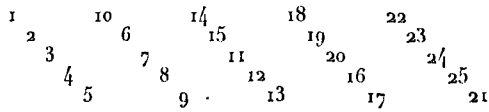
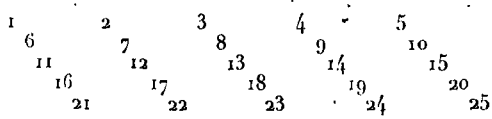


TABLEAU VI



97. Examen des tableaux. — L'examen de ces tableaux permet de voir qu'en formant pour chacun les 20 séries dont nous avons parlé ;

Dans les séries dépendant du tableau { I, II, III, IV, V, VI } 1 ne sera pas suivi de { 6, 11, 16, 21 ; 7, 13, 19, 25 ; 8, 15, 17, 24 ; 9, 12, 20, 23 ; 10, 14, 18, 22 ; 2, 3, 4, 5 }

En somme les *six* tableaux auront formé 120 séries (6×20) et dans leur ensemble, le nom-

bre 1, ou un nombre quelconque, sera suivi *cinq* fois de chacun des autres nombres, puisque à chaque tableau quatre des nombres font défaut :

$$5 \times 24 = 6 \times 20 = 120$$

Les tableaux établis, rien de plus simple que de former les alphabets cherchés ; il suffit de remplacer les nombres par des lettres d'un alphabet souche quelconque, alphabet ordinaire ou alphabet dérivant d'un mot.

98. Exemples d'alphabets. — On trouvera à la fin de cette étude cinq exemples des 120 alphabets que l'on obtient de cinq alphabets souches régulièrement inversés (1) :

1°	ABCDE	FGHIJ	KLMNO	PQRST	UVXYZ
2°	GHJFI	LMOKN	VXZUY	BCEAD	QRTPS
3°	MONLK	XZYVU	RTSQP	HJIGF	CEDBA
4°	SPQTR	DABEC	IFGJH	YUVZX	NKLOM
5°	ZYUXV	TSPRQ	EDACB	ONKML	JIFHG

(1) La clef de l'inversion est donnée par le tableau :

1	2	3	4	5
2	3	5	1	4
3	5	4	2	1
4	1	2	5	3
5	4	1	3	2

Les alphabets ont été rangés par séries ou tableaux de 24 de façon à présenter dans chaque tableau partiel la régularité la plus grande possible ; chaque tableau est désigné par une lettre.

99. Observation se rapportant au cryptographe cylindrique. — Nous rappelons encore une fois que la lecture des dépêches chiffrées avec l'appareil du commandant Bazeries a été obtenue parce que chaque génératrice d'une lettre donnée ne contient que douze ou treize des vingt-quatre autres lettres ; la théorie précédente permet de dire que ce mode de déchiffrement ne pourrait être appliqué à un cryptographe cylindrique construit de manière à recevoir 120 rondelles, si les 120 alphabets gravés sur ces rondelles dépendaient d'un alphabet souche et étaient formés comme nous venons de l'exposer. Si dans cette construction nouvelle, l'appareil restait maniable (pour un service exclusivement de bureau, par exemple celui du Ministère des Affaires Étrangères) les conditions de sécurité de son usage seraient considérablement améliorées. Dans les alphabets visés, en effet, non seulement une lettre est suivie *immédiatement* de cinq fois chacune des 24 autres, mais

cette régularité persiste à une distance quelconque de la lettre choisie. Par conséquent sur le cryptographe cylindrique envisagé, toutes les génératrices d'une lettre présenteraient identiquement la même composition.

CHAPITRE III

—

PRATIQUE DE LA MÉTHODE

100. Usage simultané de 600 alphabets. — Mais un appareil forcément compliqué est inadmissible dans un service actif comme celui de l'armée, où tout officier peut être appelé à chiffrer ou déchiffrer une dépêche, loin de son bureau ordinaire, peut-être même en rase campagne. Aussi la pratique de notre méthode n'emploie-t-elle aucun appareil mécanique. Au lieu de 120 alphabets, nous en employons simultanément 600, soit cinq séries de 120. Comme exemple, nous prendrons les 25 tableaux contenant chacun 24 alphabets ($25 \times 24 = 600$), imprimés à la fin de l'ouvrage. D'ailleurs en se conformant aux principes énoncés, on pourrait construire 600 autres alphabets entièrement diffé-

rents. Nous ne verrions aucun intérêt pratique, au point de vue de la sécurité, à cette construction, les alphabets employés pouvant impunément être connus de tous, mais il faut compter avec les errements de certaines administrations, qui réclament impérieusement le mystère pour les procédés qu'elles emploient.

101. Présentation des alphabets. — On choisira pour se servir des alphabets la forme qui sera la mieux appropriée aux circonstances variées du service. Dans un bureau, les alphabets pourront être imprimés sur un cartonnage en forme de tableaux synoptiques. En les disposant par feuillets de 120, on peut obtenir un carnet de cinq feuilles extrêmement portatif. On pourrait aussi en faire 25 feuillets contenant chacun 24 alphabets et les monter sur un pivot, tout à fait comme des lames d'éventail. Ce ne sont que des détails accessoires à noter en passant.

102. Coordonnées de la lettre chiffrée. — On a pu faire l'observation que dans toutes méthodes à alphabets connues, la désignation de la lettre du texte chiffré est donnée par l'emploi de deux coordonnées, véritables axes des X et des Y dans les tableaux carrés ; ces deux coor-

données sont la lettre de la clef et celle du texte clair. Dans notre méthode il serait impossible pratiquement de former une clef numérique de 600, aussi aurons-nous recours à un principe nouveau, qui sera l'emploi de trois coordonnées pour désigner l'emplacement de la lettre du texte chiffré. Celle du texte clair sera, bien entendu, toujours l'une d'elles, mais nous déduirons deux clefs différentes du même mot clef. Ainsi du mot clef RÉPUBLIQUE, nous formerons le tableau déjà cité :

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

et par des procédés connus et d'ailleurs évidents, nous écrirons deux clefs littérales de 25.

1re *clef, dite horizontale*

REPUBLIQKJHGFDCAMNOSTVXYZ.

2e *clef, dite verticale*

RKMEJNPHOUQSBFTLDVICXQAYZ.

Chaque tableau de 24 alphabets étant désigné par une lettre majuscule, l'une des clefs nous

servira à indiquer un tableau, la seconde à choisir dans ce tableau un alphabet. Cherchant dans cet alphabet la lettre du texte clair, nous prendrons comme texte chiffré, celle qui la suit immédiatement. Pour la traduction de la dépêche, la marche est identique : recherche d'un tableau, — 1re coordonnée ; dans ce tableau un alphabet, — 2e coordonnée ; dans cet alphabet une lettre, ici la lettre du texte chiffré, — 3e coordonnée, et obtention du texte clair par la lecture de la lettre qui précède immédiatement.

103. Usage des clefs. — La dépêche à chiffrer sera disposée par lignes contenant 25 lettres ; prenons un exemple :

Lescandidatsvélocipédiste
smilitairesnesesontgénéra
lementprésentésquentrèspe
titnombreauxexamensdumois
dejuin.

La dépêche a 106 lettres et le mot clef est RÉPUBLIQUE. En tête de la dépêche au-dessus de la 1re ligne, on écrira la 1re clef donnée précédemment, clef horizontale, en commençant par la 7e lettre IQKJH... etc, et l'on conviendra que les lettres de chaque ligne verticale seront chif-

frées avec des alphabets pris dans le tableau correspondant. Le tableau I donnera les alphabets pour chiffrer *l*, *s*, *l*, *t*, *d*, le tableau Q pour les lettres *e*, *m*, *e*, *i*, *e*, le tableau K pour la 3e colonne verticale et ainsi des autres. La 1re clef s'appellera donc *clef des tableaux*. La 2e clef sera la *clef des alphabets*, on la transcrira verticalement sur une bande de papier que l'on présentera successivement devant chaque colonne verticale. Par exemple, les trois premières colonnes seront chiffrées ainsi :

Alphabets	Tableau I		Alphabets	Tableau Q		Alphabets	Tableau K
J			U			T	
N			G			L	
+ P	*l*		+ S	*e*		+ D	*s*
H	*s*		B	*m*		V	*i*
O	*l*		F	*e*		I	*m*
U	*t*		T	*i*		C	*t*
G	*d*		L	*e*		X	*j*
S			D			Q	

Il reste à déterminer dans quelles conditions se fait cette présentation. On voit bien que d'une colonne à l'autre, nous avons suivi l'ordre des lettres sur la bande de papier. Nous avons commencé à la *septième* lettre P, été jusqu'au G, recommencé à l'S, employé l'L et de là passé au D. Nous avons l'intention de demander beaucoup à notre méthode, et l'on pourrait

craindre que cette régularité ne présentât des inconvénients au point de vue de l'indéchiffrabilité. On verra plus loin qu'il n'en est rien, et la pratique du chiffrement est très simple ainsi.

104. Caractère individuel à chaque dépêche. — Notre point de départ dans l'usage des deux clefs a été leur *septième* lettre : I pour la clef des tableaux, P pour celle des alphabets. Ce choix dépend exclusivement de la longueur de la dépêche. On additionnera les *chiffres* qui expriment le *nombre* des lettres qu'elle contient et du résultat de cette addition dépendront les lettres initiales. Ici, la dépêche contient 106 lettres $1 + 0 + 6 = 7$ et les deux clefs commencent par la *septième* lettre devenant ainsi :

Clef des tableaux

IQKJHGFDCAMNOSTVXYZREPUBL

Clef des alphabets

PHOUGSBFTLDVICXQAYZRKMEJN

Si la dépêche contenait 235 lettres, les lettres initiales seraient les dixièmes J et U car $2 + 3 + 5 = 10$. Si la dépêche contenait 100 lettres, on devrait commencer avec les premières lettres des deux clefs, mais on doit remarquer que ces

deux lettres sont identiques et qu'il semble en résulter une impossibilité, car pour chiffrer la *première* lettre du texte clair, il n'existe pas dans le tableau R (p. 153) d'alphabet dont la lettre initiale soit R. Dans ce cas, on remontera simplement la clef verticale d'un cran et on débutera par la *deuxième* lettre; on choisira donc dans le tableau R, d'abord l'alphabet K, puis les alphabets successifs M, E, J.

Cette remarque nous amène à chercher si dans le courant du chiffrement, nous ne rencontrerons pas de difficultés analogues. Pour le voir, chiffrons la dépêche donnée p. 127.

105. Traduction de la dépêche. — Le texte chiffré de la dépêche est :

QRXYQ OFBRR NTZJD AJGCP BRIIF
RJEQN PZFNO PUPVR EATLZ XGHYV
UVPTH IGQUF RINZE MODCG JGVDJ
JFYDK DFLVE BHBTO XFBDG VXQCC
XIDYU K

La septième lettre de la deuxième ligne et la sixième de la cinquième ligne sont soulignées. Au cours du chiffrement, la présentation de la bandelette indiquait l'alphabet G dans le tableau G. Cet alphabet n'existant pas, on a fait remonter la bandelette d'un cran et remplacé

l'alphabet G par le suivant S. A la colonne suivante, l'alphabet F devrait être choisi dans le tableau F ; en remontant la bandelette, l'alphabet T lui a été substitué.

On a, bien entendu, chiffré par colonnes verticales, c'est-à-dire en se servant d'un même tableau pour tous les alphabets qu'il doit fournir, et pointant à mesure sur la bandelette les lettres employées de façon à supprimer tout tâtonnement dans la suite des présentations.

106. Observations. — Le cas s'est donc présenté deux fois dans cette dépêche d'être obligé de substituer un alphabet à l'alphabet régulièrement indiqué. Ces rencontres dépendent de deux éléments variables, la longueur de la clef et la longueur de la dépêche. Si l'ennemi connaît celle-ci, il ignore la première et ne pourra que difficilement faire des conjectures sur le nombre et l'emplacement de ces rencontres. C'est un élément de sécurité, par conséquent, et c'est à lui que nous faisions allusion dans les pages précédentes (§ **103**). Le résultat est de rompre la trop grande régularité de présentation des alphabets.

CHAPITRE IV

—

QUALITÉS ATTRIBUÉES A LA MÉTHODE

107. Absence de difficultés pratiques. — Nous nous sommes efforcé dans l'application de la méthode, de satisfaire à toutes les conditions que nous avions successivement posées, au point de vue de l'indéchiffrabilité, dans les différents chapitres de cet ouvrage ; le système employé connu de tous dans tous ses détails, les dépêches écrites avec la même clef, ne commençant pas par les mêmes alphabets, enfin le chiffrement de 600 lettres consécutives avec 600 alphabets tous différents, etc. Nous estimons que malgré cela, la pratique ordinaire de la méthode n'en est pas rendue plus difficile ; tous

les détails du chiffrement sont familiers à ceux qui ont eu à s'occuper de dépêches chiffrées, et après expérience faite, le temps nécessaire pour traduire une dépêche est celui que demanderait l'emploi de tout tableau carré.

108. Qualités d'indéchiffrabilité. — Nous avons la prétention que la méthode exposée donne des dépêches indéchiffrables :

1° lorsqu'on ne sait rien du contenu de la dépêche à étudier,

et même : 2° lorsqu'on connaît un mot du texte clair.

En outre si l'on a en sa possession la traduction en clair d'une dépêche chiffrée, pour obtenir l'ordre successif des tableaux employés, c'est-à-dire la clef, il faudra un travail considérable, si même on peut y parvenir, ce que nous considérons comme douteux. A ce point de vue spécial le cryptographe à 120 rondelles dont il est parlé plus haut, serait même supérieur. Dans la méthode des 600 alphabets, il a fallu pour la pratique, grouper ces alphabets par tableaux et choisir pour lettre chiffre la voisine de la lettre en clair. Le cryptographe, quoique ayant un moins grand nombre d'alphabets, pourrait en opérer un mélange plus intime ; d'ailleurs pour

un même texte clair, il fournirait vingt-quatre textes chiffrés différents. Enfin le grand nombre de rondelles, faisant apparaître simultanément vingt ou vingt-cinq mots du texte clair, permettrait au chiffreur d'annuler un certain nombre de rondelles, sans en prévenir explicitement son correspondant, que la traduction même du texte avertirait suffisamment.

De cette façon l'ennemi possédant la traduction d'une dépêche chiffrée (cas fréquent en diplomatie, se rapporter aux pages qui précèdent), ne pourrait savoir combien de rondelles ont été annulées ; donc quelque longue que soit la dépêche interceptée, aucune hypothèse ne pourrait être faite sur les lettres chiffrées avec le même alphabet, c'est-à-dire la même rondelle ; et la traduction de la dépêche ne livrerait aucunement le secret de la clef.

CHAPITRE V

TABLEAUX DES ALPHABETS

109. Tableaux de A à Z. — On trouvera dans les pages suivantes les alphabets annoncés à la page 121 et dont le mode de formation a déjà été indiqué en détail. Les cinq premiers tableaux désignés par ABCDE renferment les 120 alphabets provenant de l'alphabet souche n° 1 ; les cinq suivants dans l'ordre alphabétique proviennent de l'alphabet souche n° 2 et ainsi de suite. Chaque tableau présente 24 alphabets qu'on distinguera par la lettre initiale. Dans le tableau A, il n'y a pas d'alphabet commençant par A, en général dans le tableau N, il n'y a pas d'alphabet dont la lettre initiale soit N ; cette remarque a déjà été faite et a trouvé son application pages 129 et suivantes.

A

Bcdefg	hijkl	mnopq	rstuv	xyzab
Cegikm	oqsux	zbdfh	jlnpr	tvyac
Dgjmps	vzcfi	loruy	behkn	qtxad
Eimquz	dhlpt	ycgko	sxbfj	nrvae
Fkpubg	lqvch	mrxdi	nsyej	otzaf
Gmszfl	ryekq	xdjpv	cioub	hntag
Hovdkr	zgnuc	jqyfm	tbipx	elsah
Iqzhpy	goxfn	vemud	ltcks	bjrai
Jsclue	nxgpz	irbkt	dmvfo	yhqaj
Kugqcm	xiseo	zfpbl	vhrdn	yjtak
Lxitfq	cnzkv	hscpb	myjug	rdoal
Mzlykx	jviuh	tgsfr	eqdpc	obnam
Nbocpd	qerfs	gthui	vjxky	lzman
Odrguj	ymbpe	shvkz	ncqft	ixlao
Pfzoes	ixmcq	gukat	jyndr	hvlbp
Qhyofv	mdtkb	rizpg	xneul	csjaq
Rjbskc	tldum	evnfx	ogyph	zqiar
Slexpi	btmfy	qjcun	gzrkd	vohas
Tnhbuo	icvpj	dxqke	yrlfz	smgat
Upkfaz	tojey	snidx	rmhcv	qlgbu
Vrnjfb	xsokg	cytpl	hdzuq	mieav
Xtqnkh	ebyur	olifc	zvspm	jgdax
Yvtrpn	ljhfd	bzxus	qomki	gecay
Zyxvut	srqpo	nmlkj	ihgfe	dcbaz

B

Ayxvuz	rqpts	lkonm	fjihg	edcba
Cdeghi	jfmno	klstp	qrzuv	xyabc
Dgifnk	sprux	acehj	moltq	zvybd
Eimktr	vadhf	osquy	cgjnl	pzxbe
Fpajty	isxhl	vgkue	ozdnr	cmqbf
Gfkpua	ejotz	ydins	rxchm	lqvbg
Hntuci	opvaj	kqxef	lryag	mszbh
Ikraho	qygnp	xemtv	dfsuc	jlzbi
Jsvenq	ailud	mpyhk	zcftx	gorbj
Kaoynx	mvfuj	zirhq	gpetd	sclbk
Lcsdte	pgqhr	izjuf	vmxny	oakbl
Mrdoug	lxita	fqcnz	ekvhs	yjpbm
Nuipdk	xfram	zhtco	vjqel	ygsbn
Oxfzhp	dlanv	jrgte	kymui	qesbo
Pjyshv	keznc	qfati	xlguo	drmbp
Qmcrnd	zoeuk	gvlhx	siytj	apfbq
Rogxtf	czkhy	pmdul	iaqne	vsjbr
Seqium	ykctg	rjvna	ldphz	fxobs
Thzmar	fxkdp	iunbs	gyleq	jvoct
Utnhbz	smgay	rlfex	qkjdv	poicu
Vqlmhc	xrsni	dyzto	jeaup	kfgbv
Xzplnj	gcyuq	sofhd	avrtk	miebx
Yvzqtl	omjhe	caxur	psknf	igdby
Zljcus	fdvtm	expng	yqoha	rkibz

C

Avzpsq	mkgjh	dbxuy	trnlo	fieca
Baxvuz	yptsr	qnmlk	ogfji	hedcb
Dehijf	goklm	nqrst	pyzuv	xabcd
Eifoln	rtyux	bdhjg	kmqsp	zvace
Fnybjm	pailt	xhksv	eorud	gqzcf
Grvhlp	bfque	ktajn	zdosx	imycg
Hfknsy	vbcjo	mrpua	diglq	tzxch
Iontub	hgmsz	aeflr	yxdjk	qpvci
Jlsudf	mtveg	npxah	oqybi	krzcj
Kyemui	qxfsb	opdlz	hnvjr	agtck
Luften	xhqbk	zjsdm	vgpao	yircl
Mxozjt	eqblv	gyisd	nakuf	phrcm
Nbmalx	kvoug	zfyjp	ithse	rdqcn
Otbgsa	frxjq	vinuh	mzely	dkpco
Pkdyle	zmhun	ivqjx	rfasg	btocp
Qdresh	tipjy	fzguo	vkxla	mbncq
Rhpfuk	andsi	ygvlb	qetjz	oxmcr
Sjzkbq	hxnet	fulcr	iyoap	gvmds
Tgarjv	nhzld	pobsf	xqium	eykct
Usljcz	rkiby	qohax	pngcv	tmfdu
Vpqkjd	xyrlf	eazsm	ghbut	noicv
Xztqlg	idaup	rmojc	bvysn	kfhcx
Ymixso	dznja	tkcuq	fbplh	vrgcy
Zqgdur	oevsk	hxtli	apmjb	ynfcz

D.

Azspol	febux	qkmgi	cvyrt	nhjda
Bvzxrp	knlgj	ecauy	sqtom	hfidb
Cbavuz	yxsrq	ptkon	mlhgf	jiedc
Eijfgh	lmnok	tpqrs	xyzuv	abcde
Fmtsuc	jlkrz	bihoq	yaegn	pxvdf
Gorueh	ksvai	ltxbj	mpycf	nqzdg
Htycgk	xbfos	ajnrv	imque	lpzdh
Ifhmot	qsyua	cejgl	nkprx	zvbdi
Jhntry	vcigm	kqxub	eflop	szadj
Kamzgs	ipcov	lyfre	tbnuh	xjqdk
Lqvjox	chpui	nshgt	zemra	fkydl
Msclrb	hqagp	vftuj	kzioy	enxdm
Nyikuf	pahrc	mxeoz	jtvgq	blsdn
Ouhsal	xjpcn	zgrek	vitbm	yfqdo
Peqirj	sfxgy	hzlum	vnaob	kctdp
Qjxhun	bterf	ylvoo	pisgz	makdq
Rgzncp	jxlas	huodq	fymbt	ivker
Slbqgv	tjzoe	xmcrh	apfuk	iynds
Tckboa	nvmul	zhygx	fsjri	qepdt
Urogdz	qnfcg	pmjbx	tliav	skheu
Vxpnge	ayqoh	ibzrk	ljcus	tmfdv
Xneyoi	zkjut	fvpga	qhbrl	csmdx
Ykfarm	eztgb	sniup	hcxoj	vqldy
Xpleuq	mivrn	jasof	bxkjc	ythdz

E

Axtlij	bypmn	fczqr	ogduv	skhea
Bzvtmo	hjcux	prkid	fayqs	lngeb
Cazxqt	rloig	jdbuy	vpsmk	nhfec
Dcbauz	yxvqp	tsrml	konih	gfjed
Fhnkms	pvyub	djgio	lrtqx	zacef
Gnlsqy	adfik	rpxuc	jhomt	vzbeg
Hksvud	gorqz	cfnmp	ybjil	txaeh
Imquaj	nrvbf	osxcg	ktydh	lpzei
Jfghin	oklmr	stpqv	xyzua	bcdej
Kvdoqc	npbit	ahsug	rzfmi	jlxek
Lyfruh	tbnqd	kxjmz	gsaip	covel
Mujrbo	xgtdl	ziqan	vfsck	yhpem
Nsydir	xchmv	bglqa	fkpuj	otzen
Opagmx	dntuf	lvcis	zjkqb	hryeo
Pgxnul	csjqh	yoamd	tfviz	kbrep
Qizldt	gxobr	jumep	hykcs	fvnaq
Rbkziv	ftdma	oyhqj	sclun	xgper
Sdrcmb	lakuo	znyix	hvgqf	pjtes
Tjpfqg	vhxiy	nzouk	albmc	rdset
Uqmiez	plhdy	tkgcx	sofbv	rnjau
Vocpia	sgzmj	xkdqn	bthur	fylev
Xljymf	zrgus	hatib	pncqo	dvkex
Yrlibqk	jzsic	vlfut	ndxmq	apoey
Ztojup	kfaql	gbvmh	cxrid	ysnez

F

Axhcmr	dnsyi	tzjeo	gblqv	kpufa
Bicken	altmp	osxqz	rugyh	vjdfb
Cntoqu	hdiel	pxryj	bkams	zgvfc
Djvhyg	urzqx	sopmt	lanek	cibfd
Emsujb	ntxga	oqyfc	lpzhd	krvie
Gsabyx	lihqt	cvzmk	jrped	uonfg
Hrsteb	vuxmn	ijgqp	acdyz	olkfh
Iknlmo	xzuyv	dbcea	tpsqr	ghjfi
Jhgrqs	ptaec	bdvyu	zxoml	nkifj
Klozyd	capqg	jinmx	uvbet	srhfk
Lzdaqj	nxves	hkoyc	pgimu	btrfl
Myeqio	vargk	xdthn	zbpjl	ucsfm
Noudep	rjkmz	vctqh	ilxyb	asgfn
Odsjmv	thlya	gnuer	kzcqi	xbsfo
Pvlgez	isdmh	aukqb	ojtyn	rcxfp
Qeymfs	culjp	bznht	dxkgr	avoiq
Rtbumi	gpcyo	khsev	xnjqa	dzlfr
Sbxiqc	zkreu	ngayl	htvmj	pdofs
Tuipyk	svnqd	lrbmg	cohex	jazft
Upkvql	bgoej	ztiys	ndrmc	hxafu
Vgzsma	kbjyr	xplei	dhuqo	tncfv
Xcrnyt	jobqk	uahmd	sizeg	lvpfx
Yqoagx	tnbju	smeiv	rkdhz	plcfy
Zajxeh	ocgmb	rldqn	vskyp	iutfz

G

Axitbk	hdzlp	cnjqu	msevf	ryoga
Blsyia	ktzjc	mqvgd	npufe	orxhb
Copylr	zfdvh	eksbm	tuiqx	jangc
Duohqy	kjrbn	ftcvi	pexls	azmgd
Enhavj	dxfqz	irult	ympbo	sckge
Fmnzba	rsjlk	xyeqp	hiovu	cdtgf
Hjfilm	oknvx	zuybc	eadqr	tpsgh
Ikzcqs	foxbd	pjmvg	athln	uergi
Jimkvz	ycaqt	shflo	nxube	drpgj
Kcsobp	mytlu	rizqf	xdjva	hnegk
Lvbqhm	xcrjo	zetfk	uapin	ydsgl
Mzaslx	epivc	tfnbr	jkyqh	oudgm
Najxqi	utmbs	kehvd	fzrly	pocgn
Oyrfve	smuqj	ncplz	dhkbt	ixago
Prdebu	xnolf	hstqa	cyzvk	mijgp
Qbvlgs	dynip	aukft	ezojr	cxmhq
Reunlh	tayvm	jpdbx	ofsqc	zkigr
Sptrqd	aecby	uzxvn	komli	fjhgs
Tdcuvo	ihpqe	yxklj	srabz	nmfgt
Uhyjbf	ciela	mdoqk	rntvp	xszgu
Vqmcjz	tkaiy	slbhx	rocfu	pndgv
Xtkdlc	jusvr	oaibh	zpnqm	efygx
Yfemqn	pzhbi	aorvs	ujcld	ktxgy
Zsxpvt	nrkqo	dmale	icfbj	yhugz

H

Aickqz	pvjdm	enrug	xfbos	ltyha
Bnpaor	visuj	clgdk	txmqy	fezhb
Czjeuf	syiqv	mrxot	akpdn	gblhc
Doszge	ltvfb	kquha	mpxic	nryjd
Eymtdl	jsvop	bzfqx	kgcui	ranhe
Fmkluv	abeqt	gjion	zyxdc	srphf
Gptrqs	ecbda	xvyuz	lnkom	ifjhg
Ikzvde	rgfol	yacqp	jmnux	hsthi
Jfimok	nlzuy	vxadb	cesqr	tpghj
Kvegoy	cpmub	tizdr	flaqj	nxshk
Lbgndp	katox	rmvqi	ysfue	jzcll
Mlvbqg	inyds	pfkua	etjoz	xcrhm
Nariuc	gkxqf	zbpov	sjldt	myehn
Oudqjk	ybrfn	vctil	xepgm	zasho
Prscdx	yznoi	jgtqe	bavul	kmfhp
Qduohs	azmgp	exlit	cvnfr	bykjq
Rcxzoj	teauk	fpsdy	nigqb	vlmhr
Sxnjqa	lfrdz	itbum	pcyog	cvkhs
Tsbxun	mjpqc	aylof	gredv	zkiht
Uqkbfv	tlegz	sodjy	rncix	pmahu
Vgyput	zrlqn	skeoc	mbidf	ajxhv
Xjafdi	bmcoe	ksnql	rztup	ygvhx
Ytlsob	fxgur	nemdj	vpzqk	ciahy
Zefyqm	xtkdg	lcjus	ivroa	pnbhz

I

Afejzh	xgvqy	supkt	ormcl	bndia
Bmtuqx	janco	pygzf	dlrks	vheib
Cksxfd	mtyhe	nqzib	opvja	lrugc
Dnblcm	rotkp	usyqv	gxhzj	efaid
Ehvskr	ldfzg	ypocn	ajxqu	tmbie
Fjhgqs	ptrcb	daezx	vyuko	mlnif
Gtdxkn	hpbzu	ljsce	ymfqr	avoig
Hsrdzy	onjqt	bevkl	fgpca	xumih
Jgstcd	exykm	nfhqp	rbazv	uolij
Kzcqgn	uerhl	yatjm	ydpfo	xbsik
Louvza	brpqh	fnmky	xedct	sgjil
Muxacp	gflkv	ebtpj	noyzd	rshim
Nlmoku	yvxze	adbcr	tpsqg	hjfin
Ovarqf	myecs	jluzb	phnkx	dtgio
Peohcv	nsakj	rxlqd	uftzm	gbyip
Qczkis	bxofp	dvmjt	aylhr	eungq
Ryjbkg	amszn	tvfcu	hdoqe	lpxir
Sdynqb	vlgcx	mhrzo	jtekf	pauis
Txnpzl	semqa	ogdkh	bujcy	frvit
Uapfke	tjozr	hmxcg	lvbqn	ydsiu
Vrfycj	ubhkd	goaqm	eslzp	nxtiv
Xpleqo	dhucf	vtnzs	magkb	jyrix
Ybgmzt	fudql	xrjka	snvch	oepiy
Zqnehy	tmdfx	skcgu	rlajv	pobiz

J

Ansvhc	otuid	lqxje	kpygb	mrzfa
Bvfpxi	szoqu	krcnt	elgam	hdyjb
Cfeiao	dkbnp	lsmqy	rvtxg	zhujc
Dmgenr	uosxf	byhal	tckqz	ipvjd
Eoblqv	gufak	pmrxh	cidns	ytzje
Fioknl	myvxz	ucead	bpsqr	tgbjf
Grsbac	zvmno	fhtqp	deuxy	lkijg
Hgtrqs	pbdae	cuzxv	ymlnk	oifjh
Iklyxu	edpqt	hfonm	vzcab	srgji
Kyudqh	omzas	jilxe	ptfnv	cbrjk
Luphnz	bgkxd	tovar	iyeqf	mcsjl
Meroxb	hlcqi	vdgnu	sfyat	kzpjm
Nxaqfl	zdrim	ubtgo	ycphk	vesjn
Olvuap	rhiny	zebqg	fkmxc	dstjo
Pzktay	fsung	dviqc	lhbxo	remjp
Qaxnjs	evkhp	cyogt	bumir	dzlfq
Rbcvnf	tpexl	igsaz	mohqd	uykjr
Scmfqe	yirav	otdxk	gbznh	puljs
Tsdcxm	kfgqb	ezyni	hrpau	vlojt
Uhzgxt	vtyqm	slpnb	kdoai	efcju
Vpizqk	ctlah	ybfxs	ourne	gmdjv
Xqldiu	tochv	snafz	rmbgy	pkejx
Ydmhag	letnc	rkuqo	zsixp	fvbjy
Ztysnd	ichxr	mpkaf	ugvql	boejz

K

Afpuch	rxmjt	zoesy	ndivl	bgqka
Biyojr	uagvn	etxcf	qldsz	mhpkb
Cjsvka	htylb	frznd	gpxoe	iqumc
Dtubsx	aizcg	ymfvo	hqnjp	lerkd
Epnhvm	gzasu	drljq	ofyci	xbtke
Fuhxjz	eydvb	qapcr	mtosn	ilgkf
Glinso	tmrcp	aqbvd	yezjx	hufkg
Hzdqct	ngujy	bmpsl	fxeva	roikh
Iorave	xflsm	pbyju	gntcq	dzhki
Jvatlf	zdpoi	ucskh	ybrng	xeqmj
Lnomca	bdcjh	fgist	rpqvy	zxukt
Mdftvu	oblhsq	xnaji	pzlce	grykm
Nmadjf	itpvz	ulocb	chgsr	qyxku
Oaefsp	yuncd	hirvx	lmbjg	tqzko
Phmzsd	lqfex	tenvg	aurjo	yibkp
Qghlvi	dnyse	oztjm	xrhcu	pfakq
Relpjn	qhovf	mygcz	iaxsb	utdkr
Scuiop	dzflt	avjmq	exgnr	byhks
Tbxicy	foqjl	rdusa	zgmvh	npekt
Uxzyvq	prtsi	gfhje	dbacm	onlku
Vsjcmu	qieox	pgdnz	rfhly	thakv
Xyqrsg	hebco	luzvp	tifjd	amnkx
Yrgecl	zpija	nxqsh	bouvt	fdmky
Zqtgjb	mlxvr	ihden	uypsf	eaokz

L

Ahtkcj	sveiq	umgpx	odrzn	bfyla
Brxmis	kafzo	gqvch	yndpu	ejtlb
Cipzla	jqxnb	hsuod	ftvme	gryke
Dqkbpv	arucf	xehzm	jyoit	ngsld
Edhqzk	mbjpy	voair	tuncg	fsxle
Fnropm	qesct	aybzd	xguiv	jkhlf
Gtojze	fuapk	dsniy	mhxcr	vbqlg
Ilkjviu	gxdzb	yatcs	eqmpo	rnflh
Izaqnh	udtmg	ycplj	xbsof	verki
Judyeq	ofkix	btepn	hvgza	smrlj
Kvuxzy	tsqpr	fhjig	dbace	monlk
Maghpt	xkocd	jrszv	nebif	qyulm
Nomeca	bdgij	hfrpq	styzx	uvkln
Oeadih	rqtzu	knmcb	gjfps	yxvlo
Pcygmt	duhnq	azikr	evfos	bxjlp
Qbvrcx	hmyin	sdkpa	ufezj	otglq
Rmsazg	vhnpe	tbxik	foqcy	dujlr
Sgntio	yjmzh	exfcu	ravpb	kqdls
Tjeupd	nyhev	qgozf	aksim	xrblt
Uyqfib	envzs	rjdco	kxtph	gamlu
Vxyspf	jgbcm	nkuzt	qrhid	aeolv
Xsfgcn	utria	ovypj	bmkzq	hdelx
Yfbnzr	doxpg	muqie	vsjck	thaly
Zpicky	rgemv	tfdou	shbnx	qjalz

M

Abdecf	gijhp	qstru	vyzxk	lnoma
Befihq	tuyxl	oadeg	jpsrv	zknmb
Chrxma	fpukb	gqvld	isyne	jtzoc
Dfjqry	kobci	ptvxn	aeghs	uzlmd
Eiquxo	dgprz	nbfht	ylacj	svkme
Fqyocp	vnchu	ldjrk	bitxa	gszmf
Gtkdhv	ofsxb	juncq	zairl	epymg
Hxapkg	vdsnj	zermf	ubqli	yetoh
Iuogrn	ftlcs	keqxd	pzbhy	ajvmi
Jybpxe	slfro	ivahz	dqkct	ngumj
Kvsjca	lythf	bnzrp	gdoxu	qoemk
Lzushg	eanxv	tpicb	okyrq	jfdml
Nkzvrs	pjgcd	aolxy	utqhi	febmn
Onlkxz	yvurt	sqphj	igfce	dbamo
Plizcu	bsohk	gyera	qnjxf	vdtmp
Qopnhl	jkixg	zfycv	eudrb	tasmq
Rczjns	dvgkp	axhot	eyilq	bufmr
Satbrd	uevcy	fzgxi	kjlhn	poqms
Tdvfxj	nqare	ygkho	sbacz	ilpmt
Ugntck	qdzha	viorf	lsexp	byjmu
Vjayhb	zpdxq	ekscl	tfnrg	ouimv
Xrhcoz	tjeny	sidlv	qgbku	pfamx
Ypelri	azqcn	ujbxs	forhd	ktgmy
Zsgaxt	ibkrj	dluhe	uvpco	yqfmz

N

Ajglci	pkegr	ydftv	mhsuo	bqxna
Bsvdgp	laqum	frkcj	xohty	eiznb
Cgtuna	irvob	jpymd	hqzke	fsxlc
Dafjtz	vlmch	ispuk	oebgq	rxynd
Ehjrul	dbitx	kmags	zyocf	qpvne
Fzmiue	qyatl	hpogx	djvcs	kbrnf
Guaroj	ydqkf	xctni	vbpmh	zeslg
Hrlbtk	asycq	vejud	ixmgz	ofpnh
Iyhxcr	mqlgv	bzeto	jkfua	pdsni
Jlikgy	fvhub	xazcp	erdtm	soqnj
Kvxptq	ifbcd	olyuz	rsjgh	aemnk
Lkyvux	zprts	qjigf	hbace	dmonl
Mealigj	srzuy	lodcb	fiqtp	xvknm
Omdeca	blifgi	jqstr	pzxuv	yklno
Pfozgm	xiduj	evqcy	saktb	lrhnp
Qosmtd	repcz	axbuh	vfygk	iljnq
Rbkscv	jdxgo	plilta	yqeui	mzfnr
Sdpauf	kjote	zbvgl	qmrcx	hyins
Texfkq	dyjor	augls	ezhmp	bvint
Utgclx	sfekz	qhdmy	pjbov	rianu
Vpqfco	yzsga	mkxti	bdlur	jhenv
Xqbous	hmvtf	dyrge	kpicl	zjanx
Yxrqgb	eokup	sihcm	lvztj	fadny
Zieyth	oxjck	rfmuq	alpgd	vsbnz

O

Atuncg	xlefs	kdlhqz	bjpym	irvoa
Beajft	psuyk	nmdci	hgrqx	vzlob
Cfqyoa	gszmb	itxkd	jrule	hpvnc
Dahtqu	znbcj	gpxyl	meifr	svkod
Ejtsyn	digqv	lbafp	ukmch	rxzoe
Fyasmi	xdrlh	vcqog	zbtkj	uepnf
Gkjvcs	brnfz	iueqm	tlhya	xpdog
Hubgye	rkaqn	jxmfv	dtzcp	lisoh
Ipzdfx	naryb	hslct	vmjqk	eguoi
Jsniql	apkcr	zetyd	gvbfu	mhxoj
Kvsrfi	emlyx	pgjcb	nzuqt	hadok
Lzvxqr	ghicd	mnkyu	sptfj	aebol
Mbdeca	ijhfg	trpqs	xuvyz	klnom
Nlkzyv	uxsqp	rtgfh	jiace	dbmon
Pdxayh	ltmqe	uizfn	rbscv	jkgop
Qcvhlr	dxims	ayfnp	eujkt	bzgoq
Rmpbqd	sexcu	aviyj	zhkfl	gntor
Silpcz	tdvfm	xjnqa	kreyg	buhos
Tnglfk	hzjyi	vaucx	esdqb	pmrot
Ugekqj	mvtcl	shbyr	anxfd	zpiou
Vrimyp	jbzqh	dksfe	lxgcn	utaov
Xhmufb	vgdyt	czrck	palqi	nsjox
Yqfcnv	phelu	rjdkx	tibmz	sgaoy
Zxrhcm	kupfa	blvqg	idnys	tjeoz

P

Adiyns	rchxm	otcjz	vlqbg	fukpa
Bjxnqe	hyktc	iulrd	fvosa	gzmpb
Czkrju	sefnt	gyobi	mqdxl	ahvpc
Dyscxo	ezlbf	kainr	hmtjv	qgupd
Eivsbh	uoajy	lrgxk	tdznq	cfmpe
Fqzfxr	ẏaubv	emcnd	kgljo	hsipf
Gvthna	flcxs	duqjm	rikbz	ocypg
Illdmby	tfsjk	cvaxq	iogne	urzph
Ishojl	gkdnc	mevbu	ayrxt	zqfpi
Jneyti	ldvsg	mbxqh	kcurf	oazpj
Kufgbq	lvzjc	tomxh	crsny	idapk
Lmgfjc	aqonu	zhdbt	skvxi	gerpl
Mfcqnz	dtkxg	rlyja	ouhbs	viepm
Nxjbpm	zgaso	vfdrl	uictk	yheqn
Okmuxf	hgcbr	qslnv	yzijd	eatpo
Qtrabe	cdgjh	ifzxy	uvmnk	lospq
Regixv	kstbd	hzuno	qacjf	ymlpr
Solknm	vuyxz	fihjg	dceba	rtqps
Taedji	zyvnl	sqrbc	ghfxu	mkopt
Ugqvjt	mhrni	akfbl	zeoxc	sydpu
Vhalxd	qmibo	ygtnf	esujr	kzcpv
Xbmgsv	dlity	enjpz	aofru	ckhqx
Ycozbk	irmjq	udsxe	lfanh	tvgpy
Zrueng	oiqxa	vckjs	ftybm	dlhpz

Q

Avkbfy	pdunr	ixscj	mthzl	egoqa
Bdijzo	kprch	gvyns	teafu	xmlqb
Cfzntd	gxkra	jylsb	huope	ivmqc
Djopcg	ysefx	lbizk	rhvnt	aumqd
Ehjxnp	bagzm	srdfv	oltci	uykqe
Fndxrj	lbupi	mcztg	kaysh	oevqf
Glhmcx	rupfk	aoezt	jsind	ybvqg
Hxpazs	dvlcu	kejnb	gmrfo	tiyqh
Iorgne	uldzp	hytfm	bjkcv	saxqi
Jpgsfl	ikhna	mdocy	exbzr	vtuqj
Kyuict	lovfd	rsmzg	abpnx	jheqk
Lmxufa	etsny	vghcr	pkozj	idbql
Muatnv	hrkzi	blxfe	sygcp	ojdqm
Nzfcqm	viepo	uhbsl	yjark	xjdtn
Ogolzh	tmjcs	xirnu	dpyfb	kvaqo
Pslknm	oyxzv	ujgfi	hadce	brtqp
Redhfj	vxonl	ptbca	iguzy	mksqr
Skmyzu	giacb	tplno	xvjfh	derqs
Trbecd	ahifg	juvzx	yomnk	lspqt
Utvrzb	xeyco	dmanh	kilfs	gpjqu
Vbydni	sjtze	oakfp	urxcm	hlgqv
Xasvck	jbmft	yhpzd	lueng	roiqx
Yitofr	mgbnj	ekucl	vdsza	pxhqy
Zcmipu	bljrx	dnfqv	eohsy	akgtz

R

Ajfzuo	stdei	vylnq	cbhgx	kmpra
Bizknt	ahvum	qdjgy	opcef	xlsrb
Cdabej	hifgv	zxyuk	lomns	pqtrc
Dbjigz	ykonp	tcaeh	fvxul	msqrd
Egunsc	jvkpd	hzlqa	ixotb	fymre
Fodvnb	xpjut	ilcgm	azsey	qhkrf
Gncvph	laxtf	meusj	kdzqi	obyrg
Hysagl	tjxnd	fkqez	mciup	bvorh
Ikthuq	jypex	sbzna	vmdgo	cflri
Jzotev	lqbgk	pafus	diync	hxmrj
Khqyes	zamgc	lituj	pxbnv	dofrk
Lfcogd	mvanz	bsxep	yjquh	tkirl
Mxhcny	idsuf	apkgb	qlvet	ozjrm
Nugerm	yfbto	xiaql	zhdpk	vjcsn
Ovbpui	cmzeq	kfdnx	jtlga	syhro
Pmkxgh	bcqnl	yvied	tsouz	fjarp
Qsmlux	vfhea	ctpno	kyzgi	jbdrq
Slxfec	poygj	dqmuv	hatnk	zibrs
Tqpsnm	olkuy	xzvgf	ihjeb	adcrt
Uemftx	alhpv	cngry	boiqz	dkjsu
Vpimck	dxtgs	hobuc	zqfnj	layrv
Xcydua	kbleo	jmhni	sfpgq	vtzrx
Yaljnf	qzcub	ohsgt	xdkem	ipvry
Ztvqgp	fsinh	mjoel	bkaud	ycxrz

S

Agzmdf	voriu	ltcyk	qehnp	hjxsa
Baktiv	majnq	cuodg	xpeyl	rfzsb
Czqfnr	jlaym	evpix	tgkdh	obusc
Diynpa	fukqb	gvlte	jzorc	hxmsd
Eumbyo	ahldj	krgnt	fxqiz	pcvse
Flexdu	qjmik	bzryp	gocna	vthsf
Gmfoil	ckenb	xazdv	rutyq	hpjsg
Htvanc	ogpyr	zbkim	jqudx	elfsh
Inauqg	lezrh	mdypf	kbvtj	ocxsi
Jphqyt	urvdz	axbne	kclio	fmgsj
Kvjcdp	lzhia	qoxyf	btmnu	gersk
Lxujib	rponv	hfedq	mkzyg	catsl
Molknx	svuyh	jgfic	ebadr	tqpsm
Nyidsm	xhcro	zjetl	vgbqk	ufapn
Okxvyj	fcbdt	pmlnz	uhgie	arqso
Pqtrda	becif	gjhyu	vzxnk	lomsp
Qracig	huznl	mptdb	cfjyv	xkosq
Regunm	tbfyx	oqaih	zlpdc	jvksr
Tacgyz	kmqde	fhvno	prbij	uxlst
Ubohdk	gtxip	vemya	ljrnf	qzcsu
Vcpziq	xftng	rkjdl	haoyb	muesv
Xjbpnh	eqkyc	tluir	ovfdm	zgasx
Ydmhrz	elgqu	anisx	cojtv	bkfpy
Zfrlye	pxgdo	ucqnj	amvit	khbsz

T

Ahvnrb	izkse	fxlpc	gyoqd	jumta
Bxoqai	lpdhz	scjvk	egunr	fymtb
Cbjxvo	kqeag	iulnp	rdfhy	zmstc
Dgxznq	cfivm	pebhu	osraj	ylktd
Edbghx	uzons	qrcaf	jiyvl	mkpte
Fukchl	qbyne	jzpax	mrgvs	diotf
Gzqfvp	busay	kdxnc	imeho	rjltg
Hnbzsf	lcyqj	mavri	kexpg	oduth
Isgmaz	eyqhk	fodvr	xpjnb	lcuti
Joeind	ysbvq	glrhm	cxkau	pfztj
Klyjar	souhb	epmvi	fcqnz	xgdtk
Ljrohe	micnx	dkyas	ubpvf	qzgtl
Myfrnu	gekvj	cszhd	pliaq	oxbtm
Nvhatm	ujdqo	ygcpl	xfesk	zibrn
Oidsvg	rmxap	zjeny	bqlhc	kufto
Pkmlvy	ijfac	rqsno	zuxhg	bdetp
Qpsknm	olzvu	yxihj	gfbad	certq
Rccdab	fgjhi	xyuvz	lomnk	spqtr
Smzyhf	drpnl	uigae	qkovx	jbcts
Uclbnj	pxrvd	ofkhq	yczam	gsitu
Vamjgy	clfsz	bnhtu	dogpx	ekirv
Xqiphs	jkgnf	mboal	dzcve	urytx
Yruevc	zdlao	bmfng	kjshp	iqxty
Zfpuak	xcmhr	lgqvb	sydni	oejtz

U

Afbgql	vnydi	shrmx	czejt	opkua
Blysmz	tkfqn	ircjp	agvdh	xeoub
Cyazdf	eibjs	gthqo	rlpmv	kxnuc
Djtlvc	fpnye	gqmxa	isozb	hrkud
Ehvajr	nftmy	boxdg	pciqk	zslue
Fglnds	rxzjo	kabqv	yihmc	etpuf
Gnsxjk	bvime	pfldr	zoaqy	hctug
Harfmb	xgcqz	levjn	tyodp	ixsuh
Ioneqx	fhkdt	vzgma	spyjl	cbrui
Jmdqug	keryh	nbpzf	ocsvi	latxj
Kpotje	zcxmr	hsidy	nvlqg	bfauk
Lszkqi	cpgdx	obymt	fnrja	vheul
Mqgeyn	pfcvl	tjduk	rhbzo	siaxm
Nxkvmp	lroqh	tgsjb	iefdz	aycun
Oexhdv	gapjc	rinqf	ktzms	ylbuo
Ptecmh	iyvqb	akojz	xrsdn	lgfup
Qdmjxt	alivs	cofzp	bnhyr	ekguq
Rbcljy	psamg	zvtdk	hfxqe	nocur
Skipdo	ytnjv	elzqc	gxbmf	rahus
Tchyqa	ozrdl	fpemi	vbkjx	sngut
Vrtbdc	klhjf	yxpqs	canmo	gizuv
Xvprqt	sbeda	cnkml	ohgji	fzyux
Yzfijg	holmk	ncade	bstqr	pvxuy
Zigomn	aesqp	xyfjb	lkcdb	trvuz

V

Ajqkyb	fslxd	grnzc	itmue	hpova
Bozsaf	xcljt	diurm	gqeny	pkhvb
Cmhxrk	fupai	ysdnz	teojq	blgvc
Dhtkjp	lycnx	efqag	smzro	ubivd
Eixbnu	coyrl	zpmjs	kgtah	qdfve
Fdqhat	gksjm	pzlry	ocunb	xievf
Glbqjo	etznd	syiap	ufkrx	hmcvg
Hkpyne	qgmru	idtjl	cxfas	zobvh
Ibuorz	msgaq	fexnc	ylpjk	thdvi
Jnarvg	odpxh	lesuf	mbtyi	kcqzj
Kyegri	tlxaz	bhpnq	mudjc	fsovk
Lqotns	ipfrh	cgbje	zdyau	kxmvl
Mxkuay	dzejb	gchrf	pisnt	oqlvm
Nrgdxl	sfbyk	qjavo	pheum	ticzn
Osfcjd	umqnp	hbzax	ltirg	eykvo
Pemjx	sbkng	utcao	hyqrd	lfzvp
Qtsprc	bedak	mloni	fhgjz	yuxvq
Ranjzq	ckiyt	bmfus	elhxp	dogvr
Scdmnh	zxtre	kofju	qpbal	igyvs
Tpceam	oihjy	xqsrb	dklnf	gzuvt
Uzgfnl	kdbrs	qxyjh	iomde	cptvu
Xuyzjg	hfino	lmkad	ebcrp	stqvx
Ygilab	pqujf	okert	xzlnm	dcsvy
Zfldrq	yhoac	tugnk	bsxji	mepvz

X

Amudky	pnzso	itljq	egrbh	vcfxa
Bjpmzd	fqouc	gskve	irlya	htnxb
Chrejt	ozpku	afvbg	qlisn	ydmxc
Dniqbf	upojr	cmysl	gvakz	tchxd
Ezagsm	roubi	dhtkv	lycjp	fqnxe
Fcvhbr	geqjl	tiosz	npykd	umaxf
Godvjn	arikc	qzmbt	yfesu	hlpxg
Hetzka	vglsy	mcrjo	pufbq	indxh
Ifocsv	zhnbp	rygkc	dqujm	latxi
Jkbsxg	nctuh	oaqyf	ldrzi	mepvj
Ksgcuo	qfdzm	pjbxn	thayl	rievk
Lueybz	ciajd	gphsf	tmqkr	nvoxl
Mdynsi	lqgbv	faukp	zotjc	rhcxm
Nqfpjc	ylvkt	hdibu	ormsg	azexn
Ovnrkq	mtfsh	pgdja	iczby	eulxo
Pihuse	fytbm	zqcki	ranjv	dogxp
Qpclkh	iursa	enfjy	vtdbo	mgzxq
Rtpabl	nmhjz	uvqsd	ccokf	giyxr
Sbkjvp	emizr	dlfyq	aohut	cngxs
Talmju	qdekg	yrpbn	hzvsc	ofixt
Uyzijg	hfmkn	olebc	adpst	qrvxu
Vrqtsp	dacbe	lonkm	fhgji	zyuxv
Yigfko	ecdsq	vuzjh	mnlba	ptrxy
Zgmobd	tvyjf	neasr	uihkl	cpqxz

Y

Akxbjs	dfrlz	tnucg	veipm	hqoya
Bftgpo	xdzci	qkslu	ehajr	nvmyb
Cjroxe	ftkza	gplub	iqnvd	hsmyc
Dumxlv	osnpk	rgqjt	iafch	bzeyd
Ezbhcf	aitjq	grkpn	sovlx	mudye
Fgodcq	suhjn	mbtpx	zikle	arvyf
Gdqujm	txila	vfocs	hnbpz	koryg
Hignld	baqpv	uzfjk	omect	rsxyh
Indapu	fkmcr	xhglb	qvzjo	etsyi
Jlcpyg	maszh	kdtvf	neqxi	obruj
Kbsflt	ugeph	oaxjd	rzncv	imqyk
Lpgazk	tfexo	rjcym	shdvn	qibul
Mvnrja	heuls	kqicz	dxapg	tfbym
Naukcx	gbvjo	sidpf	mrhlq	zotyn
Oqhmpi	evgcu	ntzlr	fdsjb	xkayo
Pcljur	boixq	enfvt	dkhzs	amgyp
Qmivcn	zrdjx	aohpe	gutlf	zbkyq
Rekzpb	nhsco	fvali	xtmju	qdgyr
Steojz	vqblg	hxrcm	kfupa	dniys
Tozqlh	rmfpd	isejv	bgxck	uanyt
Uxvspr	qtacb	edmlo	nkgjo	fhzyu
Vraelk	izxpt	bmnjh	usqcd	ogfyv
Xsrtce	mokjf	zuvpq	abdln	gihyx
Zhfijg	knolm	debca	tqrps	vxuyz

Z

Agdhef	qirjp	lsmtk	vnxou	bycza
Bxksjq	hayov	mpieg	cantl	rfdzb
Cybuox	nvktm	slpjr	iqfeh	dgazc
Dfrltn	ucgei	pmvoy	ahqjs	kxbzd
Ejsnua	frmvb	gtoyd	ipkxc	hqlze
Flncep	vyhjk	bdrtu	gimoa	qsxzf
Ghfijl	mknob	cadeq	rpstv	xuyzg
Hilkoc	dqptx	ygfjm	nbaer	svuzh
Ikcqty	fmbcs	uhlod	pxgjn	arvzi
Joetzg	lbqvh	mcrxf	kapui	ndsyj
Kqymeu	ldxja	victf	bshop	gnrzk
Lcpyjb	ruioq	xfnev	hkdtg	maszl
Mdvfor	ylath	nqujc	sgkex	ibpzm
Nphbti	axley	krgos	fcvjd	umqzn
Otgbvm	rfaun	sjezl	qhcxk	pidyo
Pbixek	gscju	qnhta	lyrof	vdmzp
Qmudjv	cfsog	rkyel	xaitb	hpnzq
Rngpoh	zbfte	ivajx	dluem	yqkzr
Samgtd	khven	fxqoi	urbjy	pclzs
Teojys	dniup	akfxr	cmhvq	blgzt
Uvsrea	bnmjf	gyxtp	qdcok	lihzu
Vranjg	xpdol	huseb	mfytq	ckizv
Xsqaom	igutr	dbkjh	yvpec	nlfzx
Yuxvts	prqed	acbon	kmlji	fhgzy

ADDENDUM

—

L'application de la méthode nouvelle exposée dans les pages précédentes a paru présenter une certaine difficulté pour les personnes, non exercées au chiffrement des dépêches. Nous avions tenu à exposer une méthode aussi irréprochable que possible en théorie; mais il est facile de présenter une pratique de la même méthode infiniment plus simple, supprimant notamment l'emploi de la bandelette mobile et même la formation des clefs littérales, formation qui suppose déjà une certaine éducation cryptographique.

C'est le mot clef lui-même qui, écrit au-dessus du texte clair et à côté de lui, nous donnera la clef des alphabets et celle des tableaux.

Supposons que ce mot clef ou plutôt cette clef se compose de deux mots : REPUBLIQUE FRANÇAISE. On disposera le texte clair en

rangées de *vingt* lettres (au lieu de vingt-cinq) et l'on écrira la clef au-dessus de la première rangée en commençant à une colonne variable suivant une convention à fixer. Parvenu au-dessus de la vingtième colonne, on descendra aux lignes suivantes, en mettant une lettre seulement à l'extrémité de chaque rangée occupée par le texte clair ; de là on reviendra à la case au-dessus de la première colonne et on continuera jusqu'à ce que l'on ait atteint la première colonne de début. La clef sera répétée autant de fois qu'il sera nécessaire. Les lettres terminant chaque rangée désigneront les tableaux où l'on cherchera les alphabets ; les initiales de ceux-ci seront les lettres surmontant chaque colonne.

Clef des alphabets :

E P U B L I R E P U B L I Q U E F R A N

L	*e*	*s*	*c*	*a*	*n*	*d*	*i*	*d*	*a*	*t*	*s*	*v*	*e*	*l*	*o*	*c*	*i*	*p*	*e*	C
d	*i*	*s*	*t*	*e*	*s*	*m*	*i*	*l*	*i*	*t*	*a*	*i*	*r*	*e*	*s*	*n*	*e*	*s*	*e*	A
s	*o*	*n*	*t*	*g*	*e*	*n*	*e*	*r*	*a*	*l*	*e*	*m*	*e*	*n*	*t*	*p*	*r*	*e*	*s*	I
e	*n*	*t*	*e*	*s*	*q*	*u*	*e*	*n*	*t*	*r*	*e*	*s*	*p*	*e*	*t*	*i*	*t*	*n*	*o*	S
m	*b*	*r*	*e*	*a*	*u*	*x*	*e*	*x*	*a*	*m*	*e*	*n*	*s*	*d*	*u*	*m*	*o*	*i*	*s*	E
d	*e*	*j*	*u*	*i*	*n*															R

Clef des tableaux

Le texte de l'exemple occupe cinq rangées entières et 6 cases de la sixième rangée. Nous avons commencé à écrire la clef à la septième

colonne, c'est-à-dire à *la colonne qui suit la dernière lettre du texte*. Telle est la convention simple à établir. Si la dernière rangée était occupée complètement par le texte, on commencerait à écrire la clef en face et à droite de la première rangée.

Alphabets :

U B L I Q U E F R A N C A I S E R E P U

. . . . . R
. . . . . (Texte de 60 lettres) . . . . . E
. . . . . P

Tableaux

Pour résumer ici en quelques mots la méthode, nous rappelons que, pour chiffrer une lettre située à l'intersection d'une rangée et d'une colonne, on cherche le groupe d'alphabets ou *tableau* désigné par la lettre de la clef inscrite en regard de la rangée ;

dans ce tableau l'*alphabet* dont l'initiale est la lettre de la clef surmontant la colonne ;

et dans cet alphabet la *lettre* à chiffrer ; son *chiffre* est celle qui la suit immédiatement.

Chaque tableau ne contient que 24 alphabets ; dans l'exemple, les lettres *e* et *m*, 46e et 53e lettres du texte ne pourront être chiffrées puisqu'il n'y a pas d'alphabet I dans le tableau I. Dans ce cas d'impossibilité, on *chiffrera la lettre par elle-même*, en l'insérant sans changement dans le

texte chiffré. On a souligné dans la dépêche les lettres 39, 46, 53, 81, 88, 96, qui se retrouveront aux mêmes places dans le texte chiffré, sans que ce mélange puisse nuire en rien à la sécurité de la méthode. Théoriquement il est même bon qu'une lettre puisse ainsi être représentée par toutes les lettres de l'alphabet au lieu des 24 autres seulement.

BIBLIOGRAPHIE

—

JACOB. — *Les secrets de nos pères, la Cryptographie*, Adolphe Delahays, éditeur. Paris, 1858.

Cet ouvrage renferme une table bibliographique des plus complètes pour tous les ouvrages parus antérieurement.

Journal des Sciences Militaires.

Articles de M. Kerckhoffs, 1883.

MAMY. — *Science et Guerre*. Etudes publiées dans le Génie Civil, 1885.

MARQUIS DE VIARIS. — *Cryptographie*. Etude publiée dans le Génie Civil, 1888.

NOTE : Des renseignements demandés aux principaux libraires de Londres, Vienne et Berlin, il résulte qu'aucun ouvrage sur les dépêches secrètes n'a paru depuis dix ans dans ces capitales.

TABLE DES MATIÈRES

—

PREMIÈRE PARTIE

NOTIONS PRÉLIMINAIRES

CHAPITRE PREMIER

Généralités

CHAPITRE II

Des clefs

CHAPITRE III

De la sécurité au point de vue du secret

DEUXIÈME PARTIE

MÉTHODES A ALPHABETS

CHAPITRE PREMIER

Généralités

CHAPITRE II

Méthodes à alphabet unique

CHAPITRE III

Méthode mixte

CHAPITRE IV

Alphabets multiples réguliers

CHAPITRE V

Alphabets multiples intervertis

TROISIÈME PARTIE

MÉTHODES A ANAGRAMME

CHAPITRE PREMIER

Méthodes sans appareil

CHAPITRE II

Méthodes avec appareils

CHAPITRE III

Du déchiffrement de ces méthodes

QUATRIÈME PARTIE

MÉTHODES A RÉPERTOIRES

CHAPITRE PREMIER

Des divers répertoires

CHAPITRE II

Du déchiffrement des dépêches chiffrées avec les répertoires

CINQUIÈME PARTIE

OBSERVATIONS ET NOTIONS GÉNÉRALES

CHAPITRE PREMIER

Observations sur l'ensemble des méthodes précédentes

CHAPITRE II

De la fréquence des lettres dans la langue française

CHAPITRE III

Renseignements sur les transmissions télégraphiques des dépêches secrètes

CHAPITRE IV

De deux méthodes à alphabets n'employant que des chiffres arabes

CHAPITRE V

Appareil du Capitaine Bazeries

CHAPITRE VI

Représentation des signes numériques et orthographiques

SIXIÈME PARTIE

MÉTHODE NOUVELLE

CHAPITRE PREMIER

Genèse de la Méthode

CHAPITRE II

Création des Alphabets

CHAPITRE III

Pratique

CHAPITRE IV

Qualités attribuées à la Méthode

CHAPITRE V

Tableaux des Alphabets

ST-AMAND (CHER). IMPRIMERIE DESTENAY, BUSSIÈRE FRÈRES

LIBRAIRIE GAUTHIER-VILLARS ET FILS
Quai des Grands-Augustins, 55.
Envoi franco *contre mandat-poste ou valeur sur Paris*

LEÇONS DE CHIMIE

(*à l'usage des Élèves de Mathématiques spéciales*)

PAR

Henri GAUTIER

Ancien élève de l'École Polytechnique,
Professeur de l'École Monge et au collège Sainte-Barbe,
Professeur agrégé à l'École de Pharmacie ;

ET

Georges CHARPY

Ancien Élève
de l'École Polytechnique, professeur à l'École Monge.

Un beau volume grand in-8, avec 83 figures ; 1892. . . 9 fr.

Ces *Leçons de Chimie* présentent ceci de particulier qu'elles ne sont pas la reproduction des Ouvrages similaires parus dans ces dernières années. Les théories générales de la Chimie sont beaucoup plus développées que dans la plupart des Livres employés dans l'enseignement ; elles sont mises au courant des idées actuelles, notamment en ce qui concerne la théorie des équilibres chimiques. Toutes ces théories, qui montrent la continuité qui existe entre les phénomènes chimiques, physiques et même mécaniques, sont exposées sous une forme facilement accessible. La question des nombres proportionnels, qui est trop souvent négligée dans les Ouvrages destinés aux candidats aux Ecoles du Gouvernement, est traitée avec tous les développements désirables. Dans tout le cours du Volume, on remarque aussi une grande préoccupation de l'exactitude, les faits cités sont tirés des mémoires originaux ou ont été soumis à une nouvelle vérification. Les procédés de l'industrie chimique sont décrits sous la forme qu'ils possèdent actuellement. L'ouvrage ne comprend que l'étude des métalloïdes, c'est-à-dire les matières exigées pour l'admission aux Écoles Polytechnique et Centrale.

En résumé, le Livre de MM. Gautier et Charpy est destiné, croyons-nous, à devenir rapidement classique.

LIBRAIRIE GAUTHIER-VILLARS ET FILS

Envoi franco *contre mandat-poste ou valeur sur Paris*

COURS
DE PHYSIQUE
DE
L'ÉCOLE POLYTECHNIQUE

PAR M. J. JAMIN

QUATRIÈME ÉDITION

AUGMENTÉE ET ENTIÈREMENT REFONDUE,

PAR

M. BOUTY,

Professeur à la Faculté des Sciences de Paris.

Quatre Tomes in-8, de plus de 4000 pages, avec 1587 figures et 14 planches sur acier, dont 2 en couleur ; 1885-1891. (OUVRAGE COMPLET) . . . . . 72 fr.

On vend séparément :

TOME I. — 9 fr.

(*) 1er fascicule. — *Instruments de mesure. Hydrostatique ;* avec 150 fig. et 1 planche . . . . . 5 fr.

2e fascicule. — *Physique moléculaire ;* avec 93 figures . . 4 fr.

TOME II. — CHALEUR. — 15 fr.

(*) 1er fascicule. — *Thermométrie. Dilatations ;* avec 98 fig . . 5 fr.

(*) 2e fascicule. — *Calorimétrie ;* avec 48 fig. et 2 planches . 5 fr.

3e fascicule. — *Thermodynamique. Propagation de la chaleur ;* avec 47 figures . . . . . 5 fr.

TOME III. — ACOUSTIQUE ; OPTIQUE. — 22 fr.

1er fascicule. — *Acoustique ;* avec 123 figures. . . . . 4 fr.

(*) 2e fascicule. — *Optique géométrique ;* avec 139 figures et 3 planches. . . . . 4 fr.

3e fascicule. — *Étude des radiations lumineuses, chimiques et calorifiques ; Optique physique ;* avec 249 fig. et 5 planches, dont 2 planches de spectres en couleur . . . . . 14 fr.

(*) Les matières du programme d'admission à l'École Polytechnique sont comprises dans les parties suivantes de l'Ouvrage : Tome I, 1er fascicule ; Tome II, 1er et 2e fascicules ; Tome III, 2e fascicule.

LIBRAIRIE GAUTHIER-VILLARS ET FILS
Envoi franco *contre mandat-poste ou valeur sur Paris*

BIBLIOTHÈQUE

PHOTOGRAPHIQUE

La Bibliothèque photographique se compose d'environ 150 volumes et embrasse l'ensemble de la Photographie considérée au point de vue de la science, de l'art et des applications pratiques.

A côté d'ouvrages d'une certaine étendue, comme le *traité* de M. Davanne, le *Traité encyclopédique* de M. Fabre, le *Dictionnaire de Chimie Photographique* de M. Fourtier, etc., elle comprend une série de monographies nécessaires à celui qui veut étudier à fond un procédé et apprendre les tours de main indispensables pour le mettre en pratique. Elle s'adresse donc aussi bien à l'amateur qu'au professionnel, au savant qu'au praticien.

EXTRAIT DU CATALOGUE.

Davanne. — *La Photographie. Traité théorique et pratique.* 2 beaux volumes grand in-8, avec 234 figures et 4 planches spécimens. **32 fr.**

On vend séparément :

Ire Partie : Notions élémentaires. — Historique. — Épreuves négatives. — Principes communs à tous les procédés négatifs. — Epreuves sur albumine, sur collodion, sur gélatinobromure d'argent, sur pellicules, sur papier. Avec 2 planches et 120 figures ; 1886 . . 16 fr.

IIe Partie : Épreuves positives : aux sels d'argent, de platine, de fer, de chrome. — Epreuves par impressions photomécaniques. — Divers : Les couleurs en Photographie. Épreuves stéréoscopiques. Projections, agrandissements, micrographie. Réductions, épreuves microscopiques. Notions élémentaires de Chimie ; vocabulaire. Avec 2 planches et 114 figures ; 1888 . . . . . 16 fr.

Donnadieu (A. L.) Docteur ès sciences. *Traité de Photographie stéréoscopique. Théorie et pratique.* — Grand in-8 avec figures et atlas de 20 planches stéréoscopiques en photocollographie ; 1892.. . 9 fr.

Fabre (C.), Docteur ès sciences. — *Traité encyclopédique de Photographie.* 4 beaux volumes, gr. in-8, avec plus de 700 figures et 2 planches ; 1889-1891 . . . . . 48 fr. »»

Chaque volume se vend séparément 14 fr.

Tous les trois ans, un Supplément, destiné à exposer les progrès accomplis pendant cette période, viendra compléter ce Traité et le maintenir au courant des dernières découvertes.

Premier Supplément triennal (A). Un beau volume grand in-8 de 400 pages, avec 176 figures ; 1892. . . . . 14 fr.

Fourtier (H.). — *Dictionnaire pratique de Chimie photographique*, contenant une *Étude méthodique des divers corps usités en Photographie*, précédé de *Notions usuelles de Chimie* et suivi d'une Description détaillée des *Manipulations photographiques*. Grand in-8, avec figures; 1892 . . . . . 8 fr. »»

— *Les Positifs sur verre. Théorie et pratique. Les positifs pour projections. Stéréoscopes et vitraux. Méthodes opératoires. Coloriage et montage.* Grand in-8, avec figures; 1892 . . . . . 4 fr. 50

— *La pratique des projections.* Etude méthodique des appareils. Les accessoires; usages et applications diverses des projections. Conduite des séances. 2 volumes in-18 jésus se vendant séparément.

I. *Les appareils*, avec 66 figures; 1892;. . . . . 2 fr. 75

II. *La séance de projections*, avec figures ... (*Sous presse*).

— *Les tableaux de projections mouvementés. Étude des tableaux mouvementés, leur confection par les méthodes photographiques. Montage des mécanismes.* In-18 jésus, avec figures; 1893 . . . . . 2 fr. 50

Fourtier (H.), Bourgeois et Bucquet. — *Le formulaire classeur du Photo-club de Paris.* Collection de formules sur fiches, renfermées dans un élégant cartonnage et classées en trois Parties : *Phototypes, Photocopies et Photocalques. Notes et renseignements divers*, divisées chacune en plusieurs Sections.

Première série; 1892. . . . . 4 fr.

Londe (A.), Chef du service photographique à la Salpêtrière. — *La Photographie instantanée.* 2e édition. In-18 jésus, avec belles figures; 1890 . . . . . 2 fr. 75

— *Traité pratique du développement.* Étude raisonnée des divers révélateurs et de leur mode d'emploi. 2e édition. In-18 jésus, avec figures et 4 doubles planches en photocollographie; 1892 . 2 fr. 75

— *La photographie médicale. Applications aux sciences médicales et physiologiques.* Grand in-8, avec 80 figures et 19 planches; 1893 9 fr.

Marco Mendoza, membre de la société française de photographie. — *La Photographie la nuit.* Traité pratique des opérations photographiques que l'on peut faire à la lumière artificielle. In-18 jésus, avec figures; 1893. . . . . 1 fr. 25

Mercier (P.), Chimiste, Lauréat de l'Ecole supérieure de Pharmacie de Paris. — *Virages et fixages. Traité historique, théorique et pratique.* 2 vol. in-18 jésus; 1892 . . . . . 5 fr.

On vend séparément :

Ire Partie : *Notice historique. Virages aux sels d'or.* . . 2 fr. 75

IIe Partie : *Virages aux divers métaux. Fixages* . . . . 2 fr. 75

Trutat (E.), Docteur ès-sciences, Directeur du Musée d'Histoire naturelle de Toulouse. — *Traité pratique des agrandissements photographiques.* 2 vol. in-18 jésus, avec 105 figures; 1891.

Ire Partie : Obtention des petits clichés; avec 52 figures . . . 2 fr. 75

IIe Partie : Agrandissements; avec 53 figures . . . . . 2 fr. 75

— *Impressions photographiques aux encres grasses. Traité pratique de photocollographie à l'usage des amateurs.* In-18 jésus, avec nombreuses figures et 1 planche en photocollographie; 1892 . . 2 fr. 75

Vieuille. — *Nouveau guide pratique du photographe amateur.* 3e édit. refondue et beaucoup augmentée. In-18 jésus avec fig. 1892. 2 fr. 75

REVUE GÉNÉRALE

DES SCIENCES

PURES ET APPLIQUÉES

Paraissant le 15 et le 30 de chaque mois, par cahiers de 32 pages grand in-8° colombier, imprimés à 2 colonnes

avec de nombreuses figures dans le texte.

Le moins cher et le plus complet de tous les journaux scientifiques

---

DIRECTEUR : **Louis OLIVIER**, DOCTEUR ÈS SCIENCES

4e ANNÉE

Astronomie, Mécanique, Physique, Chimie, Géologie, Botanique, Zoologie, Anatomie, Physiologie, Anthropologie, Géodésie, Navigation, Génie civil et Génie militaire, Industrie, Agriculture, Hygiène, Médecine, Chirurgie.

Abonnements : chez Georges CARRÉ, Éditeur

58, rue Saint-André-des-Arts, Paris

Paris.	Un an,	20 fr. ;	6 mois,	11 fr.
Départements et Alsace-Lorraine . .	—	22 —	—	12 —
Union postale	—	25 —	—	13 —

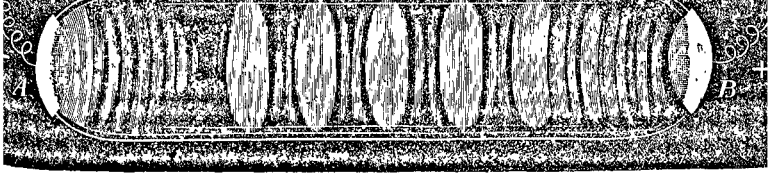
Revue générale des Sciences pures et appliquées

Vulgariser la Science sans jamais l'abaisser ; vulgariser sans vulgairiser.

Le but de cette *Revue* est de permettre à tous ceux qui pratiquent, enseignent ou appliquent la science, d'en suivre régulièrement le progrès théorique et pratique.

A une époque où il devient impossible de lire assidûment les gros ouvrages, le savant, l'ingénieur, le chimiste, l'industriel, le médecin ont besoin d'un recueil périodique qui les renseigne *d'une façon rapide et précise* sur l'état des grandes questions scientifiques à l'ordre du jour.

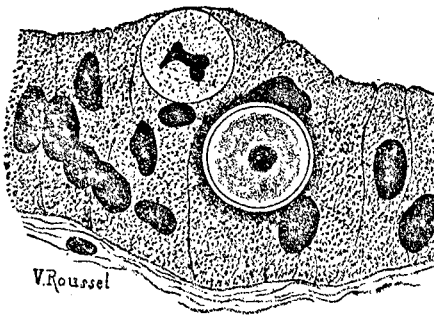
A mesure que celles-ci surgissent et se développent, la *Revue* s'applique à les faire connaître au moyen d'articles très substantiels, très condensés, et en même temps très clairs, faciles à lire, accessibles à tous les hommes instruits, quelle que soit la spécialité professionnelle de chacun d'eux.



Stratification de la lumière dans un tube de Crookes.
Spécimen de l'illustration de la Revue.

Si étroite que soit cette spécialité, elle est toujours tributaire de plusieurs sciences : le chimiste ne peut rester indifférent au progrès général de la Physique ; l'agriculteur, le médecin, l'hygiéniste ont à chaque instant besoin de la chimie, de la physiologie, de la bactériologie. Toutes les branches de la Science sont solidaires, et personne ne saurait, sans dommage pour sa propre spécialité, se priver de leur apport. Mais il est impossible de compulser livres et mémoires pour savoir ce qui se fait en chaque science.

La *Revue* s'acquitte de ce travail au profit du lecteur et lui en donne en peu de mots le résultat positif.



Cellules cancéreuses (article de M. Metchnikoff).
Spécimen de l'illustration de la Revue

Les articles de fonds ont pour objet cette *mise au point* de toutes les questions d'actualité. Le lecteur y trouve, très-clairement exposée, la synthèse précise de ce qui se fait en chaque Science.

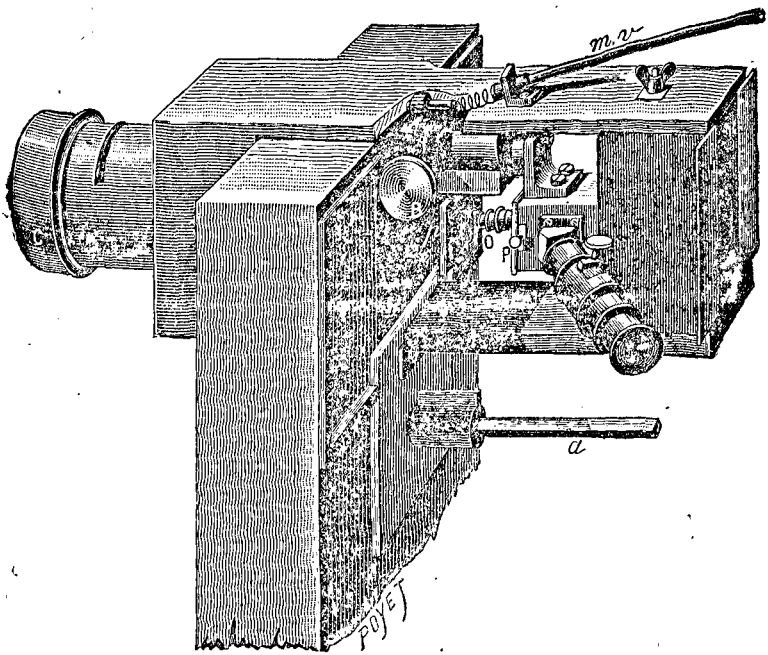
Tous ces articles sont rédigés par des spécialistes, dont la haute notoriété et le talent d'exposition sont universellement appréciés.

Pour ne citer que quelques exemples, les récents perfectionnements des machines à vapeur et de leurs chaudières, des machines à gaz, des régulateurs, les nouvelles dispositions adoptées en Amérique pour l'étude des machines, le transport de la lumière et de la force à grande distance, l'installation des usines centrales pour la distribution de la force motrice par voie électrique ou télédynamique, l'emploi nouvellement fait des courants alternatifs pour actionner les dynamos, la construction de nouveaux types de dynamos, etc., etc., ont été en ces derniers temps, dans la *Revue*, l'objet d'articles très-remarqués de MM, Aimé Witz, H. Léauté (de l'*Académie des Sciences*), V. Dwelshauvers-Dery, J. Hirsch, Sinigaglia, Hospitalier, Rechniewski, Unwin (de la *Société Royale de Londres*), etc., etc.

En chimie pure, agricole, industrielle, photographique, ou physiologique, les beaux articles signés P. P. Dehérain (de l'*Académie des Sciences*), Friedel, (de l'*Académie des Sciences*), Armand Gautier (de l'*Académie des Sciences*), Moissan (de l'*Académie des Sciences*), Schutzenberger (de l'*Académie des Sciences*), Combes, Etard, Ph. A. Guye, Haller, Lebel, Le Chatelier, Le Verrier, Lindet, L. et A. Lumière, Lunge, Maquenne, L. Mond (de la *Société Royale de Londres*), Noelting, etc., etc., n'ont pas moins vivement attiré l'attention.

Dans un autre domaine, celui des sciences biologiques et médicales, les problèmes soulevés par les récentes recherches des zoologistes, paléontologistes, géologues, physiologistes et bactériologistes ont été exposées par MM. A. Milne-Edwards (de l'*Académie des Sciences*). Gaudry (de l'*Académie des Sciences*), H. Filhol, de Lapparent, Bergeron, Marcel Bertrand, Yves Delage, L. Guignard, L. Frédéricq, E. Gley, Bouchard (de l'*Académie des Sciences*), Fournier, Le Dentu, E. Metchnikoff, Charrin, Roger, etc.

Revue générale des Sciences pures et appliquées



Nouvel appareil de M. Marey pour photographier les mouvements des organismes microscopiques
Spécimen de l'illustration de la Revue.

Chaque numéro de la *Revue* renferme 3 parties :

La *première* se compose des ARTICLES DE FONDS précités ;

La *seconde* comprend sous le nom de BIBLIOGRAPHIE l'analyse critique des livres et principaux mémoires récemment parus sur les Sciences : 1° mathématiques ; 2° physiques ; 3° naturelles ; 4° médicales.

Ces analyses sont faites par des spécialistes et signés de leurs noms.

Il en est de même des comptes-rendus de toutes les thèses pour le doctorat de la Faculté des Sciences de Paris.

La *troisième* partie de la *Revue* est consacrée aux comptes-rendus des travaux soumis aux ACADÉMIES ET SOCIÉTÉS SAVANTES DE LA FRANCE ET DE L'ÉTRANGER.

La *Revue* accorde un grand développement au compte-rendu des travaux étrangers, qu'il importe de faire connaître en France dès leur apparition.

Revue générale des Sciences pures et appliquées

Dans ce but, elle a organisé un SERVICE RÉGULIER DE CORRESPONDANCE avec des savants étrangers, qui lui envoient le compte-rendu des travaux soumis à leurs sociétés.

Grâce à ces trois parties de la *Revue*, **l'ensemble de la production scientifique contemporaine est revisé**, — d'une part avec assez de détail pour qu'aucun travail de valeur n'échappe au spécialiste intéressé, — d'autre part avec assez d'ampleur, de critique et de méthode pour fixer nettement dans l'esprit du lecteur l'*état précis du progrès théorique et pratique en chaque science.*

Tous ceux qui, à des titres divers, s'y intéressent, — savants, hommes de laboratoire, professeurs, chimistes, médecins, ingénieurs et grands industriels, trouvent dans la *Revue* le **tableau complet du mouvement scientifique actuel.**

Chaque numéro est accompagné d'un SUPPLÉMENT faisant connaître les NOUVELLES DE LA SCIENCE ET DE L'ENSEIGNEMENT, et donnant, — avantage inestimable pour les hommes d'étude, — le relevé des SOMMAIRES DES PRINCIPAUX JOURNAUX SCIENTIFIQUES DU MONDE ENTIER. Les journaux cités sont au nombre de **300.**

Tous les abonnés reçoivent *de droit*, sous forme de fascicule supplémentaire, la TABLE DES MATIÈRES de la *Revue.*

SPÉCIMEN D'UN NUMÉRO :

I. **P. G. Tait**, *Secrétaire de la Société Royale et Professeur de l'Université d'Edimburg :* Sur la durée du choc (avec figures).

II. **Dr Ledoux-Lebard**, *Chef de Laboratoire à l'Hôpital des Enfants :* la Diphtérie et son traitement par le sérum d'animaux immunisés.

III. **W. Foester**, *Directeur de l'observatoire de Berlin*, et **O Jesse**, *Astronome de l'Observatoire de Berlin :* Les Nuages nocturnes lumineux.

IV. **P. P. Déhérain**, *de l'Académie des Sciences :* Revue annuelle d'Agronomie.

V. **Bibliographie** : Analyse des ouvrages récemment parus sur les sciences : 1° mathématiques ; 2° physiques ; 3° naturelles ; 4° médicales.

VI. **Académies et Sociétés Savantes de la France et de l'Etranger** : Comptes-Rendus de leurs récents travaux.

VII. **Correspondance** : Sur la Zoologie à la *British Association*, par M. J. DE GUERNE.

VIII. **Supplément** : Prochaines élections à l'Académie des Sciences. Prévisions à ce sujet. — Hommage à M. Hermite — Société de Secours des Amis des Sciences. Inventions nouvelles. — SOMMAIRES *des journaux Scientifiques, de la France et de l'Étranger.*

Revue générale des Sciences pures et appliquées

Principaux collaborateurs Français de la Revue :

Membres de l'Académie des Sciences de Paris :

MM. J. Bertrand. — M. Berthelot.
Secrétaires perpétuels de l'Académie.

MM.

Appell (P.), Professeur de Mécanique rationnelle à la Sorbonne.
Becquerel (H), Professeur de Physique au Muséum.
Bouchard (Dr), Professeur de Pathologie et Thérapeutique générale à la Faculté de Médecine.
Bouquet de la Grye (A.), Ingénieur hydrographe de la Marine.
Boussinesq, Professeur de Mécanique physique et expérimentale, à la Faculté des Sciences de Paris.
Cornu (A.), Ingénieur en chef des Mines, Professeur de Physique à l'Ecole Polytechnique.
Chauveau, Inspecteur général des Ecoles vétérinaires, Professeur de Pathologie comparée au Muséum.
Dehérain (P.-P), Professeur de Chimie agricole au Muséum et à l'Ecole d'Agriculture de Grignon.
Faye, Président du Bureau des Longitudes.
Fouqué, Professeur de Minéralogie au Collège de France.
Friedel, Professeur de Chimie organique à la Faculté des Sciences de Paris.
Gaudry (A.), Professeur de Paléontologie au Muséum.
Gautier (A.), Professeur de Chimie à l'Ecole de Médecine.
Grandidier, Géographe.
Janssen (J.), Directeur de l'Observatoire d'Astronomie physique sis à Meudon.
Lénuté (H.), Répétiteur de Mécanique à l'Ecole Polytechnique.
Lévy (Maurice), Professeur de Physique mathématique au Collège de France.
Lippmann (G.). Professeur de Physique à la Faculté des Sciences de Paris.
Lœvy, Sous-Directeur de l'Observatoire de Paris.
Marey (J.), Professeur de Physiologie au Collège de France.
Milne-Edwards (A.), Professeur de Zoologie au Muséum.
Moissan (H,), Professeur de Chimie à l'Ecole supérieure de Pharmacie de Paris.
Picard (E.), Professeur de Calcul différentiel et intégral à la Faculté ees Sciences de Paris.
Poincaré (H.), Professeur de Physique mathématique à la Faculté des Sciences de Paris.
Ranvier, Professeur d'Anatomie générale au Collège de France.
Sarrau (E.), Directeur des Poudres et Salpêtres. Professeur de Mécanique à l'Ecole Polytechnique.
Schutzenberger (P.), Professeur de Chimie générale au Collège de France, et Directeur de l'Ecole de Physique et Chimie de la Ville de Paris.
Tisserand (F.), Directeur de l'Observatoire.

Revue générale des Sciences pures et appliquées

Principaux Collaborateurs étrangers :

Membres de la Société Royale de Londres

R. H. Lord **Kelvin**. — Prof. Michael **Foster**

(Sir William Thomson) ancien Président. Secrétaire.

Boys (C. V.), Professeur au Royal College of Science, à Londres.
Brunton (Th. Lauder) du Collège Royal des Médecins, à Londres.
Christie, Directeur de l'Observatoire de Greenwich.
Common (Andrew-Ainstie), Astronome à Ealing.
Crookes (William), Physicien-Chimiste.
Ferrier (David), Professeur à King's College, à Londres.
Horsley (Victor), Professeur à University-College, à Londres.
Lankester (Ray), Professeur d'Anatomie à l'Université, à Oxford.
Lockyer (N.), Professeur au Royal College of Science, à Londres.
Lodge (Oliver), Pr de Physique à l'Université, à Liverpool.
Lubbock (Right Hon. Sir John). Anthropologiste, à Down.
Mond (L.), Chimiste, à Londres.
Perry (John), Secrétaire de la Société de Physique de Londres.
Pye-Smith (Philip, Henry), Médecin de Guy's Hospital, à Londres.
Ramsay (W.), Pr de Chimie à University College, à Londres.
Rutherford (W.), Professeur à l'Institut de Médecine, à Edimbourg.
Sanderson (J. S. Burdon), Professeur à l'Université, à Oxford.
Schafer (F. A.), Professeur de Physiol. à l'Université, à Londres.
Sollas (W. J.) Professeur de Géolog. à l'Université, à Dublin.
Thompson (S. Philipps), Professeur au Technical College, à Londres.
Tristram (Rev, Henry Baker), Canon of Durham.
Unwin (W.), Professeur à l'Institution centrale de la Cité, à Londres.

Membres de diverses Academies étrangères :

Backlund (O.). Astronome de l'Académie de Saint-Pétersbourg.
Cerruti, Recteur de l'Université Royale de Rome.
Dwelshauvers-Dery, Professeur à l'Université de Liège.
Frédéricq, Professeur de Physiologie à l'Université de Liège.
Gérard (Éric), Directeur de l'Institut électrotechnique Montefiore.
Héger (Dr Paul), Professeur de Physiologie à l'Université.
Holmgron, Professeur de Physiologie à l'Université, à Upsal.
Kuhne (W.), Professeur de Physiologie à l'Université, à Heidelberg.
Lunge, Professeur de Chimie à l'Ecole Polytechnique de Zurich.
Mendelejeff (M.), Membre de l'Académie de Saint-Pétersbourg.
Mosso (A.), Professeur de Physiologie à l'Universite de Turin.
Ostswald, Directeur Zeitschrift fur phys. Chemie à Leipzig.
Perroncito, Président de l'Acad. de Médecine vétérin. de Turin.
Rosenthal (Dr J.), Prof. de Physiologie à l'Université, á Erlangen.
Schoute, Membre de l'Académie des Sciences d'Amsterdam.
Sherrington (Ch. S.) Physiologiste, à Londres.
Sinigaglia, Membre correspondant du Royal Institut de Naples.
Tarchanoff, Prof. de Physiologie à l'Université de St-Pétersbourg,
Tiddeman (D. H.), du Geological Survey of England, Skipton.
Thurston, Directeur du Sibley College à Ithaca (New-York).
Waller (Dr A.), Physiologiste, médecin des Hôpitaux, à Londres.
Wedensky (N. E.), Pr à l'Université de Saint-Pétersbourg.
Weyr (Emil), de l'Académie des Sciences de Vienne.
Wiedemann (Eilhard), Prof. de Physique à l'Université, à Erlangen.

TRAITEMENT DE LA TUBERCULOSE PULMONAIRE

DE LA PLEURÉSIE D'ORIGINE TUBERCULEUSE
ET DES BRONCHITES AIGUES ET CHRONIQUES
par le

GAIACOL IODOFORME SÉRAFON

Et le Gaïacol-Eucalyptol iodoformé érafon

En solutions pour injections hypodermiques
et en capsules pour l'usage interne

PRÉPARATION ET VENTE EN GROS : Société Française de Produits Pharmaceutiques, 9 et 11, rue de la Perle, Paris.

ALIMENTATION DES MALADES PAR LES POUDRES DE *Viande* ADRIAN

La **POUDRE de BIFTECK ADRIAN** (*garantie pure viande de bœuf français*) est aussi inodore et insapide qu'il est possible de l'obtenir en lui conservant les principes nutritifs de la viande. C'est exactement de la chair musculaire privée de son eau, gardant sous un volume très réduit et sous un poids quatre fois moindre, toutes ses propriétés nutritives, et chose importante, n'ayant rien perdu des principes nécessaires à l'assimilation de l'aliment.

Se vend en flacons de 250, 500 gr. et 1 kil.

La **POUDRE DE VIANDE ADRIAN**, d'un prix moins élevé que la poudre de bifteck, ce qui en permet l'emploi aux malades peu fortunés est garantie pure viande de bœuf d'Amérique.

boîtes de 250, 500 gr. et 1 kil.

LA

QUASSINE ADRIAN

essentiellement différente de toutes celles du commerce, est la SEULE dont les effets réguliers aient été constatés. Elle excite l'APPÉTIT, développe les FORCES, combat efficacement les DYSPEPSIES ATONIQUES, les COLIQUES HÉPATIQUES et NÉPHRÉTIQUES. (Bulletin général de thérapeutique, 15 novembre 1882).

Dragées contenant 25 milligrammes de Quassine amorphe.
Granules — 2 — Quassine cristallisée

ANÉMIE

CHLOROSE

Épuisement

Affaiblissement

général

Dans les cas de CHLOROSE et d'ANÉMIE rebelles aux moyens thérapeutiques ordinaires les préparations à base.

D'HÉMOGLOBINE SOLUBLE

DE V. DESCHIENS

ont donné les résultats les plus satisfaisants. Elles ne constipent pas, ne noircissent pas les dents et n'occasionnent jamais de maux d'estomac comme la plupart des autres ferrugineux.

Se vend sous la forme de

SIROP, VIN, DRAGÉES ET ÉLIXIR

préparés par ADRIAN et Cie, 9 rue de la Perle, Paris.

CAPSULES DE TERPINOL ADRIAN

Le TERPINOL a les propriétés de l'essence de Térébenthine dont il dérive, mais il est plus facilement absorbé et surtout *très bien toléré*, ce qui le rend préférable.

Il n'offre pas, comme l'essence de Térébenthine, l'inconvénient grave de provoquer chez les malades des nausées, souvent même des vomissements.

Le TERPINOL est un diurétique et un puissant modificateur des sécrétions catarrhales (bronches, reins, vessie).

Le TERPINOL ADRIAN s'emploie en capsules de 10 centigrammes (5 à 10 par jour).

TRAITEMENT de la SYPHILIS par les PILULES DARDENNE

POLY-IODURÉES SOLUBLES

SOLUBLES dans tous les liquides servant de boisson (Eau, lait, café vin, bière, etc.) elles peuvent être prises en pilules ou transformées par les malades, en **solutions** ou en **sirops**, au moment d'en faire usage.

Premier type (type faible)
(Syphilis ordinaire 2e et 3e année)

2 pilules par jour correspondent à une cuillerée à soupe de *Sirop* de *Gibert*.

Quatrième type (type fort)
(accidents tertiaires, viscéraux et cutanés)

8 pilules par jour correspondent à un centig bi-iodure de mercure et à 4 grammes iodure de potassium.

Vente en GROS : Société Française de Produits Pharmaceutiques, 9 et 11 rue de la Perle, PARIS.

ENCYCLOPÉDIE SCIENTIFIQUE DES AIDE-MÉMOIRE

DIRIGÉE PAR M. LÉAUTÉ, MEMBRE DE L'INSTITUT

Collection de 300 volumes petit in-8 (30 à 40 volumes publiés par an)

CHAQUE VOLUME SE VEND SÉPARÉMENT : BROCHÉ, 2 FR. 50; CARTONNÉ, 3 FR.

Ouvrages en cours de publication

Section de l'Ingénieur

R.-V. PICOU.— Distribution de l'électricité par installations isolées.
A. GOUILLY.— Transmission de la force par air comprimé ou raréfié.
DUQUESNAY.— Résistance des matériaux.
DWELSHAUVERS-DERY.— Étude expérimentale calorimétrique de la machine à vapeur.
A. MADAMET.— Tiroirs et distributeurs de vapeur.
MAGNIER DE LA SOURCE.— Analyse des vins.
ALHEILIG.— Recette, conservation et travail des bois; outils et machines.
R.-V. PICOU.— Distribution de l'électricité par usines centrales.
AIMÉ WITZ.— Thermodynamique à l'usage des Ingénieurs.
LINDET.— La bière.
TH. SCHLŒSING fils.— Chimie agricole.
SAUVAGE.— Divers types de moteurs à vapeur.
LE CHATELIER.— Le Grisou.
MADAMET.— Détente variable de la vapeur.
CRONEAU.— Canon, torpilles et cuirasse.
DUDEBOUT.— Essais des moteurs à vapeur.
LECOMTE.— Les textiles végétaux. Leur examen microchimique.
H. GAUTIER.— Essais d'or et d'argent.
ALHEILIG.— Corderie.
DE LAUNAY.— Formation des gîtes métallifères.
BERTIN.— État actuel de la marine de guerre.
FERDINAND JEAN.— L'industrie des peaux et des cuirs.
BERTHELOT.— Calorimétrie chimique.
DE VIARIS.— L'art de chiffrer et de déchiffrer les dépêches secrètes.
GUENEZ.— La décoration de la porcelaine au feu de moufle.
GUILLAUME.— Unités et étalon

Section du Biologiste

FAISANS.— Maladies des organes respiratoires.
MAGNAN et SÉRIEUX.— Le délire chronique à évolution systématique.
AUVARD.— Gynécologie.— Séméiologie génitale.
G. WEISS.— Technique d'électrophysiologie.
BAZY.— Maladies des voies urinaires.
WURTZ.— Technique bactériologique.
TROUSSEAU.— Hygiène de l'œil.
FÉRÉ.— Epilepsie.
LAVERAN.— Paludisme.
POLIN et LABIT.— Examen des aliments suspects.
BERGONIÉ.— Physique du physiologiste.
MÉGNIN.— Les acariens parasites.
AUVARD.— Menstruation et fécondation.
DEMELIN.— Anatomie obstétricale.
CUÉNOT.— Les moyens de défense dans la série animale.
OLIVIER.— Accouchement physiologique.
CHARRIN.— Poisons de l'urine.
BERGÉ.— Guide de l'étudiant à l'hôpital.
BROCQ et JACQUET.— Traité élémentaire et pratique de dermatologie.
LANGLOIS.— Le lait.
WEILL.— Guide du médecin d'assurances sur la vie.
HANOT et LEGRY.— De l'endocardite.
BROCA.— Les ostéo-arthrites tuberculeuses chez l'enfant.
DE BRUN.— Maladies des pays chauds.
DU CAZAL.— Organisation du service de santé militaire.
DE LAPERSONNE.— La cataracte.
ROGER.— Physiologie normale et pathologique du foie.
KŒHLER.— Application de la photographie aux sciences naturelles.

ENCYCLOPÉDIE SCIENTIFIQUE DES AIDE-MÉMOIRE

Ouvrages en cours de publication. (Suite.)

Section de l'Ingénieur

WIDMANN. — Principes de la machine à vapeur.
POL MINEL. — Électricité industrielle.
GÉRARD-LAVERGNE. — Les Turbines.
BLOCH. — Appareils producteurs d'eau sous pression.
WALLON. — Objectifs photographiques.
H. LAURENT. — Théorie des jeux de hasard.
NAUDIN. — Fabrication des vernis.
DWELSHAUVERS-DERY. — Étude expérimentale dynamique de la machine à vapeur.
MADAMET. — Épures de régulation. Courbes d'indicateurs.
CRONEAU. — Construction du navire.
VERMAND. — Moteurs à gaz et à pétrole.
CASPARI. — Chronomètres de marine.
ALHEILIG — Construction et résistance des machines à vapeur.
POL MINEL. — Électricité appliquée à la marine
H. LÉAUTÉ et A. BÉRARD. — Transmissions par câbles métalliques
GUYE (PH.-A.). — Matières colorantes.
HOSPITALIER (E.). — Les compteurs d'électricité.
EMILE BOIRE. — La sucrerie.
G. CHARPY. — Production industrielle du froid.
MOISSAN et OUVRARD. — Le nickel, sa production et ses applications.
ROUCHÉ. — La perspective.
LE VERRIER. — La fonderie.
SEYRIG — Statique graphique
Cte BASSOT et Ce DEFFORGES. — Géodésie.
DELAFOND — Recherche des gites de houille.
DE LA BAUME PLUVINEL. — La théorie des procédés photographiques.
J. RESAL. — Emploi des métaux et du bois dans les Constructions.
GARNIER et GODARD. — Montage et conduite des machines à vapeur.
ARMENGAUD JEUNE. — Brevets d'invention.
CANDLOT. — Chaux, ciments et mortiers.

Section du Biologiste

HÉBERT. — Les boissons falsifiées.
BEAUREGARD. — Le microscope.
LETULLE. — L'inflammation.
OLLIER. — Les résections.
BUDIN. — Thérapeutique obstétricale.
BAZY. — Troubles fonctionnels des voies urinaires.
FAISANS. — Diagnostic précoce de la tuberculose.
DASTRE. — La Digestion.
AIMÉ GIRARD. — La betterave à sucre.
LANNELONGUE. — La Tuberculose chirurgicale.
STRAUS. — Les bactéries.
NAPIAS. — Hygiène industrielle et professionnelle.
GOMBAULT. — Pathologie du bulbe rachidien.
LEGROUX. — Pathologie générale infantile.
MARCHANT-GÉRARD. — Chirurgie du système nerveux : Cerveau.
BERTHAULT. — Les prairies naturelles et temporaires.
BRAULT. — Myocarde et artères.
CORNEVIN. — Production du lait.
GAMALEIA. — Vaccination préventive
ARLOING. — Maladies charbonneuses.
NOCARD. — Les Tuberculoses animales dans leur rapport avec la Tuberculose humaine.
EDM. PERRIER. — Le Système de l'évolution.
MATHIAS DUVAL. — La Fécondation.
BRISSAUD. — L'Hémisphère cérébral.
RECLUS. — Affections des organes génitaux de l'homme.
HÉNOCQUE. — Spectroscopie biologique.
J. CHATIN. — Anatomie comparée.
DEHÉRAIN. — Les céréales.
MERKLEN. — Maladies du cœur.
A.-J. MARTIN. — Hygiène de l'habitation privée.
BRUN. — Examen et exploration de l'œil.
FRANÇOIS-FRANK. — Physiologie normale et pathologique du cœur.