COMMANDANT BAZERIES

LES CHIFFRES SECRETS DÉVOILÉS

ÉTUDE HISTORIQUE SUR LES CHIFFRES

APPUYÉE DE DOCUMENTS INÉDITS

TIRÉS DES DIFFÉRENTS DÉPÔTS D'ARCHIVES

PARIS

LIBRAIRIE CHARPENTIER ET FASQUELLE

EUGÈNE FASQUELLE, ÉDITEUR

11, RUE DE GRENELLE, 11

1901

LES

CHIFFRES SECRETS

DÉVOILÉS

DU COMMANDANT BAZERIES

Tables chiffrantes et déchiffrantes. — Librairie de A. Hermann, éditeur, 8, rue de la Sorbonne, Paris, 1893.

Introduction et usage. — Fascicule in-12. Envoi *gratuit* et *franco* sur demande à l'éditeur.

Table n° 1. — In-12, toile formant portefeuille . . **7 50**
Table n° 2. — In-12, toile formant portefeuille . . **7 50**

Les chiffres de Napoléon Ier, pendant la campagne de 1813. — Épisodes du siège de Hambourg. Éditeur M. Bourges, imprimeur breveté, 32, rue de l'Arbre-Sec, Fontainebleau, 1896. Fascicule in-12. . . . . **2** »

En collaboration avec M. Emile BURGAUD

Le Masque de Fer. — Révélation de la Correspondance chiffrée de Louis XIV. Firmin-Didot et Cie, éditeur, 56, rue Jacob, Paris, 1893. Un volume in-18. . . . . **3 50**

Il a été tiré de cet ouvrage
6 exemplaires numérotés sur papier de Japon.

COMMANDANT BAZERIES

LES

CHIFFRES SECRETS

DÉVOILÉS

ÉTUDE HISTORIQUE SUR LES CHIFFRES

APPUYÉE DE DOCUMENTS INÉDITS

TIRÉS DES DIFFÉRENTS DÉPÔTS D'ARCHIVES

« C'est en frappant toujours sur le même clou
« qu'on parvient à l'enfoncer. »

***

« Divulguer des faits qui tenus secrets peuvent
« compromettre la Défense Nationale, c'est faire
« acte de bon Français. »

(X***).

PARIS
LIBRAIRIE CHARPENTIER ET FASQUELLE
EUGÈNE FASQUELLE, ÉDITEUR
11, RUE DE GRENELLE, 11

1901

INTRODUCTION

Le retentissement donné au déchiffrement des dépêches du duc d'Orléans, par suite du procès pour complot contre la sûreté de l'État, devant la Haute-Cour de Justice, a eu pour résultat de remettre la cryptographie en honneur et de nous faire demander par de bons esprits la vulgarisation de nos procédés de déchiffrement.

De tous côtés on nous prie de publier un *Traité de Cryptographie*.

*
* *

Des auteurs contemporains éminents se sont occupés déjà de la cryptographie, et ont surtout visé la cryptographie militaire. Parmi les

plus remarquables, M. H. Josse, alors capitaine d'artillerie, breveté, a fait preuve d'une érudition parfaite ; mais les règles qu'il a développées et suggérées sont loin d'être exemptes de critique.

Comme quelques-unes de ces règles cryptographiques sont, à notre avis, désastreuses, et pourraient devenir néfastes pour le Pays, nous nous décidons à publier, non un *Traité de Cryptographie* — cela nous mènerait trop loin — mais une simple étude historique sur certains chiffres en usage de nos jours, et quelques déchiffrements intéressants.

* *

Le lecteur pourra juger combien sont fragiles ces chiffres, surtout les chiffres militaires français; combien ces derniers offrent peu de résistance au déchiffrement et, par suite, peu de sécurité ; combien les chiffres employés par les anarchistes et par le duc d'Orléans étaient mieux établis.

Puisse cette révélation amener le départe-

ment de la Guerre à changer ses serrures. Le but que nous poursuivons depuis dix ans serait atteint et nous nous déclarerions satisfait si nous pouvions par la publication de cette étude obtenir ce résultat.

Il est des choses qu'on voudrait ne pas dire, mais, en présence de l'aveuglement *voulu* des bureaux compétents, le devoir est d'en parler.

* * *

Si cette question des chiffres a son importance, nous savons aussi combien elle est aride. Pour ne pas rebuter le lecteur, nous avons agrémenté cette étude de quelques anecdotes historiques, peu connues ou inédites pour la plupart. Nous espérons rendre ainsi sinon attrayante, du moins intéressante, la lecture de *Chiffres secrets dévoilés*.

Paris, *Janvier* 1901.

COMMANDANT BAZERIES.

PREMIÈRE PARTIE

CONSIDÉRATIONS GÉNÉRALES RENSEIGNEMENTS HISTORIQUES

CHAPITRE PREMIER

DES DIFFÉRENTS SYSTÈMES ET MÉTHODES

CLASSEMENT DES MÉTHODES. — Les méthodes cryptographiques sont nombreuses, on peut même dire qu'il y a autant de méthodes qu'il y a de personnes qui se sont occupées de cryptographie.

Pour obtenir un peu de clarté dans cet amas de méthodes et pour que le lecteur s'y reconnaisse sans fatigue, nous les ramènerons toutes à deux systèmes principaux :

Premier système : Chiffrement lettre par lettre ;

Deuxième système : Chiffrement mot par mot.

* * *

Dans le premier système, chaque lettre du texte clair est représentée par un signe.

Ce signe s'appelle : **chiffre**.

Il peut être quelconque : lettre, chiffre arabe, signe particulier, géométrique, algébrique, astronomique ou arithmétique, note de musique, etc., etc.

*
* *

Dans le deuxième système, le **chiffre** est un groupe de chiffres arabes, de lettres, ou un mot de convention.

Dans ce système, chaque **chiffre** représente soit une lettre, soit une syllabe ou fraction de mot, soit un mot, soit plusieurs mots formant une expression usuelle du texte clair.

*
* *

ANCIENNETÉ DES MÉTHODES. — Ce sont les méthodes du premier système qui sont les plus anciennes.

Tous les auteurs cryptologues ont dit que Jules César correspondait en chiffres avec ses généraux. D'après les uns, il remplaçait chaque lettre de l'alphabet par la suivante ; d'après d'autres, il faisait usage d'un alphabet où chaque lettre était avancée de quatre rangs.

L'alphabet à la **Jules César** est devenu classique en cryptographie.

*
* *

Les mêmes auteurs ont parlé de la scytale des Lacédémoniens. Le bibliophile Jacob l'a décrite dans *les Secrets de nos Pères*.

C'était tout simplement un bâton sur lequel s'enroulait l'écrit chiffré.

Si les cryptogrammes obtenus par ce moyen échappaient à la sagacité des Spartiates, ils ne résisteraient guère aujourd'hui aux recherches des déchiffreurs. Le lecteur peut s'en rendre compte en traduisant lui-même le cryptogramme suivant, obtenu avec une scytale :

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

En relevant les lettres de 17 en 17, en commençant par la première, il devient facile de lire : *quand ils avaient à correspondre avec leurs généraux, les Lacédémoniens*, etc.

Une seule lettre Q, et l'écart de 17 avec la première lettre U a suffi pour permettre la lecture ; cette lecture sera encore bien plus facile si on place les lettres en colonnes horizontales et verticales sur 17 de front. On lira ainsi colonne verticale par

colonne verticale de la première à la dernière.

*
* *

Ce sont ces deux antiques procédés qui ont donné naissance aux innombrables méthodes du système de chiffrement, lettre par lettre :

1° Méthodes de substitution (Jules César) ;

2° Méthodes de transposition (Lacédémoniens).

*
* *

Les méthodes du deuxième système — chiffrement — mot par mot — sont plus récentes. Elles sont dues à Rossignol dont on parle plus loin, et elles ont été la conséquence logique et forcée de déchiffrements retentissants faits sous les règnes de Henri IV et de Louis XIII.

*
* *

Indépendamment des systèmes et méthodes cryptographiques que nous venons d'exposer, d'autres, moins classiques, n'en étaient pas moins connus et employés dans l'antiquité, au moyen âge, et même de nos jours.

Nous allons leur consacrer quelques lignes.

Ces autres systèmes sont :

La cryptographie par initiales ou par abréviations ;

Le jargon;
Le langage allégorique;
La cryptographie par mots convenus;
Les écritures secrètes.

CRYPTOGRAPHIE PAR INITIALES OU PAR ABRÉVIATIONS

Ce système était connu dès la plus haute antiquité.

En traduisant une inscription que Xantus ne pouvait parvenir à comprendre, Esope se trouve être le premier déchiffreur célèbre[1].

Le christianisme a fait et fait encore un grand usage de ce genre de cryptographie.

L'inscription INRI, sur le Christ (*Jesus Nazareus Rex Judæorum*), en est l'exemple le plus saillant.

Les épigraphies grecque, romaine, chypriote et du moyen âge ne sont que de la cryptographie par initiales.

Sous la Commune, en 1871, le F.F.F. (Faites Flamber Finances) de Raoul Rigault montre que ce système est encore employé de nos jours et que les initiés, quelquefois, ne le comprennent que trop bien.

A vrai dire, ces abréviations de mots ne peuvent

[1] Voir la *Vie d'Esope le Phrygien*, par La Fontaine.

constituer un système cryptographique, car, de même qu'Esope donna trois sens différents à l'inscription grecque qui fit trouver un trésor à son maître, de même que les archéologues ne sont pas toujours d'accord sur le déchiffrement des inscriptions romaines ou autres, les cryptologues traduiraient les lettres R. F. par exemple, les uns par République Française, d'autres par Rothschild Frères.

Les abréviations employées au moyen-âge, principalement à la fin des mots, ne peuvent guère se rattacher à la cryptographie. Il faut être simplement initié pour savoir, par exemple, que : *p̄lemēt* signifie parlement, et que *m̄glr̄s* veut dire marguilliers.

JARGON

Le jargon est un système cryptographique, qui a été fort en vogue à la cour de France, pendant le XVII^e^ siècle.

Les instructions données au commandeur de Sillery, s'en allant en ambassade à Rome, près de Sa Sainteté, en l'an 1622, renferment un chiffre spécial exclusivement composé de jargon[1]. Tous les per-

[1] Bibliothèque nationale, L^b^. 36-65.

sonnages sont désignés par des noms baroques, noms de fleurs, d'arbres, de sports, d'armes, de meubles, etc.

A titre de curiosité, on donne ce chiffre.

Personnages ou pays désignés.	Mots convenus pour les désigner.
Rome	Jardin.
Le Pape	La Roze.
Cardinal Ludovisio	L'Œillet.
— Borghèse	La Pensée.
— Aldobrandin	Le Jasmin.
— de Savoye	Le Laurier.
— de Montalte	Le Cyprez.
— de Sourdis	Le Pescher.
— de Vicenze	Le Coigner.
— de la Rochefoucaud	Le Poirier.
— de Retz	Le Prunier.
— de la Valette	Le Pommier.
— Bentivoglio	L'Abricotier.
— Bevilacqua	Le Cerisier.
— Barberin	Le Griottier.
— Ubaldini	L'Alizier.
— Baudini	La Marguerite.
— de Médicis	Le Muguet.
— Mullini	L'Oranger.
— Sainte-Suzanne	Le Citronnier.
— Verallo	Le Figuier.
— Ara-Celi	Le Thin.
— des Ursins	La Marjolaine.
— Campora	La Laictue.
— d'Est	La Buglose.
— Savelli	La Bourrache.
Le Grand-Duc	Passe-velours.
La Grande-Duchesse	La Vigne.
L'Archiduché	Le Raisin.
Monsieur de Mantoüe	Le Noyer.
La Seigneurie de Venise	L'Amandier.
Le gouverneur de Milan	L'Aubépine.
La République de Gennes	Le Tillac.
Monsieur de Savoye	La Tulipe.

Monsieur le prince de Piémont. .	L'Anémone.
Le duc de Mantoüe	La Sauge.
L'Empereur	Le Coursier.
Le Roy d'Espagne.	Le Barbe
L'Archiduc Léopold	L'Alsan.
L'Infante de Flandres.	La Haquenée.
Le comte d'Olivarez	Le gris pommelé.
Don Balthazar de Cuniga	Le Fauve.
Allemagne.	L'Écurie.
Espagne	La Mangeoire.
Flandres	Le Râtelier.
L'Angleterre.	La Fourche.
Le Roy de la Grand'Bretagne. . .	Le Palefrenier.
Le prince de Galles	Le Bidet.
L'Électeur Palatin.	Le Courtault.
Le duc de Bavière.	Le Roussin.
Monsieur de Lorraine.	Le Mallier.
Les Suisses	Les Étriers.
Les Grisons	Les Esperons.
La Valteline.	La Selle.
Catholiques	Les Bottes.
Protestants	Les Resnes.
Le Nonce de France	Le Mords.
— des Suisses	La Bride.
Le vice-légat d'Avignon.	La Housse.
L'évesque de Lusson.	La Houssine.
Monsieur de Lyon.	L'Escuyer.
— de Villiers.	Le Page.
— de Marini	Le Manège.
Les ambassadeurs du Roy en Suisse.	Les Pilliers.
Le sieur Eschinard.	La Lisse.
— Rabi.	La Bague.
Le secrétaire le Fèvre	La Lance.
Le sieur Pol-Fiefco	La Carrière.
— Frangipani	La Picque.
Monsieur Rucellai.	Le Mousquet.
France.	Bastiment.
Le Roy.	Pied d'Estail.
La Reyne.	La Corniche.
La Reyne-mère.	La Porte.
Monsieur frère du Roy.	La Fenestre.
Madame sœur du Roy	La Chambre.
Monsieur le Prince.	La Salle.

Monsieur le comte de Soissons . .	Le Grenier.
Monsieur de Guyse.	La Cour.
— le Prince de Joinville. .	La Cheminée.
— de Longueville	La Table.
— de Vendôme	La Chaise.
— de Nemours	Le Banc.
— d'Elbœuf.	Le Lict.
— le comte de Saint-Paul .	Le Buffet.
— d'Angoulême	Le Cabinet.
— d'Espernon.	Le Tapis.
— de Montmorency. . . .	Le Chevron.
— d'Esdiguières	La Poultre.
— de Créquy	L'Entablement.
— de Schoomberg	La Croisée.
— de Bassompierre. . . .	Le Pignon.
— le marquis de Cœuvres .	L'Escalier.
— le commandeur de Sillery.	Le Tabernacle.
— le chancelier de Sillery .	Le Chapelain.
— de Puyfieux.	L'Oratoire.
Madame de Puyfieux.	La Chapelle.
Monsieur de Marais	Le Prestre.
— de Bellièvre.	Le Clerc.
— de Valençay	Le Choriste.
L'évesques de Chartres	Le Chantre.
Le chevalier de Valençay	Le Novice.
Monsieur de Berry.	Le Diacre.
— de Léon.	L'Accolyte.
— le garde des Sceaux . .	L'Arquebuze.
— de Gesvres.	Le Morion.
— de la Ville-aux-Clercs. .	L'Espée.
— d'Herbault.	La Pertuisanne.
— de Beaumarchais. . . .	La Hallebarde.
— Morant	Le Pistolet.
Pensions de Rome.	Les Balles.
Le duc Sforce.	La Poudre.
— de Saint-Gemini	La Carabine.

Les correspondances faites avec ce système de chiffre étaient entièrement en clair, sauf les noms des personnages, qui étaient remplacés par leur chiffre.

Pour les personnes au courant des questions traitées, il n'était pas bien difficile d'en faire la traduction.

*
* *

Dans différents documents de la Bibliothèque Nationale, on peut trouver des chiffres en jargon, entre autres dans le *Journal de Monsieur le cardinal de Richelieu, qu'il a faict durant le grand orage de la Court en l'année* 1630 *et* 1631.

LANGAGE ALLÉGORIQUE

La cryptographie par langage allégorique suivit le jargon et le remplaça à la cour de France.

Le meilleur exemple que nous puissions donner du langage allégorique est celui imaginé par la diplomatie secrète de Louis XV, et dont on trouve la clef dans les instructions données au chevalier Douglas, le 1er juin 1755, pour sa mission secrète en Russie[1].

D'après ces instructions le fond du langage allégorique devait être des achats de fourrures.

[1] Voir Boutaric, *Correspondance secrète inédite de Louis XV sur la politique étrangère avec le comte de Broglie, Tercier, etc.*, t. I, p. 203-209, ou *le Secret du roi, par le duc de Broglie*, t. I, p. 449-454.

Le *renard noir* signifiait le chevalier William, ministre de l'Angleterre.

Le *renard noir était cher* en cas de réussite de ce ministre.

L'*hermine* signifiait le parti russien.

L'*hermine était en vogue* en cas de domination de ce parti.

Le *loup-cervier* signifiait le parti autrichien, à la tête duquel était M. de Bestucheff.

Le *loup-cervier avait son prix*, en cas de prépondérance de ce parti.

La phrase :

Les Soboles ou martres zibelines diminuent de prix marquait la diminution du crédit de M. de Bestucheff.

La phrase :

Les Soboles ou martres zibelines sont toujours au même prix indiquait que M. de Bestucheff était toujours dans la même faveur.

Les *peaux de petit-gris* indiquaient les troupes à la solde de l'Angleterre.

Dix peaux de petit-gris signifiaient 30.000 hommes; *vingt peaux*, 60.000 hommes, etc.; chaque peau indiquant 3.000 hommes.

La question de santé, de remises, etc., jouait aussi un rôle important pour les déplacements prévus et, enfin, la phrase : *On a trouvé ici un manchon, par conséquent on le prie de n'en point acheter*, était l'ordre de revenir.

*
* *

Les méthodes de guerre au XIX^e^ *siècle*, de M. le général Pierron, contiennent une lettre envoyée par un espion, au quartier général autrichien, le 31 juillet 1813, après une reconnaissance à Trieste, qui est un modèle de cryptographie allégorique[1].

Le fond du langage allégorique est un commerce d'articles d'épicerie.

CRYPTOGRAPHIE PAR MOTS CONVENUS

Ce système est surtout fort en honneur dans les grandes agences européennes.

Il oblige à un travail incessant; il faut prévoir les événements et adopter à l'avance les mots convenus pour les annoncer lorsqu'ils se produisent.

On se sert généralement de termes de bourse, parce que les dépêches financières ont un droit de priorité.

*
* *

Lorsqu'un télégramme mentionne une *baisse sur les cotons*, par exemple, l'agence étrangère qui le

[1] M. H. Josse a donné cette lettre dans *la Cryptographie et ses applications à l'art militaire*, p. 85.

reçoit, et qui sait que *baisse des cotons* est une expression convenue pour annoncer la chute de tel ministère ou la mort de tel personnage, s'empresse de porter ce fait à la connaissance de la Presse, ainsi rapidement informée, souvent à l'insu du Gouvernement, qui aurait voulu retarder de quelques heures la publication de cet événement.

Ce système a un défaut, il n'est sûr que tant qu'on n'y prend pas garde. Du moment où l'attention est en éveil, on reconnaît facilement le sens secret des mots de convention, surtout si les correspondances échangées sont nombreuses.

Les correspondances téléphoniques ont considérablement réduit ce mode de cryptographie.

ÉCRITURES SECRÈTES

Les écritures secrètes s'obtiennent au moyen d'une convention ou avec une encre invisible dénommée encre sympathique.

Écriture secrète au moyen d'une convention

M. H. Josse donne dans son livre[1] un exemple historique d'écriture secrète. C'est une lettre de

[1] *La Cryptographie et ses applications à l'art militaire*, p. 88.

Mme de Saint-André à Louis Ier de Bourbon, prince de Condé, arrêté le 31 octobre 1560 et emprisonné à Orléans.

Il fallait lire la lettre par lignes impaires pour en avoir le sens secret.

*
* *

Récemment une nouvelle méthode a été inventée; nous allons lui consacrer quelques lignes.

MÉTHODE BOETZEL ET O'KEENAN

En 1895, MM. Boetzel et O'Keenan publiaient un ouvrage intitulé : *Ecriture secrète.*

Le 26 novembre, une conférence sur cette méthode était faite par l'un des auteurs, M. Boetzel, dans les salons de l'Institut Rudy, 4, rue Caumartin.

*
* *

Le conférencier ne réussit pas à convaincre de l'indéchiffrabilité de sa méthode les quelques audi-

teurs compétents qui y assistaient : colonel Fix, de Viaris, capitaine Marin, Gavrelle, etc.

En effet, c'était par des liaisons de lettres (de 1 à 6) et par des crochets plus ou moins grands, soit avant, soit après (se traduisant de 0 à 3), que les auteurs réussissaient à transformer un sens clair insignifiant en un écrit chiffré.

L'allure de l'écriture trahissait à première vue le système.

*
* *

Nous nous sommes amusé à vérifier le déchiffrement de la page 97 du livre de MM. Boetzel et O'Keenan, et dont les auteurs donnaient la traduction. Le texte insignifiant était : « Reçu votre honorée... » etc.

D'après les auteurs, le sens secret de cette missive était : « L'ennemi a 297 canons, 138.900 hommes à pied, 32.000 cavaliers, les 4 sur 5 malades. »

Pour déchiffrer, nous avons transformé l'écrit insignifiant en cryptographie système Mirabeau[1].

[1] Ce système nous a été révélé par le déchiffrement de quelques lettres authentiques de la marquise Sophie de Monnier à son célèbre amant M. de Mirabeau, que M. Cottin devait publier dans *la Revue Rétrospective*. Cette publication n'ayant pas encore été faite, nous supposons avec juste raison que la teneur pornographique de cette correspondance chiffrée a dû être un obstacle insurmontable.

Voici ce que cette opération nous a donné[1] :

3	4	2	2	4	3	2	4	1	2	2	5	4	2	6	2	1
0	0	1	1	0	1	0	1	2	1	2	2	1	1	0	1	0
l	e	n	n	e	m	i	a	d	n	p	c	a	n	o	n	s
								2	9	7						

5	6	1	2	5	6	1	6	3	3	4	1	4	2	2	4	1
3	1	1	1	3	3	1	0	1	1	0	0	1	2	0	0	2
x	t	h	n	x	z	h	o	m	m	c	s	a	p	i	e	d
6	3	8	9	6	0											

6	1	6	6	6	5	4	5	4	3	2	4	5	1	3	4	1
1	2	3	3	3	2	1	1	1	0	0	0	0	0	0	0	0
t	d	z	z	z	c	a	v	a	l	i	e	r	s	l	e	s
3	2	0	0	0												

3	1	4	5	5	3	4	3	4	1	4	1
3	0	3	0	2	1	1	0	1	2	0	0
q	s	u	r	c	m	a	l	a	d	e	s
4				5							

Au lieu de 138.900 hommes que voulaient chiffrer les auteurs, ils ont chiffré 638.960.

Les erreurs avaient été commises au mot SEREZ qui, au lieu d'être ainsi écrit : *serez*, aurait dû s'écrire : *sere 3*, et au mot SATIS qui aurait dû être : *satisf* et non *satis f*.

[1] Les numérateurs indiquent le nombre de lettres liées ensemble et formant un groupe; les dénominateurs indiquent les boucles (0 sans boucle, 1, 2, 3 petite ou grande boucle, avant et après).

*
* *

Le lecteur peut juger que ce système demande une attention par trop soutenue pour éviter les erreurs. Une liaison omise ou une lettre en trop ou encore un crochet omis avant ou après le groupe, ou trop grand ou trop petit, changent complètement la valeur de la lettre que l'on veut représenter.

*
* *

Le système d'écriture secrète, imaginé par MM. Boetzel et O'Keenan, a le mérite de l'originalité ; mais, comme valeur cryptographique, cela revient absolument au mode de cryptographie par un simple alphabet convenu.

ENCRE SYMPATHIQUE

On ne peut moins faire que de dire un mot sur ce système cryptographique, connu aussi dans l'antiquité.

D'après un auteur cryptologue, Philon de Byzance, qui vivait au IIe siècle avant Jésus-Christ, avait composé tout un traité sur l'envoi des lettres secrètes ; mais cet ouvrage aurait été perdu.

D'après un autre auteur, le même Philon de Byzance s'exprime comme ci-après, dans son livre *de l'Attaque des places :*

« Les lettres secrètes s'écrivent avec une infusion « de noix de galle concassées. Quand les caractères « sèchent, ils deviennent invisibles. Il suffit, pour « les voir reparaître, de les mouiller avec une éponge « imbibée d'une dissolution de sulfate de cuivre, « comme lorsqu'on prépare l'encre. »

Une dissolution de sulfate de cuivre, cela nous paraît bien savant pour le IIe siècle avant Jésus-Christ.

* * *

Ce qu'il y a de certain, c'est que, si l'encre sympathique était employée au XVIIe siècle, elle était peu connue. Fouquet la connaissait; Louvois l'ignorait. La lettre de Louvois à Saint-Mars, du 26 juillet 1665, existant au *Dépôt de la Guerre*, en fait foi :

« Il faut que vous essayiez de savoir du valet de « M. Fouquet comment il a écrit les quatre lignes « qui ont paru dans le livre en le chauffant et de « quoi il a composé cette écriture. »

* * *

Nous tenons d'un de nos parents mêlé, en Espagne, à la guerre carliste de 1833 à 1839, que c'était au

moyen de l'encre sympathique que s'échangeaient les correspondances secrètes entre Don Carlos, son allié Dom Miguel, les généraux Cabrera, Zumala-Carregui, etc., et leurs principaux partisans.

L'encre sympathique dont ils faisaient usage était le jus de citron.

Ils écrivaient avec ce jus entre les lignes d'une correspondance insignifiante ou sur le papier blanc de cette correspondance, ce qu'ils voulaient se communiquer d'important ou de secret. Le correspondant n'avait qu'à faire chauffer le papier, les caractères de l'écrit secret ressortaient, à la chaleur, suffisamment lisibles.

* * *

Un auteur a indiqué le lait comme encre sympathique. C'est une mauvaise encre, car elle laisse des traces visibles sur le papier.

* * *

Quelques ouvrages donnent aussi, comme encre sympathique la plus employée, une dissolution étendue de chlorure de cobalt. En chauffant le papier, l'écriture ressort en bleu, le refroidissement rend de nouveau les caractères secrets invisibles.

Cette encre sympathique nous paraît bien compliquée, et puis, n'en ayant pas fait l'essai, nous

sommes un peu incrédule sur les propriétés attribuées au chlorure de cobalt.

*
* *

Le jus d'oignon et de cerises et, en général, tous les sucs incolores peuvent servir d'encre sympathique ; mais la meilleure et la plus pratique, à notre avis, est celle des carlistes : le jus de citron.

On trouve toujours des citrons partout et en tout temps, tandis que les cerises n'ont qu'un temps et que les oignons sont désagréables pour les yeux et pour l'odorat.

En résumé, les correspondances secrètes au moyen d'encres sympathiques sont dévoilées soit en chauffant le papier, soit en le mouillant.

*
* *

Pour terminer cet exposé de systèmes cryptographiques, nous dirons que l'écriture cunéiforme des Assyriens et des Mèdes, et les hiéroglyphes des Egyptiens pourraient presque se rattacher à la cryptographie.

En effet, ces écrits sont restés indéchiffrables pendant des siècles et le seraient encore, si des savants n'en avaient reconstitué les alphabets, au commencement du XIX^e^ siècle.

Grâce à George Rawlinson, auteur des *Quatre*

grandes Monarchies de l'Ancien Monde oriental, et à Jules Oppert, auteur des *Inscriptions cunéiformes déchiffrées une seconde fois*, pour les écritures assyriennes; grâce aussi à François Champollion, pour l'écriture sacrée des Egyptiens, aujourd'hui tout le monde peut interpréter les écritures assyriennes et égyptiennes aussi couramment qu'un texte de vieux latin ou de vieux français.

*
* *

Enfin la sténographie pourrait aussi se rattacher à la cryptographie, si les récits sténographiés n'étaient du clair pour les initiés, comme les signes de l'alphabet Morse sont du clair pour les télégraphistes.

CHAPITRE II

MÉTHODES DE SUBSTITUTION

Les méthodes de *substitution* ont d'abord été basées sur un alphabet conventionnel.

Cet alphabet s'est considérablement augmenté par la suite : des nulles y sont entrées en grande quantité ; on a attribué plusieurs signes à chaque lettre ; d'autres signes représentaient les personnages et les mots usuels. On sent la préoccupation de dépister les déchiffreurs, et en même temps ces chiffres étaient un acheminement naturel vers le système du chiffrement mot par mot.

A titre de curiosité, on donne trois chiffres historiques :

1° Chiffre de M. de Bassefontaine . . . 1555
2° Chiffre de M. de Béthune. 1599
3° Chiffre des Emigrés. 1793

Le lecteur pourra remarquer, en comparant ces trois chiffres, le progrès réalisé de 1555 à 1599 et la faiblesse du chiffre des émigrés par rapport à ceux du XVI^e^ siècle.

ANNÉE 1555

Chiffre de M. de Bassefontaine, en ses négociations avec le Lantgrave et autres

Le pappe..... ✱
Le Roy ..... on
L'empereur..... ne
Les protestants..... 4
La guerre..... ey
La Paix..... Bien
Les allemands..... 7e
Lantgrave..... 7our
Bronzmeh..... nour

NULLES

DOUBLES

CHIFFRE BAILLÉ A

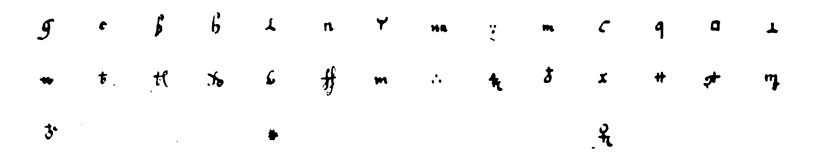
MAY

		A	B	C	D	E	F	G	H
Le Roy	4	3	10	8	11	7	2	15	4
Le Pappe	3								
L'Empereur	5								
Le Roy d'Espagne	2								
Le grand Seigneur	6								
La Royne d'Angleterre	7								
Le Roy d'Ecosse	8								
L'Archiduc d'Autriche	9								
L'Infante d'Espagne	10								
Les Etats du Pays-Bas	11								
La Seigneurie de Venize	12	ayant					a,	entre	
Le Roy de Danemark	13	ans					b,	faut	
Le Roy de Suède	14	argent					c,	faire	
Les cantons de Suisse	15	actendu					d,	foy	
Le duc de Savoye	16	actendant					e,	grand	
Le duc de Lorraine	17	après					f,	gens	
Le duc de Guyse	18	buy					g,	garde	
Le prince Maurice	19	bon					h,	guesre	
Le comte d'Essex	20	beau					j,	hon	
Le secrétaire Cecyl	21	baille					k,	hommes	
— L'Eviston	22	car					l,	hautes	
Le sieur de Boissize	23	convient					m,	heur	
Le sieur de Buzanval	24	con					n,	je	
L'archevesque de Glasco	25	contenant					o,	intention	
France	26	donne					p,	jay	
Ecosse	27	dire					q,	Il	
Flandres	28	dont					r,	Le	
Hollande	29	despesche					s,	La	
Angleterre	30	dequoy					t,	Lettres	
Suède	31	ent					U,	mois	
Danemarck	32	encores					x,	ment	
		et					y,	mons	

M. DE BÉTHUNE

1599

J	L	M	N	O	P	Q	R	S	T	U	X	Y	Z
12	16	1	13	17	5	19	14	18	6	9	22	21	



z,	nous	z	selon
a	nostre	a	sa majesté ou votre majesté
b	nest	b	tout
c	non	c	tant
d	ouverture	d	toutesfois
e	occasion	e	t st
f,	outre	f	vous
g	obligation	g	vostre
h	pour	h	venu
i	par	i	venant
l	pro	k	véritable
m	pacquet	l	vivs
n	que	m	
o	qui	n	
p	quoy	o	
q	quand	p	
r	quelle	Ù	
s	reçu	r	
t	réception	s	
Ù	reste	t	
x	sans	q	
y	sinon	x	

y	1,
z	2,
a	3,
b	4,
c	5,
d	6,
e	7,
f	8,
g	9,
h	10,
i	11,

Ce caractère Δ doublera son prochain précédent et cestuy ϒ ϕ l'annullera.

Chiffre des émigrés.	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
CHIFFRANT	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

CHANGEMENT POUR LES VOYELLES

a	22, 23, 24 ou 25
e	26, 27, 28 ou 29
i	30, 31, 32 ou 33
o	34, 35, 36 ou 37
u	38, 39, 40 ou 41

NOMS PROPRES

Anjou	aa	Harcourt (Duc d')	an	Régent (M. le)	bb
Argent	ab	Hector (Comte d')	ao	Reine (La)	bc
Arras (Evêque d')	ac	Hermann	ap	Roi (Le feu)	bd
Artois (Comte d')	ad	Hervilly (Comte d')	aq	Romanzow	be
Berlin	ae	Jaucourt (Marquis de)	ar	Russie	bf
Bretagne	af	Londres (Cour de)	as	Saintonge (La)	bg
Castries (M^{al} de)	ag	Louis XVII.	at	Serent (Duc de)	bh
Condé (Prince de)	ah	Marigny (Bernard de)	au	Serent (Vicomte de)	bi
Émigrés	ai	Marine	aw	Tours (Archevêque de)	bk
Flachslanden (Baron de)	ak	Normandie	ax	Vaugirard (De)	bl
Gaston	al	Paris	ay	Vienne	bm
Grenville (Lord)	am	Pitt	az	Woronzow	bn
		Poitou	ba		

DÉCHIFFRANT

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
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

CHANGEMENTS POUR LES VOYELLES

22, 23, 24 ou 25	A
26, 27, 28 ou 29	E
30, 31, 32 ou 33	I
34, 35, 36 ou 37	O
38, 39, 40 ou 41	U

NOMS PROPRES

aa	Anjou.
ab	Argent.
ac	Evêque d'Arras.
ad	Comte d'Artois.
ae	Berlin.
af	La Bretagne.
ag	Maréchal de Castries.
ah	Prince de Condé.
ai	Emigrés.
ak	Baron de Flachslanden.
al	Gaston.
am	Lord Grenville.
an	Duc d'Harcourt.
ao	Comte d'Hector.
ap	Hermann.
aq	Comte d'Hervilly.
ar	Marquis de Jaucourt.
as	Cour de Londres.
at	Louis XVII.
au	Bernard de Marigny.
aw	La marine.
ax	La Normandie.
ay	Paris.
az	M. Pitt.
ba	Le Poitou.
bb	Monsieur le Régent.
bc	La Reine.
bd	Le feu Roi.
be	M. de Romanzow.
bf	La Russie.
bg	La Saintonge.
bh	Duc de Serent.
bi	Vicomte de Serent.
bk	Archevêque de Tours.
bl	De Vaugirard.
bm	Vienne en Autriche.
bn	M. Woronzow.

Les chiffres du XVI^e^ siècle, comme le lecteur a pu s'en rendre compte, étaient établis de main de maître ; ils donnaient des cryptogrammes certes plus difficiles à déchiffrer que ceux des émigrés ou que ceux de M. D... (inculpé dans le complot de 1899), dont nous donnons ci-après l'alphabet astronomique et zodiacal, presque complet.

SIGNES ASTRONOMIQUES

Le Soleil	☉	A	La Terre	♁	F
Jupiter	♃	B	Vénus	♀	G
Saturne	♄	C	Mars	♂	H
Neptune	♆	D	Mercure	☿	I
Uranus	♅	E	La Lune	☾	J

SIGNES DU ZODIAQUE

Le Taureau	♉	K	Le Scorpion	♏	Q
Les Gémeaux	♊	L	Le Sagittaire	♐	R
Le Cancer	♋	M	Le Capricorne	♑	S
Le Lyon	♌	N	Les Poissons	♓	T
La Vierge	♍	O	Le Bélier	♈	U
La Balance	♎	P	Le Verseau	♒	V

W	X	Y	Z	
»	»	I	»	

NUMÉRATION

1	2	3	4	5	6	7	8	9	0
.	—	△	□	★	✡	✿	○	⊙	»

*
* *

Aux alphabets conventionnels ont aussi succédé, en même temps que le chiffrement mot par mot,

les méthodes de Porta, de Blaise de Vigenère, de l'amiral de Beaufort, etc., etc., connus sous le nom de *chiffres carrés*.

Ces chiffres ont conservé la réputation d'indéchiffrabilité pendant longtemps ; lorsqu'on a su que cette réputation était usurpée, quelques-uns ont perfectionné les procédés d'application, de manière à éviter le déchiffrement, d'autres ont cessé de s'en servir.

*
* *

La *Guerre* a alors imaginé et adopté la cryptographie par *transposition*.

Cette adoption, selon nous, est désastreuse.

C'est un danger public.

Dans le chapitre suivant le lecteur pourra juger du peu de valeur des *méthodes de transposition*, et peut-être réussirons-nous enfin à les faire abandonner à tout jamais.

CHAPITRE III

MÉTHODES DE TRANSPOSITION

Abandonner les méthodes de *substitution* pour celles de *transposition* a été changer son cheval borgne pour un aveugle. Dans les méthodes de *substitution*, fallait-il encore chercher la valeur des lettres ; dans celles de *transposition*, il n'y a pas à la chercher ; chaque lettre est en clair ; il n'y a qu'à chercher sa place. C'est relativement facile.

L'Etat-Major général français, en adoptant ces méthodes, a cru réaliser un progrès !... Il n'a fait que reculer.

*
* *

On a commencé à transposer avec un appareil carré composé de 10 réglettes mobiles : 400 nombres étaient gravés sur les réglettes. Ce cryptographe jouissait d'une réputation d'indéchiffrabilité absolue.

Lorsqu'on sut, à l'Etat-Major du XI[e] corps, qu'un

officier d'un corps de troupes, se basant sur la fixité des 400 nombres gravés sur les réglettes mobiles, avait émis l'avis que ce système pouvait se lire sans clef, ce fut un éclat de rire général.

Le général Fay, commandant le corps d'armée, à qui le fait fut raconté, au lieu de faire chorus avec les rieurs, mit l'officier à l'épreuve en lui faisant envoyer par son Etat-Major quelques cryptogrammes.

La traduction en fut faite ; on s'en émut à Nantes, on en rendit compte à Paris.

Peu de temps après, ces cryptographes à réglettes furent réformés, martelés et livrés au Domaine ; on adopta une méthode de transposition présentée par un officier du bureau..... *compétent* (?).

Cette dernière méthode fut déchiffrée avant d'être appliquée, c'est-à-dire que des cryptogrammes d'essai furent lus avant la date fixée pour l'application de la nouvelle méthode.

*
* *

On avait réalisé le rêve de l'Etat-Major : on avait fait de la cryptographie avec un crayon et du papier. Seulement on était lu, facilement même, quelquefois en moins d'une heure. Tout le monde le savait, du moins ceux qui avaient qualité pour en connaître.

Le lecteur se dira : du moment où le système est lu, on va l'abandonner et en adopter un autre qui ne puisse se lire sans clef.

Détrompe-toi, ami lecteur ! Tu es bien naïf ! Tu ne connais pas la vaillance des bureaux compétents !

Ce système dure encore, ou, tout au moins, était en usage à la *Guerre*, il n'y a pas bien longtemps.

Les déchiffrements, relatés ci-dessus, furent faits en 1890.

Il est heureux, que pendant cette longue période de temps, nous n'ayons pas eu de guerre, car qui sait les conséquences qu'aurait pu avoir un semblable désintéressement. Toutes les dépêches chiffrées, faites avec ce chiffre et interceptées, auraient été lues par l'ennemi en moins d'une heure de temps.

*
* *

Les méthodes de *transposition*, chères à la Guerre et adoptées officiellement, étaient tellement compliquées que les esprits superficiels avaient pris ces complications pour de l'indéchiffrabilité, alors que ce n'était que de l'enchevêtrement.

En un mot, c'était une salade des lettres du texte clair.

Pour lire, il s'agissait simplement de démêler cette salade.

De même qu'au moyen d'une roue aimantée on

peut, en un instant, trier le fer du cuivre dans un amas de vieilles ferrailles, de même, un cryptologue, en s'appuyant sur les particularités de la langue, peut remettre chaque lettre à sa place.

*
* *

Les esprits lents à saisir, ou peu patients, *possédant la clef*, s'ils venaient à commettre la moindre erreur, ne pouvaient plus venir à bout de faire le déchiffrement; il fallait des esprits alertes et surtout patients pour s'assimiler les subtilités de ces méthodes et pour pouvoir les appliquer.

*
* *

Des anecdotes nombreuses et variées sont à ce sujet connues de toute l'armée française. Nous en citerons une.

Un général commandant un corps d'armée reçut un télégramme chiffré en pleine nuit. Ne voulant pas déranger son Etat-Major, il essaya d'en faire le déchiffrement lui-même. Comme il avait omis un petit détail, il ne put en venir à bout et, après une heure de travail, il fut obligé d'envoyer chercher son chef d'Etat-Major pour savoir ce que lui voulait le Ministre.

*
* *

Et à quoi aboutissent ces subtilités, ces complications, ces mystères?

A un cryptogramme que le premier déchiffreur venu peut lire sans en avoir la clef et même sans connaître la méthode employée.

Nous disons premier déchiffreur venu, à dessein, parce que ce premier déchiffreur venu existe, et a toujours existé dans tous les pays du monde; qu'il soit célèbre ou obscur, il n'en existe pas moins et, du moment où il y en a un, il peut y en avoir d'autres.

*
* *

Nous racontons ces faits, simplement, tels qu'ils se sont passés. Nous croirions manquer à tous nos devoirs, si nous les passions sous silence ou si nous les déguisions.

CHAPITRE IV

LES DÉCHIFFREURS CÉLÈBRES

Les archives du XVI^e^ et du XVII^e^ siècle ont fait connaître quelques déchiffreurs ; il paraît intéressant de leur consacrer quelques lignes.

*
* *

Les plus célèbres sont : Viète sous Henri IV et Rossignol sous Louis XIII. Encore ce dernier serait-il oublié depuis longtemps si Perrault ne l'avait placé dans ses *Hommes illustres du* XVII^e^ *siècle* (t. I^er^).

Sous Louis XIV, on trouve comme déchiffreurs habiles : Vimbois et de la Tixeraudière.

Les auteurs cryptologues n'ont cité que Viète dans leurs ouvrages ; ils ignoraient les autres déchiffreurs. Et, comme ils n'ont fait qu'effleurer le sujet, il n'est pas inutile de compléter la notice sur Viète.

VIÈTE

Viète François, né à Fontenay-le-Comte, en 1540, mort en 1603, était un mathématicien déjà célèbre par ses travaux lorsqu'il fut chargé par Henri IV de déchiffrer quelques dépêches espagnoles interceptées par les troupes royales.

Après avoir appris en peu de temps les notions de langue espagnole, indispensables pour aboutir, il réussit à faire la traduction des dépêches interceptées.

* * *

Le chiffre espagnol, était à cette époque, constitué par un alphabet conventionnel composé de 99 nombres (1 à 99) et d'environ 40 signes. Les nombres représentaient une syllabe ; les signes, un mot ou une lettre.

De temps en temps l'alphabet changeait. Viète suivit ce chiffre dans ses variations pendant plusieurs années (1588 à 1594). Nous donnons à l'*Appendice* un des principaux déchiffrements faits par Viète, relatant les négociations du duc de Mayenne avec Philippe II, roi d'Espagne (Voir *Note I*).

*
* *

Viète suivait Henri IV dans ses voyages. Il ne garda pas toujours la discrétion dont il n'aurait pas dû se départir.

Étant à Tours, il bavarda avec l'ambassadeur de Venise, Giovanni Mocenigo ; il lui raconta qu'on avait intercepté un très grand nombre de lettres en chiffres, tant du roi d'Espagne que de l'Empereur et autres princes, et qu'il les avait déchiffrées et interprétées.

L'ambassadeur vénitien, en fin diplomate, se récria, disant que ce n'était pas possible, etc., etc. Viète, emballé, lui promit de lui donner des preuves de ce qu'il avançait ; il alla dans son appartement et en revint bientôt avec un gros paquet des lettres qu'il avait déchiffrées.

Ces chiffres ne concernaient pas la république vénitienne. L'ambassadeur tenait surtout à être fixé sur la valeur de résistance des chiffres de son pays. Comme Viète lui avait avoué comprendre et traduire aussi son chiffre : « Je ne veux pas le croire, lui dit-il, à moins que je ne le voie. »

Mais Viète lui prouva qu'il comprenait un de ses chiffres, et qu'il ne possédait l'autre qu'en partie.

L'ambassadeur, rentré à Venise, fit part de ces faits au Conseil des Dix, dans sa séance du 5 juin 1595.

Sept jours après, le 12 du même mois, tout le service des chiffres des ambassadeurs de la République était changé. On avait adopté les inventions nouvelles du plus habile cryptologue de l'époque, Pietro Partenio[1] (Voir *Notes II* et *III*).

Les Vénitiens étaient gens pratiques.

La cour d'Espagne ne trouva, comme remède, qu'une plainte au Pape, accusant la France d'avoir le diable et des sorciers à ses gages.

Heureusement pour lui, Viète était soutenu par un monarque puissant; sans quoi, il aurait payé cher ses indiscrétions. Jugé comme magicien, on l'aurait infailliblement condamné à être brûlé vif.

*
* *

Viète participa aux affaires publiques comme maître des requêtes.

On trouve à la Bibliothèque de la Sorbonne les *Ouvrages de Viète*, par François Schooten, professeur de mathématiques à Leyde, aidé de J. Golius et du P. Mersenne (Leyde, 1646).

Les principaux déchiffrements faits par Viète sont à la Bibliothèque Nationale (Département des Manuscrits. Les 500 de Colbert).

[1] *Les Archives de Venise*, Paris. Henri Plon, 1870. — Armand Baschet, *Histoire de la Chancellerie secrète*.

ROSSIGNOL

Rossignol est né à Albi en 1590, d'après Avenel (t. Ier, p. xxii des *Documents inédits sur l'histoire de France*) et, en 1600, d'après Perrault (*les Hommes illustres pendant le* XVIIe *siècle*, t. Ier).

Rossignol se fit connaître comme déchiffreur, en 1626, dans les circonstances suivantes :

Le prince de Condé assiégeait Réalmont, en Languedoc. On intercepta une lettre chiffrée que les habitants de Réalmont envoyaient à Montauban.

On parla au prince de Condé de Rossignol, qui jouissait, dans cette partie de la France, d'une certaine réputation d'habilité comme déchiffreur. Le prince l'envoya chercher, et Rossignol déchiffra facilement le cryptogramme.

Il était très important :

Les habitants de Réalmont mandaient, à Montauban, que, si on ne venait pas les secourir sous peu, ils seraient obligés de se rendre, étant dans une grande détresse et manquant de tout.

Le prince de Condé envoya la traduction de cette lettre à Réalmont. Les notables s'assemblèrent, crurent que le diable était avec les troupes royales, et décidèrent d'ouvrir leurs portes et de se rendre.

*
* *

Rossignol serait resté en Languedoc, obscur et oublié, si, au siège de la Rochelle, l'année suivante, on n'avait intercepté des lettres chiffrées des Rochelais.

Richelieu, qui en avait vainement demandé la traduction aux employés du chiffre, en parla dans son entourage. Le prince de Condé se souvint alors de Rossignol et raconta au cardinal ce qui lui était arrivé à Réalmont, l'année précédente.

Richelieu ne perdit pas de temps, fit venir Rossignol et lui soumit les lettres interceptées. Celui-ci les déchiffra.

Richelieu attacha Rossignol à son service d'une manière définitive.

*
* *

Tallement des Réaux prétend que Rossignol n'a trouvé qu'un seul chiffre, et que Richelieu exagéra son talent dans le but de décourager les conspirateurs, nombreux à l'époque, et de leur faire peur.

Rossignol, plus discret que Viète, ne se vantait point de ses travaux. Ce qu'il y a de certain, c'est qu'il créa un véritable service de déchiffrement, qui fonctionna après lui, et dont nous trouverons des traces plus loin.

L'habileté de Rossignol, dans l'art du déchiffrement était si notoire qu'il y a lieu de supposer que c'est son nom qui a été donné à l'instrument qui sert à ouvrir les serrures dont on a perdu la clef. Ceci seul serait un hommage rendu à sa capacité, et certainement Tallement des Réaux n'est pas dans le vrai, lorsqu'il soutient que Rossignol n'a jamais découvert qu'un seul chiffre.

* * *

C'est pendant le séjour de Rossignol aux affaires de chiffres qu'un changement complet et radical s'est effectué dans les méthodes cryptographiques.

Au chiffrement lettre par lettre, il substitue le chiffrement mot par mot, au moyen de deux tables : l'une appelée : table du chiffre à chiffrer dans laquelle les lettres, syllabes et mots étaient rangés par ordre alphabétique, avec, en regard, un nombre pour les représenter ; l'autre appelée : table du chiffre à déchiffrer, dans laquelle les nombres étaient rangés par ordre numérique, avec, en regard, le mot, syllabe ou lettre, qu'ils représentaient.

* * *

On peut dire que c'est Rossignol qui a créé les chiffres diplomatiques en usage de nos jours.

Evidemment, à cette époque, les chiffres étaient moins riches qu'aujourd'hui. Ils ne se composaient que de quelques centaines de groupes et étaient forcément syllabiques. Ils pouvaient passer pour aussi sûrs que ceux de nos jours, qui possèdent quelques milliers de groupes.

En effet les déchiffreurs de l'époque ne pouvaient essayer le déchiffrement que sur les lettres interceptées ou saisies, tandis que, de nos jours, l'usage du télégraphe livre aux Gouvernements étrangers des textes chiffrés en telle abondance qu'un chiffre du genre de ceux inaugurés par Rossignol ne résisterait pas longtemps aux recherches des cryptologues.

Il est vrai qu'au bon xvii[e] siècle on avait la ressource de décacheter les paquets confiés à la poste et qu'à une certaine époque on ne s'en fit pas faute, comme l'attestent de nombreux documents.

*
* *

Les services de Rossignol furent si bien appréciés que Louis XIII le recommanda à Anne d'Autriche.

Il servit sous Mazarin, devint Maître des comptes et s'éleva à une brillante fortune. Anobli seigneur de Juvisy, il reçut dans son château de Juvisy la visite de Louis XIV. Il mourut en 1673.

*
* *

On n'a pu trouver, dans les différents dépôts d'archives, aucun des déchiffrements faits par le seigneur de Juvisy.

AUTRES DÉCHIFFREURS

Après Rossignol, les déchiffreurs sont peu connus ; mais le service qu'il créa n'en fut pas moins très utile à l'Etat.

On en trouve la preuve dans différents documents.

*
* *

Saint-Simon, à l'occasion de la mort du fils de Rossignol, président aux Requêtes du Palais, dit qu'aucun chiffre ne lui échappait; il y en avait même qu'il lisait de suite.

M. de Louvois, toujours d'après Saint-Simon, aurait connu Rossignol fils et l'aurait employé comme déchiffreur.

*
* *

En 1673, on trouve deux déchiffreurs officiels, Vimbois et de La Tixeraudière.

On n'a sur eux aucune notice bibliographique. C'est le dépôt de la Guerre qui les dévoile[1].

On relève, dans une lettre de Louvois à Carpatry, datée du camp sous Maestricht, le 2 juillet 1673 : « Faites donner 200 écus à Vimbois par gratifica- « tion, pour avoir trouvé le chiffre. » Et dans une autre lettre du même au même, datée du Camp près Vizor, le 6 juillet 1673 : « Il faut faire donner au « sieur de La Tixeraudière 600 livres par gratifica- « tion pour avoir trouvé ce chiffre, et ce afin qu'une « autre fois, il soye plus ardent et plus diligent « à y travailler. »

En rapprochant ces deux dates, 2 et 6 juillet 1673, on peut conclure qu'il y avait un bureau de déchiffrement organisé, et que les employés n'y chômaient pas.

Ces deux lettres de Louvois à Carpatry montrent en même temps que les déchiffreurs de cette époque étaient royalement rémunérés.

[1] Dépôt de la Guerre, vol. 305, p. 27 et 69.

DÉCHIFFREURS INCONNUS

Vimbois et de La Tixeraudière avaient sans doute fait des élèves, car dix-huit ans après, comme le prouve la lettre suivante, existant aux Archives Nationales, il y avait à Paris, près du Roy, des gens habiles dans l'art du déchiffrement.

14 juillet 1691. — A Mr Bégon[1] : « Les Srs de Court « et Coderey m'ont escrit que le Me d'Ecole qui a « été arresté a esté fort interdit, lorsqu'on l'a « pressé de déchiffrer quatre lignes de chiffres qui « se sont trouvées dans une de ses lettres.

« Prenez la peine de m'envoyer copie figurée « de ce qui est en chiffres et copie de l'alphabet « de chiffres qui luy a esté repincé. J'ay icy des « gens qui le déchifreront en un moment. »

A la date du 16 juillet 1691[2], on trouve un ordre du roi pour tirer des prisons de la Rochelle le nommé Folluisse, maître d'école, et sa femme, et les conduire sous « bonne et seure garde en prisons royales de Poictiers. »

Le maître d'école Folluisse avait ouvert un pensionnat dans un village, près de la Rochelle, et il

[1] Archives Nationales, O[1], vol. 35, f° 202.
[2] Archives Nationales, O[1], vol. 35, f° 203.

instruisait ses pensionnaires dans la religion protestante. C'était son seul crime; il suffisait, à l'époque, pour être l'hôte du grand roi en ses prisons royales de Poitiers.

DÉCHIFFREURS MODERNES

Les recherches faites dans les différents dépôts d'archives n'ont pas fait connaître de noms pour la période comprise entre les règnes de Louis XIV et de Napoléon Ier.

FIN DE LA PREMIÈRE PARTIE

DEUXIÈME PARTIE

ÉTUDE SUR LE CHIFFRE CARRÉ DICTIONNAIRES CHIFFRÉS

CHAPITRE PREMIER

DES PRINCIPALES MÉTHODES

Le *chiffre carré* s'obtient en dénaturant les lettres du texte clair, une par une, au moyen d'un tableau et d'une clef.

* * *

C'est avec ce chiffre qu'étaient faites les dépêches secrètes envoyées par ou au duc d'Orléans et qui ont été versées aux débats de la Haute-Cour de Justice (1899).

Ce chiffre est classique en cryptographie. On l'appelle aussi chiffre de Vigenère[1] et chiffre de Beaufort[2], selon la méthode employée.

[1] Blaise de Vigenère, diplomate français (1586).
[2] Francis de Beaufort, amiral anglais (1857).

*
* *

Tableau cryptographique. — Le tableau dont se servait le duc d'Orléans est reproduit ci-contre.

Ce tableau s'appelle, en cryptographie, tableau de Beaufort.

Il présente une légère différence avec le tableau de Vigenère.

Cette différence consiste dans la répétition de la première colonne horizontale et de la première colonne verticale.

*
* *

Vigenère répète ces deux colonnes au commencement de son tableau ; Beaufort les répète à la fin du sien.

Il résulte de ce qui vient d'être expliqué que, dans le tableau de Vigenère, la première et la deuxième colonne horizontales sont identiques, de même que la première et la deuxième colonne verticales, alors que, dans le tableau de Beaufort, les colonnes identiques sont, aussi bien horizontalement que verticalement, la première et la dernière.

*
* *

L'explication des nombres de 11 à 37, qui figurent sur le tableau du duc d'Orléans au-dessus du premier alphabet horizontal est donnée au chapitre v.

11	12 13	14 15	16 17	18 19	20 21	22 23	24 25	26 27	28 29	30 31	32 33	34 35	6 37
A	B C	D E	F G	H I	J K	L M	N O	P Q	R S	T U	V W	X Y	Z A
B	C D	E F	G H	I J	K L	M N	O P	Q R	S T	U V	W X	Y Z	A B
C	D E	F G	H I	J K	L M	N O	P Q	R S	T U	V W	X Y	Z A	B C
D	E F	G H	I J	K L	M N	O P	Q R	S T	U V	W X	Y Z	A B	C D
E	F G	H I	J K	L M	N O	P Q	R S	T U	V W	X Y	Z A	B C	D E
F	G H	I J	K L	M N	O P	Q R	S T	U V	W X	Y Z	A B	C D	E F
G	H I	J K	L M	N O	P Q	R S	T U	V W	X Y	Z A	B C	D E	F G
H	I J	K L	M N	O P	Q R	S T	U V	W X	Y Z	A B	C D	E F	G H
I	J K	L M	N O	P Q	R S	T U	V W	X Y	Z A	B C	D E	F G	H I
J	K L	M N	O P	Q R	S T	U V	W X	Y Z	A B	C D	E F	G H	I J
K	L M	N O	P Q	R S	T U	V W	X Y	Z A	B C	D E	F G	H I	J K
L	M N	O P	Q R	S T	U V	W X	Y Z	A B	C D	E F	G H	I J	K L
M	N O	P Q	R S	T U	V W	X Y	Z A	B C	D E	F G	H I	J K	L M
N	O P	Q R	S T	U V	W X	Y Z	A B	C D	E F	G H	I J	K L	M N
O	P Q	R S	T U	V W	X Y	Z A	B C	D E	F G	H I	J K	L M	N O
P	Q R	S T	U V	W X	Y Z	A B	C D	E F	G H	I J	K L	M N	O P
Q	R S	T U	V W	X Y	Z A	B C	D E	F G	H I	J K	L M	N O	P Q
R	S T	U V	W X	Y Z	A B	C D	E F	G H	I J	K L	M N	O P	Q R
S	T U	V W	X Y	Z A	B C	D E	F G	H I	J K	L M	N O	P Q	R S
T	U V	W X	Y Z	A B	C D	E F	G H	I J	K L	M N	O P	Q R	S T
U	V W	X Y	Z A	B C	D E	F G	H I	J K	L M	N O	P Q	R S	T U
V	W X	Y Z	A B	C D	E F	G H	I J	K L	M N	O P	Q R	S T	U V
W	X Y	Z A	B C	D E	F G	H I	J K	L M	N O	P Q	R S	T U	V W
X	Y Z	A B	C D	E F	G H	I J	K L	M N	O P	Q R	S T	U V	W X
Y	Z A	B C	D E	F G	H I	J K	L M	N O	P Q	R S	T U	V W	X Y
Z	A B	C D	E F	G H	I J	K L	M N	O P	Q R	S T	U V	W X	Y Z
A	B C	D E	F G	H I	J K	L M	N O	P Q	R S	T U	V W	X Y	Z A

*
* *

De même que le tableau, la manière de chiffrer diffère dans les méthodes de Vigenère et de Beaufort.

Vigenère trouve son chiffre dans le corps du tableau, à la rencontre de deux colonnes, l'une horizontale, l'autre verticale ; Beaufort trouve le sien à l'extrémité d'une ligne soit horizontale, soit verticale.

*
* *

Que l'on cryptographie la lettre du texte clair avec la lettre de la clef ou cette dernière avec la lettre du texte clair, on n'obtient qu'un seul chiffre par la méthode de Vigenère, alors que l'on en obtient deux, différents, avec la méthode de Beaufort.

Ces deux derniers chiffres sont complémentaires l'un de l'autre. On explique cette particularité à l'*Appendice* (Voir *Note IV*).

*
* *

On peut donc obtenir trois chiffres différents avec un tableau de Vigenère ou de Beaufort.

L'exemple suivant le fera mieux ressortir.

Soit à chiffrer le mot : *bien*, avec la clef : *vive*.

Méthode de Vigenère	Clef en dessous.	Clef en dessus.
	B I E N	V I V E
	V I V E	B I E N
Chiffre (rencontre de 2 colonnes)	WQ Z R	W Q Z R
Méthode de Beaufort	B I E N	V I V E
Chiffre (extrémité d'une colonne,	V I V E	B I E N
soit horizontale, soit verticale).	U A R R	G A J J

Comme on le voit, WQZR — UARR — GAJJ représentent le mot : bien, chiffré avec la clef : vive.

CHAPITRE II

PROCÉDÉS DE DÉCHIFFREMENT DÉCRITS PAR LES AUTEURS CONTEMPORAINS

On va maintenant examiner les procédés de déchiffrement indiqués par les principaux auteurs cryptologues, qui, dans ces dernières années, ont étudié le chiffre carré.

Procédons par ordre chronologique.

KASISKI

1863, Berlin. *Die geheimschriften und die Dechiffrirkunst.* Kasiski, major allemand.

C'est Kasiski qui, le premier, a démontré que le chiffre carré pouvait mathématiquement être lu sans clef.

Nous devons à l'obligeance du capitaine Valerio un extrait de *Die geheimschriften und die Dechiffrirkunst* von F. W. Kasiski, major Z. D.

Voici cet extrait :

« §§ 76. — Il arrive souvent que des répétitions « de deux ou plusieurs lettres au clair seront, « dans le chiffrement, liées aux mêmes lettres de « la clef ; il s'ensuivra que, dans le cryptogramme, « apparaîtront également des répétitions de deux « ou plusieurs chiffres.

« Réciproquement on pourra conclure que les « répétitions de deux ou plusieurs chiffres dans le « cryptogramme sont nées de répétitions analogues « du clair chiffrées avec les mêmes lettres de la « clef.

« §§ 78. — La dépêche chiffrée est-elle compo- « sée avec un ou plusieurs alphabets ? Pour s'en « rendre compte, il est nécessaire de procéder à un « examen attentif, car un coup d'œil superficiel ne « permet pas d'apercevoir la différence.

« Dans le chiffrement simple, les répétitions « sont fréquentes et seulement accidentelles ; les « intervalles qui les séparent sont, par suite, rare- « ment réguliers ; dans le chiffrement composé, au « contraire, ces répétitions sont moins fréquentes ; « elles se présentent habituellement à des inter- « valles tels que le nombre de lettres d'un inter- « valle est divisible par le nombre de lettres de la « clef.

*
* *

M. Kasiski parle d'examen attentif pour déterminer si la dépêche chiffrée a été composée avec un ou avec plusieurs alphabets.

L'examen attentif ne suffit pas, il faut enregistrer les lettres, et c'est cet enregistrement qui permet de déterminer sûrement, par l'ordre de fréquence et par les répétitions, si l'on se trouve en présence d'un chiffre fait avec un seul alphabet, ou d'un chiffre fait avec plusieurs.

KERCKHOFFS

1883, Paris. *La Cryptographie militaire*, ou *Des chiffres usités en temps de guerre*. Auguste Kerckhoffs, docteur ès lettres (L. Baudoin).

Brochure de 64 pages. — M. Kerckhoffs classe les différents systèmes d'écriture secrète en trois méthodes principales :

1° La méthode qui se borne à une simple transposition des lettres du texte en clair ;

2° Celle qui fait reposer la combinaison du chiffre sur une interversion de l'ordre alphabétique des lettres ;

3° Celle qui représente les syllabes, les mots, ou même des phrases entières par des nombres ou des groupes de lettres.

*
* *

Résumer la brochure de M. Auguste Kerckhoffs est assez difficile. Tout ou presque tout est à retenir dans cette étude extrêmement bien faite. De nombreux renseignements bibliographiques permettent de remonter aux sources. Toutes les méthodes connues en 1883 y sont l'objet d'une description détaillée.

*
* *

Limitant cette étude aux chiffres *carré* et *militaire*, nous allons énumérer les différentes méthodes décrites par M. Kerckhoffs, et qu'il appelle des systèmes à double clef :

Système de Porta ; — Chiffre carré de Vigenère ; — Système de Saint-Cyr ; — Système de Beaufort ; — Système de Gronsfeld ; — Système à clef variable.

Ce dernier système a été imaginé par un membre de la Commission de télégraphie militaire, dont M. Kerckhoffs n'a pas donné le nom ; mais un cryptogramme composé d'après ce système a été lu en moins de deux heures par M. Kerckhoffs.

Pour toutes les méthodes, M. Kerckhoffs indique les procédés de déchiffrement ; il a prouvé que le chiffrement par la méthode de Beaufort était exactement le même que celui obtenu par les méthodes

de Vigenère et de Saint-Cyr, en retournant tout simplement l'alphabet normal dans ces deux méthodes ou en mettant en nombre carré :

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

*
* *

La réciproque aussi se trouve vraie, c'est-à-dire que le chiffrement obtenu par les méthodes de Vigenère et de Saint-Cyr est identiquement le même que celui obtenu en chiffrant d'après la méthode de Beaufort, si on fait usage, pour chiffrer, d'une table, où l'alphabet sera retourné dans toutes les colonnes verticales.

*
* *

Citons M. Kerckhoffs :

Page 35 : « Le déchiffrement d'un cryptogramme « dont on n'a pas la clef comporte un calcul de « probabilité et un travail de tâtonnement. Dans « le système à double clef, il s'agit de trouver deux « inconnues : 1° le nombre des alphabets ; 2° leur « disposition respective. »

*
* *

Pour le nombre des alphabets, il est facile de le déterminer, s'il s'est produit des répétitions; mais

si la clef, par sa longueur, empêche les répétitions de se produire, il faut renoncer à trouver la longueur de la clef et, par suite, le nombre d'alphabets employés. Les répétitions qui existent dans ce dernier cas sont fortuites et accidentelles; elles ne peuvent que dérouter un déchiffreur et l'induire en erreur.

*
* *

Page 37 : « Les alphabets peuvent être ordonnés de trois manières différentes :

« 1° Ou bien les lettres se suivent dans l'ordre « de l'alphabet normal, comme dans le tableau de « Vigenère ;

« 2° Ou bien cet ordre est interverti d'une façon « quelconque, mais les vingt-six alphabets n'en « sont pas moins disposés en nombre carré ;

« 3° Ou bien encore les vingt-six lettres sont pla- « cées dans un ordre différent dans chacun des « vingt-six alphabets.

« Le déchiffreur n'a généralement aucune peine « à constater laquelle de ces trois dispositions a été « adoptée. »

*
* *

Ce n'est que par l'essai de déchiffrement que l'on peut déterminer laquelle de ces trois dispositions a été adoptée. Si c'est la première, le déchiffrement

se fait avec aisance ; mais, si c'est une des deux dernières, c'est moins facile. On peut y arriver, mais on a à vaincre des difficultés presque insurmontables. Il faut reconstituer le tableau interverti pour pouvoir aboutir, et, malgré toute l'ingéniosité de la théorie sur la *symétrie de position*, on serait certainement impuissant, si on se trouvait en présence de dépêches fort courtes et faites avec des clefs différentes.

JOSSE

1885, Paris. *La cryptographie et ses applications à l'art militaire.* H. Josse, capitaine en premier, breveté d'artillerie (L. Baudoin).

Livre de 103 pages. — Comme son titre l'indique, c'est surtout la cryptographie militaire qui y est traitée.

Il y a d'excellentes choses dans ce livre; malheureusement, après un exposé logique, survient une hérésie cryptographique qui en détruit ou, tout au moins, en fausse la valeur.

*
* *

M. H. Josse divise les principaux systèmes cryptographiques en quatre grandes catégories :

1° Systèmes dont l'emploi n'exige ni livres, ni appareils;

2° Appareils;

3° Livres, tables ou dictionnaires chiffrés. Langage convenu;

4° Systèmes exceptionnels ne rentrant dans aucune des trois premières catégories.

Il classe les systèmes de la première catégorie (ni livres, ni appareils) en quatre groupes principaux. Au quatrième groupe, figure la méthode du chiffre carré et ses dérivés.

Remarquons, en passant, que cette méthode exige généralement un tableau.

Or, en cryptographie, un *tableau* est tout aussi bien un *appareil* qu'un instrument quelconque, car ce tableau, le cryptologue doit le porter sur lui, s'il veut opérer rapidement.

*
* *

Indépendamment des méthodes exposées par M. Kerckhoffs, M. H. Josse donne celles ci-après :

Méthode allemande, du capitaine Hirsh des Hohenzollernschen Fusilier regiments, n° 40. Cologne, 1884;

Méthode Auvray, imaginée en 1870, par un commis principal de première classe, au Ministère de la Marine et des Colonies;

Méthode Delaunay, imaginée en 1884 par un capitaine d'artillerie, et modifiée par M. H. Josse lui-même, de manière à en augmenter la sécurité ;

Enfin, méthode de Saint-Cyr, modifiée par un membre de la Commission de télégraphie militaire dont le nom n'est pas indiqué.

Quant aux procédés de déchiffrement pour le chiffre carré, M. H. Josse n'en indique aucun d'original ; il se borne à commenter M. Kerckhoffs.

*
* *

Nous allons signaler les hérésies cryptographiques dont nous venons de parler, et qui, d'après nous, abondent dans *la Cryptographie et ses applications à l'art militaire.*

Le lecteur jugera. Citons M. H. Josse.

Page 11 :

« Qualités que doit posséder un déchiffreur : .....
« Il doit posséder enfin une aptitude spéciale, une
« sorte de *flair*, lui permettant de limiter ses
« recherches et de s'engager rapidement dans la
« bonne voie. »

*
* *

Flair est en italique dans le texte.

Pour limiter les recherches, le flair ne suffit pas (serait-il même d'artilleur).

On ne peut obtenir ce résultat que par la décomposition rationnelle et complète du cryptogramme. C'est une opération souvent fort longue et fastidieuse; si on veut aboutir, il faut commencer par là; c'est indispensable. Une fois cette décomposition faite, le flair peut s'exercer, mais pas avant.

*
* *

Page 12:

« Le déchiffreur doit... posséder des notions « étendues en philologie comparée, connaître à « fond sa propre langue, puis l'histoire, la géogra- « phie, la littérature ancienne et moderne, » etc.

*
* *

On avoue ne pas saisir en quoi la philologie comparée, l'histoire, la géographie, les littératures ancienne et moderne, peuvent permettre à celui qui les possède d'être déchiffreur.

Aujourd'hui toutes ces connaissances sont, pour ainsi dire, dans le domaine public: officiers, magistrats, notaires, avocats, etc., les possèdent. On ne pense pas que cela les qualifie pour être déchiffreurs.

*
* *

Page 12 :

« Renseignements préliminaires que doit se pro-
« curer un déchiffreur : Dans les circonstances im-
« portantes, on ne doit rien négliger pour obtenir
« d'une manière quelconque la connaissance de la
« clef ou, tout au moins, du procédé employé pour
« écrire la dépêche. »

*
* *

Si, d'une manière quelconque, on a eu connaissance de la clef, ou du procédé employé, le déchiffreur n'a pas à intervenir, c'est affaire aux employés du chiffre.

Le déchiffreur est utile pour déterminer d'abord le procédé employé, et, une fois cette détermination faite, pour rechercher la clef et faire la traduction.

La décomposition du cryptogramme, dont il a été parlé plus haut, suffit généralement pour obtenir ce triple résultat.

*
* *

Page 13 :

« Ne pas oublier qu'il est toujours plus difficile
« de déchiffrer un cryptogramme court qu'un cryp-
« togramme long (sauf le cas d'emploi des méthodes
« de transposition). »

*
* *

Ceci n'est pas tout à fait exact.

Evidemment un cryptogramme long donne plus de prise au calcul pour déterminer la longueur de la clef, mais aussi un cryptogramme court limite les recherches du déchiffreur, et celui-ci traduit pour ainsi dire d'assaut.

*
* *

Page 96 :

« La cryptographie militaire prend donc une « importance que nous n'hésitons pas à qualifier « de capitale.

« Il faut remarquer, d'ailleurs, que l'on ne peut « compter que sur elle pour donner un caractère « d'*authenticité* à une dépêche envoyée par le télé- « graphe.

« Les progrès de la science permettent aujour- « d'hui à un ennemi entreprenant de greffer en « quelque sorte sur une ligne télégraphique, utili- « sée par une armée en campagne ou une place « forte assiégée, une ligne secondaire, au moyen de « laquelle il pourra non seulement avoir connais- « sance des dépêches échangées, mais encore lan- « cer des dépêches fausses[1].

[1] « Cela a été déjà pratiqué plusieurs fois avec succès en Amérique, pendant la guerre de Sécession. »

*
* *

Authenticité est en italique dans le texte de M. H. Josse.

On a répondu par ailleurs[1], et voici cette réponse :

Quelle erreur profonde ! Il sera on ne peut plus facile à l'ennemi, alors qu'il aura reconstitué votre chiffre, ou qu'il en aura retrouvé la clef, de vous faire parvenir des dépêches chiffrées.

Vous croirez qu'elles émanent du Gouvernement français, ou du généralissime, parce qu'elles seront faites avec votre chiffre ? C'est bien naïf !

*
* *

Page 99, M. H. Josse énumère les desiderata de la cryptographie militaire, qui avaient déjà été magistralement décrits par M. Kerckhoffs, et résumés sous les six chefs ci-après :

« 1° Le système doit être matériellement, sinon « mathématiquement, indéchiffrable ;

« 2° Il faut qu'il n'exige pas le secret, et qu'il puisse « sans inconvénient tomber entre les mains de « l'ennemi ;

[1] *Les chiffres de Napoléon Ier pendant la Campagne de* 1813. Fontainebleau, Maurice Bourges, 1896. — Page 55.

« 3° La clef doit pouvoir en être communiquée et « retenue sans le secours de notes écrites, et être « changée ou modifiée au gré des correspondants;

« 4° Il faut qu'il soit applicable à la correspon- « dance télégraphique;

« 5° Il faut qu'il soit portatif, et que son manie- « ment ou que son fonctionnement n'exige pas le « concours de plusieurs personnes;

« 6° Enfin il est nécessaire, vu les circonstances « qui en commandent l'application, que le système « soit d'un usage facile, ne demandant ni tension « d'esprit, ni la connaissance d'une longue série de « règles à observer. »

A ces desiderata M. H. Josse ajoute une septième condition :

« Il faut que le système ne comporte pas l'emploi « d'un livre ou d'un appareil. »

Cette septième condition détruit toute l'économie des desiderata de M. Kerckhoffs et amène à la conclusion forcée : « La cryptographie militaire, « proprement dite, doit employer un système n'exi- « geant qu'un crayon et du papier. »

*
* *

Déclarons hautement que vouloir obtenir une méthode pratique et sûre avec un crayon et du papier est chose matériellement impossible.

C'est s'exposer de gaîté de cœur à voir lire par l'ennemi tous les cryptogrammes qu'il interceptera.

Réagissons contre des théories aussi fausses et aussi dangereuses ; détrônons toutes les hérésies cryptographiques qui s'étaient implantées jusque dans l'*Aide-mémoire de l'officier d'Etat-Major en campagne* (édition de 1890). Les desiderata de la cryptographie, en général, et de la cryptographie militaire, en particulier, devraient se renfermer dans les trois conditions suivantes :

1° Indéchiffrabilité absolue ;

2° Simplicité et rapidité ;

3° Non-nécessité du secret.

*
* *

Page 100 :

« D'ailleurs un changement fréquent de *clef* est « le plus sûr moyen d'assurer le secret de la corres- « pondance. »

*
* *

Il a déjà été répondu à ce sujet[1] ; et voici la réponse faite.

Un changement fréquent de clef ne peut rendre bon un système défectueux ; en outre de la perturbation qu'il apporte dans le service, l'inconvénient

[1] *Les Chiffres de Napoléon Ier. — Loc. cit.*, p. 54.

le plus grave, à notre avis, est que, si les changements de clef sont fréquents, il faut, pour se les rappeler, les écrire, et l'on dit, avec raison d'ailleurs, que toute clef écrite est une clef livrée.

Ces changements n'offrent que des inconvénients et aucun avantage. On aura beau changer de clef, on n'empêchera point le déchiffrement sans clef de se faire, si le système adopté permet ce déchiffrement.

* * *

Pages 100 et 101 :

« Nombre de systèmes cryptographiques à em-
« ployer simultanément : M. le général Lewal a
« défini très nettement les besoins de la cryptogra-
« phie militaire : « Il faut, dit-il dans sa *Tactique*
« *des renseignements :*

« *Un chiffre personnel* pour le commandant en
« chef, seul ;

« *Un chiffre spécial* pour les commandants de
« corps d'armée ou de division de cavalerie ;

« *Un chiffre général* pour toutes les unités : divi-
« sions, brigades, régiments et chefs de service ;

« *Un chiffre particulier* pour les officiers d'un
« même régiment.

« Ces quatre chiffres ne présentent qu'une com-
« plication apparente : en réalité, chaque unité n'en
« possède que deux. Au grand quartier général, on

« doit cependant avoir tous les chiffres employés par « l'armée.

« Le chiffre *spécial*, le chiffre *général* et le chiffre « *particulier* peuvent d'ailleurs appartenir au même « système cryptographique, employé avec une ou « plusieurs *clefs* différentes dans chaque cas.

« Enfin, il faudra se ménager la possibilité de « changer de système, si l'on s'apercevait que « l'ennemi en a obtenu connaissance. »

* * *

Tout ceci est fort bien dit; mais quatre chiffres sont-ils indispensables? Voyez-vous le grand quartier général possédant le chiffre *particulier* aux officiers d'un même régiment? Il est vrai que ce chiffre appartenant au même système cryptographique que ceux *spécial* et *général*, il ne serait nécessaire que d'en posséder les clefs.

Mais que de clefs! au moins 250!

Est-ce bien utile?

Quelle nécessité, pour un officier d'un régiment, qui marche avec son chef, d'avoir un chiffre?

Et puis, la précaution, bonne, de se ménager la possibilité de changer de système en cas de surprise, ne nécessite-t-elle pas un autre recueil de 250 nouvelles clefs et d'un système différent?

*
* *

Nos ancêtres étaient sages,
Respectons tous leurs usages;

dit la chanson. Louis XIV, Napoléon Ier, pour ne citer que les plus illustres, se contentaient de deux chiffres :

Un grand chiffre pour le souverain ;

Un petit chiffre pour les sous-ordres.

De plus, Louis XIV avait une bonne précaution : il tenait en réserve, sous pli cacheté, un chiffre neuf de rechange [1].

Napoléon Ier avait négligé cette excellente précaution. Aussi, en 1813, lorsque le général Jomini, chef d'Etat-Major du prince de la Moskova, aigri par une série de passe-droits que lui faisait Berthier, passa à l'ennemi, il fallut changer de chiffre, et ce changement apporta quelques retards dans l'exécution d'ordres importants de l'Empereur [2].

*
* *

La précaution du chiffre neuf, de rechange, sous pli cacheté, a, paraît-il, été reprise en ces derniers temps.

[1] *Le Masque de fer*, Paris, 1893, p. 171. Firmin-Didot.
[2] *Les Chiffres de Napoléon Ier*, p. 31.

Un bon point pour cette décision; mais cela ne suffit peut-être pas; il faudrait que le système adopté fût bon, et on est en droit de craindre, vu les désintéressements que nous avons signalés, vu les idées erronées qui ont cours en haut lieu, etc., qu'il n'en soit point ainsi.

Il serait à souhaiter que nous nous trompions et que nos craintes ne soient point fondées!

VIARIS

1888, Paris. *Cryptographie.* Marquis de Viaris, ancien officier de Marine, ancien élève de l'Ecole Polytechnique.

Publications du Génie civil.

Livre de 80 pages.

M. de Viaris classe les méthodes en trois catégories :

Méthodes à alphabets;

Méthodes à anagrammes;

Méthodes à répertoire.

*
* *

Pour le chiffre carré, après une longue discussion scientifique, il appuie sur le dispositif de la clef, et il donne l'équation cryptographique. Il

arrive à trouver quatre chiffres différents pour un même texte, soit que l'on opère d'après Vigenère ou d'après Beaufort. Trois de ces chiffres sont donnés par le tableau cryptographique; le quatrième est donné par le calcul.

Il conclut à un dispositif autoclave pour assurer la sécurité, et il ne pense pas que les alphabets intervertis aient une valeur théorique supérieure à celle des alphabets normaux.

*
* *

En 1893, M. de Viaris a publié une nouvelle étude cryptographique : *L'art de chiffrer et déchiffrer les dépêches secrètes*. Gauthier-Villars et fils.

Livre de 175 pages.

A la page 27, M. de Viaris dit : « Dans toute « phrase française, sur cinq lettres environ on ren- « contre un E. »

Cette indication ne concorde pas avec la décomposition qu'il a faite de 80.223 lettres recueillies dans le numéro du *Temps* du 2 mars 1891.

Il n'a, en effet, rencontré sur ce nombre que 13.884 E (p. 86).

C'est donc sur six lettres environ et non sur cinq qu'on rencontre un E.

En effet 80.223 : 6 = 13.370;

Tandis que 80.223 : 5 = 16.044.

Le lecteur peut constater *de visu* que 13.370 est bien plus rapproché de 13.884 que 16.044.

*
* *

Comme *chiffre carré*, M. de Viaris n'ajoute rien à sa précédente publication ; comme procédé de déchiffrement, c'est toujours M. Kerckhoffs qui est commenté.

Ce livre de 175 pages a surtout voulu prouver que le cryptographe cylindrique Bazeries pouvait être déchiffré.

M. de Viaris abandonne son système de numération (p. 61 de *Cryptographie*) et adopte celui indiqué par nous, en 1891, au Congrès de Marseille pour l'avancement des sciences.

Il déchiffre ensuite des cryptogrammes faits avec le cryptographe cylindrique et pour lesquels de nombreuses indications lui avaient été données. Il arrive enfin à déchiffrer des cryptogrammes, *ne connaissant rien?*

Il est regrettable que le cryptogramme fait en 1891 par M. Edouard Lucas, qui figure au *Compte Rendu du Congrès de Marseille*, cryptogramme que M. de Viaris a cependant fortement travaillé, ne figure pas parmi ceux qu'il a traduits. Cette traduction aurait été la preuve concluante que son procédé de déchiffrement est infaillible.

Mais nous sommes tranquille, nul ne déchiffrera ce cryptogramme, tant que nous n'aurons pas livré le mot clef. Il figure d'ailleurs à l'*Appendice* (*Note VII*). Les alphabets dont on *s'est servi* sont donnés au chapitre III de la troisième partie.

VALÉRIO

1893. Paris, *De la Cryptographie. Essai sur les méthodes de déchiffrement.* P. Valério, capitaine d'artillerie (L. Baudoin).

M. P. Valério a fait un livre de 228 pages, dont 160 traitent des lois phonétiques du langage. Il reconnaît lui-même que c'est un long et fastidieux répertoire (p. 154); mais, au lieu de s'arrêter, il continue par l'examen des formes schématiques de VVV, VVC, CVV, CVC, VCV, VCC, CCV, CCC.

Nous avouons humblement n'avoir ni compris ni saisi le lien subtil qui rattache ces lois aux méthodes cryptographiques de déchiffrement.

*
* *

Un déchiffreur n'a que faire de tant de science : du gros bon sens et un raisonnement sain le conduisent beaucoup plus sûrement au but à atteindre, c'est-à-dire à la traduction du cryptogramme dont

il ne possède pas la clef et dont il ne connaît même pas la méthode.

La possession, même complète, des labiales, des gutturales, des dentales, des sifflantes, des liquides de l'aspiration H, des articulations doubles, etc., etc. est insuffisante à lui faire atteindre ce but.

On ne croit pas trop s'avancer en donnant cette appréciation. Les bons esprits seront certainement de notre avis.

Cette critique faite, et elle devait être faite, passons à l'examen du livre de M. Valério, ou au moins des 68 pages sensées qui en restent. Sauf quelques pages de graphiques et de décomposition peu utiles, les autres ne sont pas sans valeur; de très bonnes choses y sont dites et bien dites. M. Valério apporte un peu d'ordre dans le classement des méthodes ; trois lui suffisent :

1° Système d'interversion;

2° Système de transposition;

3° Tables et dictionnaires chiffrés.

Ce classement est certes plus méthodique que les classements faits par les cryptologues qui l'ont précédé.

Citons M. Valério. Page 12 :

« Nous tenons avant tout à faire observer qu'en « cryptographie aucun principe n'est absolu : un « principe, vrai quand il a trait à un texte assez long, « ne l'est plus quand il s'agit de textes de peu

« d'étendue ; dans tous les cas, on n'a affaire qu'à « des probabilités et non à des certitudes, probabi- « lités qui dominent les tâtonnements, sans toute- « fois les supprimer d'une façon complète. »

On ne peut mieux dire.

Page 30 :

« La difficulté de déchiffrement augmente évi- « demment avec la brièveté de la dépêche et la lon- « gueur de la période ; mais le déchiffreur ne devra « pas négliger de s'entourer de tous les documents « qui peuvent le mettre sur la voie de la découverte : « noms et qualités de l'expéditeur, du destinataire, « lieu d'expédition, de réception, etc., etc. »

Une simple observation : les etc., etc., sont une forme commode de ne rien dire. Les noms de l'expéditeur et du destinataire, les lieux d'expédition et de réception sont généralement donnés par la possession du cryptogramme à déchiffrer.

RÉSUMÉ

Nous avons fidèlement analysé les écrits des auteurs contemporains.

Il résulte de cette analyse que si, en 1838, Vesin de Romanini était fondé à donner le nom d'*obscurigraphie* à la cryptographie, ce nom ne peut plus lui être conservé aujourd'hui.

Les découvertes de MM. Kasiski, Kerckhoffs, Viaris ont illuminé cette science.

*
* *

On vient de voir, en ce qui concerne le *chiffre carré*, qu'il peut se traduire sans clef :

1° Si plusieurs dépêches sont faites avec la même clef ;

2° Si la dépêche est suffisamment longue et si des répétitions permettent de trouver la longueur de la clef.

*
* *

Par la lecture du chapitre v, on pourra se rendre compte que les cryptogrammes du duc d'Orléans ne remplissaient aucune de ces deux conditions.

En effet, ces dépêches étaient faites chacune avec une clef différente, et elles étaient généralement fort courtes.

De plus, chose extrêmement rare dans le chiffre carré, un trigramme et un tétragramme répétés étaient dus au hasard et non à la périodicité de la clef. Nous avons consacré quelques lignes à cette particularité fort intéressante pour les cryptologues, à l'*Appendice* (Voir *Note V*).

CHAPITRE III

MANIÈRE DE RECONNAITRE LE SYSTÈME ET LA MÉTHODE CRYPTOGRAPHIQUES EMPLOYÉS

Avant de pouvoir faire le déchiffrement d'un cryptogramme, il faut que le déchiffreur détermine sûrement de quel chiffre il a été fait usage.

Les indications développées dans ce chapitre pourront servir de guide et de point de repère; mais nous n'avons pas la prétention de donner tous les moyens utiles permettant d'obtenir ce résultat.

Il faut savoir trouver au besoin d'autres indications, si celles qui suivent ne réussissent pas.

* * *

Posséder à fond la science cryptographique, être excellent calculateur, avoir du flair même, ne suffisent pas toujours pour savoir faire parler les chiffres.

Il faut surtout avoir l'esprit intuitif.

L'intuition, comme un éclair, ne dure qu'une seconde.

En matière cryptographique, elle se produit généralement quand on est obsédé par un déchiffrement laborieux et qu'on se remémore les essais infructueux qui ont été faits.

Une idée jaillit.

Tout s'illumine.

Souvent, en quelques minutes, on trouve ce que des journées et des mois d'un travail assidu n'avaient pu vous révéler.

* * *

1° Cryptogramme composé exclusivement de lettres ou de signes quelconques

Pour établir si ce cryptogramme a été chiffré au moyen d'un *alphabet conventionnel*, ou si c'est une méthode de *transposition*, ou enfin si c'est de la *cryptographie à clef*, il faut *enregistrer* les caractères employés, établir la *fréquence* de leur emploi et noter les *répétitions*.

* * *

Si on se trouve en présence d'un simple *alphabet convenu*, la division du nombre de caractères par 6 donnera très approximativement le nombre de fois qu'est reproduite la lettre la plus employée : E; la division par 10 ou 12 donnera ensuite (très approxi-

mativement toujours) le nombre de fois que sont reproduites les 5 ou 6 lettres les plus employées après l'E. Ce sont S, A, R, I, N, T ; enfin la division par 15 donnera le nombre de fois que sont employées les 3 ou 4 lettres venant ensuite dans le rang de fréquence, T, U, L, O.

Les caractères restant varieront entre 5 et 1 pour 100.

Si ces calculs se trouvent être à peu près exacts, le déchiffreur peut conclure hardiment que le cryptogramme qu'il examine a été chiffré au moyen d'un alphabet conventionnel.

* * *

Ce mode de cryptographie est enfantin. Toutefois, si plusieurs signes sont employés pour chiffrer la même lettre, cela devient plus laborieux ; mais l'obstacle n'est pas insurmontable ; il en est de même si les mots sont abrégés.

Les proportions qui viennent d'être indiquées n'ont rien d'absolu ; elles sont, en outre, notablement changées par l'emploi de plusieurs chiffres pour la même lettre.

Le nombre des signes employés dévoile cette ruse cryptographique, même à un déchiffreur novice.

*
* *

Si on se trouve en présence d'une méthode de *transposition*, chaque lettre étant pour sa valeur, l'ordre de fréquence donnera forcément E, S, A, R, I, N, T, U, L, O, etc.

C'est la caractéristique de la méthode.

On ne peut pas cacher cela.

Par quelques nulles on peut changer un peu ce rythme; mais c'est justement le changement dans l'ordre de fréquence qui fait reconnaître qu'il y a des nulles. Résultat imprévu : au lieu de dépister le déchiffreur, les nulles, étant de préférence placées au commencement ou à la fin des cryptogrammes, lui jalonnent le chemin.

*
* *

Si enfin c'est de la *cryptographie à clef*, on constate que toutes ou presque toutes les lettres sont employées.

Le rang de fréquence des caractères du cryptogramme examiné forme une échelle descendante sans écart brusque. La division du nombre total des caractères par 15, 20, 25, 30, 35, 40, 45, 50, donne chacune, comme quotient, le nombre très approximatif de fois que sont employées 2, 3 ou 4 lettres.

Si avec cela on constate quelques répétitions de bigrammes, de trigrammes, etc., il n'y a pas à hésiter, on se trouve en présence d'un chiffre à clef (chiffre carré, etc.).

*
* *

Si le cryptogramme présentait de distance en distance des trigrammes semblables, et que le nombre des lettres soit un multiple de 3, il y aurait lieu d'examiner si ces trigrammes sont disséminés sans loi qui les régisse ; dans ce cas, au lieu de se trouver en présence d'un chiffrement lettre par lettre, il pourrait se faire que ce fût un chiffrement mot par mot.

Une seule dépêche n'est pas toujours suffisante pour faire cette constatation.

Le seul répertoire français qui soit établi par groupes de 3 lettres est celui de Mamert Gallian.

*
* *

2° Cryptogramme composé exclusivement de chiffres arabes

Généralement l'examen de ces sortes de cryptogrammes permet d'établir à quel système ou à quelle méthode ils appartiennent.

Les chiffres sont groupés régulièrement par 2, 3, 4, 5, ou se suivent sans interruption, ou bien encore présentent des groupes irréguliers de 1 à 5 chiffres.

*
* *

S'ils sont groupés par 2, il faut conclure que c'est un alphabet conventionnel où chaque lettre est représentée par un nombre de 2 chiffres.

*
* *

S'ils sont groupés par 3, et qu'ils ne proviennent pas d'un pays soumis au régime extra-européen, il y a lieu de supposer que c'est un chiffrement mot par mot avec un chiffre de 1.000 groupes seulement.

*
* *

S'ils sont groupés par 4, on est en droit de supposer qu'il a été fait usage d'un répertoire chiffré existant dans le commerce (Sittler, Nilac, Bazeries, Baravelli, etc.).

*
* *

Toutefois, si les nombres formés par les groupes de 4 n'emploient pas les 10 chiffres de la numération, c'est-à-dire qu'ils soient toujours compris

entre un nombre moins élevé et un autre plus élevé, il peut se faire qu'on se trouve en présence d'un chiffrement lettre par lettre, et il faut alors examiner les groupes, 2 chiffres par 2 chiffres. La télégraphie privée ne pouvant faire usage de groupes de lettres, les particuliers sont obligés de transformer les lettres en chiffres pour pouvoir se servir du télégraphe ; les dépêches chiffrées du duc d'Orléans étaient transformées ainsi.

*
* *

S'ils sont groupés par 5, il y a lieu d'examiner s'il n'existe pas un chiffre nul dans chaque groupe; si on reconnaît ce chiffre, on revient au déchiffrement régulier, par groupe de 4. Si on ne trouve pas, après examen attentif, le chiffre nul, il y a lieu de compter le nombre de chiffres total du cryptogramme. Si ce nombre est un multiple de 4, il y a beaucoup de raisons de croire que c'est un chiffre de 10.000 groupes, transmis sans interruption. La formation des groupes réguliers de 5 est une simple mesure économique, 5 chiffres comptant pour un seul mot.

*
* *

Si les chiffres se suivent sans interruption, il faut, par une division du nombre total des chiffres par 3 et par 4, examiner si on est en présence d'un

chiffre de 1.000 ou de 10.000 groupes. La division par 2 permet aussi d'établir si c'est un chiffrement lettre par lettre.

*
* *

Si le cryptogramme présente des groupes irréguliers de 1 à 5 chiffres, il n'y a pas à hésiter, on est en présence soit d'un chiffre diplomatique, soit d'un chiffre fait avec un livre quelconque. Dans ce dernier cas, 3 groupes représentent un mot, et il faut enregistrer les groupes par séries de 3.

OBSERVATIONS

Il ne faut pas perdre de vue que les indications qui viennent d'être données, comme d'ailleurs toutes les règles cryptographiques, n'ont rien d'absolu.

*
* *

Des chiffres nuls placés en tête, en queue ou dans le corps d'un cryptogramme peuvent induire en erreur. Avec de la pratique on finit généralement par reconnaître sûrement le système et la méthode employés. C'est un premier point d'obtenu ; il est énorme, car il limite les recherches. Il faut ensuite examiner si ce système ou cette méthode permettent la lecture sans clef.

En règle générale, tous les chiffrements, lettre par lettre, peuvent se lire. Il en est de même des chiffrements mot par mot, si l'on s'est contenté de transformer un clair en chiffres avec un répertoire existant dans le commerce ou un répertoire particulier établi par séries alphabétiques et ne comportant que 3 à 4.000 groupes.

*
* *

La question change du tout au tout pour les chiffres du 2e système, si le répertoire comprend 8, 10, 12, 15.000 groupes ou si l'on fait de la cryptographie à clef.

L'opération qui consiste à transformer du clair en chiffres au moyen d'un répertoire ne constitue pas, en réalité, un travail cryptographique, c'est une traduction.

Le travail cryptographique consiste à dénaturer, au moyen d'une combinaison quelconque, cette traduction chiffrée de manière à en empêcher la lecture. Si on sait bien s'y prendre, on supprime d'abord les répétitions, dangereuses dans ces systèmes, et on arrive même à déguiser le système employé.

CRYPTOGRAMME DE BALZAC

Balzac, dans *la Physiologie du mariage* (méditation xxv, § 1 : *Des religions et de la confession considérées dans leurs rapports avec le mariage*), donne un cryptogramme composé d'environ 3.600 caractères.

Nous allons appliquer les principes énumérés au commencement de ce chapitre pour reconnaître le système cryptographique employé par Balzac.

Reproduisons d'abord son cryptogramme.

ɐnnɐr snsff iNfid gdc': 'ɟptq ogvtm ffo.d
t-aot o;tod fda:d hoiOo ɻdâsa dêcss mcird
ersqv t'odh t.tdi toâdg daodt gtdot ahtod
ccoce 'tèto egodè vo'de âadsd ieaia sabdB
:oaov fiPsè fiB,a .'oqb maO;t o;afv àtmtd
odêi' diafi tbdmv oh;ɪo èothd toBdo odtbt
fitff idoad 'go:d aoqtè -adto ;omac sâoos
boffl t',to qtdpo toqtd o-fdt ;dï'd ètost
;itdo t;'dâ osiêa sdo'; 'vBff dffso hPaos
fiè.d cèêto fid.t dodia sfion dnn-. sadom
fi;oc oq;d- ditso aLfds so,vd a.oɻs -èttà
èodot oqotd -gèoo bdtot dtdoq d;toɪ dndnv
pdcdt t'odq dnq.d nogaà odtqa rttnc ascca
vsvis fidod htædà 'dttL fi'qo ɪddtd fg.ot

btto; qtdod ;tcas ffias scsàv sdoys cssaa
dotot hacai dgbdq ,tdto gottd .ocdt mtsrd
êmddP d'odo d'aêo cotaL t'ass asq's ;fltt
qt;do qsdod flss1 t:t-l .dtat dotsa tbeqæ
d-tod .tdê- ohêhg o;odà snsat -oâ*f to'uc
tPdcə ise,s dotno '.aos rs-1ı ê'.it d;êvc
t;.de sdta- tbmæb dLomb Nffio dbq'm to'qo
dê.to b-:o: d-doq tdqod dhooo 4oqtd adthd
;ada. terat aePaï dotot oêè'- tt'a- 'têdt
oeaob totot aqdff ghdov 'otêo 'doe- '.bdd
godho smoh, e1dod oaet- :ooPd e,odt obdds
deg"o 1eqff iogié ooftd ot..à otLod ddroa
-dood 1d'od ,deod odgfb odc'o ddoo' ddhff
iffdd Kodff itdtq dté'o d'ooo tgffl hflat
tqol- tbddg 'cqdd oboob o:ddt 't-do fgdêo
d,odo 'oeom oPdab adomd g'*ot d-qo- 'doei
oeot» d.doi 'b'og 'gPcf lhimc tda:o m,oot
pdqoo goans ctd'o édo't gdtoo dtoto ttfdf
fiodf fi,dd oN1t; d.voo opdto. dodàm bgo,t
gddea edctt t.-oo 1g,tq c.oar ciodd ,,omq
td'po hodtt tæKfl :d1dv dt..g oKdgf fiede
utmeb deé-ç ecf;h g.rta uxmev nieto arqfc
tuvtx irnmc bç-'h :fi.r atnim udv,t ffidg
éoætd odtPa doLgq od-gv ot;ff obàdt rsidh
ddqco t'tdo dolda daoxé z-ent micso staqr
aep;g dhfi; rtaml uxcny tizni mdcc- éfq.a

d,tux vmcbz obo;o tobod toqo- tædd. o.fft
t.fco ,bPtt dm:do 'dsoè dsàaq oedes racfi
:fiod mbxzl emciu tvdfu flcdû yrrqo ïa,q.
fi;he ebçcè -idmo idzby vlmig qio't uprdé
doPto t»aom oP.to ht;Ps fotto cvoad Pqdff
icdNv do'od qoeot odtff oed7u tica. rqfgs
iedmc b-éwi nantu ifi:k hOidm txoq: ,g.qa
rbzxà mides oratm to'do ffiqd oèovï dtqto
idoto oæ1od toadh toqdo qoaog adoda éo;ff
itsed ob-rv ybzé- dcfee iqoin tx'èm qtubn
oprai dnmûq arloe inlmb zyxfn 1itqm udoèd
o'dto t.vo. 'cod; to'dg ototo vdoad o.:dê
t-vtd tot;o dott1 .ovd' dho't dévtr odqzy
xtmid ofapr .fi,h ;qaod ivytb çdéc- mqino
peiéb xtubl cdefq goran eveâs dthoc v;.ot
sed-m dædot dotdv qdtdo 'ædto toèfd obfit
d:.dO iao.o d,dLd (dmûe deycb mutia ntosd
eg;ff i.qoi pr,fı gdfcn lybzu iqnfT bfd-é
bmcnt Potb- o'oct 8ffo- èobof fiotd dosob
otd1o Do'df i:odh cd'dè vd;'o tffid cd.td
oecym gzih. aoqim bvtnx d-ps. ri,at cb,fi
;ecin doylw uvmd- éçèÉf'l"sin !raoq gdahd
go1ad o*ocq h-èbè qpbd- tvv1o dqom8 :odod
dootè dotco dtiff otèvt mxutd -éçmH 'ém-e
Toq;f fih9f dcSmt uyinz dufq. rax¯L mlcbe
rinbu avrqy ;vo.m qyyté ivq'g qtsqé 1qègq

qgita ia.yè ;qé.g i;qém goPy(dytmî digqb
æicbé yiqtm qoécb giva- æg'éd îbmœo 'tété
tioét o.èqo cia m -èbyœ iètit ;iyim uvtyt
gébvt tmryv t!vya mimxt qtqio i-o.é cééma
icdét uitœn tcbgq miygy yb-r. tqxmé yg-it
gmtuœ t'ncq rdap, ,œiuy rtgtû arxœd ,'xœy
'gtoy rfliœ gaèaé ytmé, xaBth èe'qv ffbeg
-»és q ,aàœt hmebq riési ;OEy. iq-èh »,,gd
fflFl aurnt igsbO 'èeee 6à,qC sî,rs »ràso
qmn(q 'q,mé qCséf ffsff an.me fz.s. Cisei
e,Cfè ſ'pCc ă'otl ffnét zt-c(C,éCJ ftoyo
tPofS ,-tc. sciPi zédot oédog z.ofx yCie,
Pyso, dtoea évés- oseno -tboy eDyà(PnCqx
cj'nà nasfm céfef facab md,ɔt eftfm Pzszg
ts:oq aéPèe oœ,,n ,xœhn hWReh ÿCe.e i,iis
àbqêf Rrgqo fobqf ja.,é mysei tggég sf-Rr
ivc,x gyrdt cezyP eegst sjRtq uzayd .xs.r
eCéf' zimbi rgœcq àqbsr gdiri éecge feqé,
é.ens DsCfm gche, eeycé biqsg ',vre exr'œ
qeéé; ctbri tr,év qzCmé Rà.yz e-xcc sw.ém
,mrxv bég,g xs.y. é.efy zj'rî àgei, ré,ét
xto.x .et.d yaac, tatrx egcqy sty,t rqye'
s(bms digqq étcyc ia,ej -tcxv é,oiv qe-yy
engte roeqq twqèt icmtd tqteé t'c,P g,s';
agmag 'bwta irnjt irmat iooit éy.it vioti
wtggg mt.ti rsndd égtéc tefeé dém', tyéym

eéqry eyscr tgtfé f-éti q;.qc qt,yo -eé'e
eénéi tit-a gcaec tobt. ict.s gbcfw gy.yg
.éi,i a.cac 'gtév cntoz oigté .itàq irdcb
.séém 'tdtf iairt edvsy totyo .oat, qétbs
avtfa tr-s' icrot q-qdé rstvi trdre é,y,t
,qmsy ,ia'r o'osg ngéot csiyd oy-éb g,éia
teréi cd-td tigt, tobét év,iq iu,it q-ytg
irtéi -isie .q.si eot't odiog yvtzd t.aor
tryi. odt.g tsost d'ia. ês,éi rtéé, d:rst
otaéi od,.q tisvt i,tgt ày,ro lviét fl,td
fig.v qosas .gsét àdadt a.tw- c,iia d.

*
* *

Bien des esprits se sont appesantis sur ces caractères ; nul n'a pu arriver à en faire la traduction.

Certains ont émis l'avis que le compositeur avait renversé sa casse, et que Balzac aurait dit : « C'est très bien, ramassez les caractères tombés, et replacez-les n'importe comment au gré de votre caprice. » D'où ce cryptogramme.

*
* *

Nous avons fait l'application de nos principes pour reconnaître le système de cryptographie employé par Balzac.

En voici le résultat :

Comme il était inutile de décomposer et d'établir l'ordre de fréquence des 3.600 caractères de ce cryptogramme, nous n'avons opéré que sur les premières lignes.

Nous avons trouvé 1.013 caractères ainsi employés :

1° Lettres minuscules placées normalement :

d.	137	*Report*. . .	673	*Report* . .	798
o.	131	g.	20	l.	7
t.	120	b.	19	p.	3
a.	57	e.	19	x.	3
f.	51	h.	18	u.	1
s.	51	v.	15	y.	1
i.	34	m	13	j.	»
q.	29	n.	13	k.	»
c.	23	r.	8	w	»
A reporter.	673	*A reporter.*	798	TOTAL. . .	813

2° Lettres minuscules renversées :

ɐ	2	TOTAL 10
ə	2	
ƨ	1	
ɥ	5	

3° Lettres minuscules accentuées :

é.	14	TOTAL 41
è.	12	
â.	7	
à.	4	
ê.	2	
î.	2	

4° Lettres majuscules placées normalement :

P.	6	
L.	5	
B.	4	
N.	2	TOTAL 19
K.	1	
O.	1	

5° Lettres majuscules renversées :

d.	1	TOTAL 1

6° Chiffres arabes :

1.	5	
0.	1	TOTAL 7
4.	1	

7° Signes de ponctuation placés normalement :

'	37	
-	22	
. . . . .	21	
;	20	TOTAL 119
, ...	9	
:	9	
«	1	

8° Signes de ponctuation renversés :

¿	1	TOTAL 1

9° Renvois et abréviations :

¹	1	
°	1	TOTAL 2

RÉCAPITULATION

1° Minuscules.	813
2° — renversées.	10
3° — accentuées.	41
4° Majuscules.	19
5° — renversées.	1
6° Chiffres arabes	7
7° Signes de ponctuation.	119
8° — — renversés.	1
9° Divers.	2
TOTAL ÉGAL.	1.013

*
* *

Ce n'est pas un système cryptographique basé sur un alphabet conventionnel, parce que la division de 1.013 par 6 donne 169 et que 2 caractères *d* et *o* répondent à cette division.

Les caractères qui seraient mis pour les lettres S, T, A, I, R, N, O, U, L, ne peuvent se déterminer par la division de 1.013 par 10, 12 et 15.

De plus, beaucoup de lettres 3 fois répétées existent dans les cryptogrammes (nous les avons soulignées pour qu'on les trouve plus facilement). Avec un système d'alphabet conventionnel, la lettre triplée ne pouvant être que la lettre E, ce serait toujours le même caractère qui serait triplé ; or on peut constater que le caractère triplé est tantôt o, tantôt d, tantôt t ; il est aussi e, f, g.

Donc, ce n'est certainement pas de la cryptographie par un alphabet conventionnel.

C'est encore bien moins un système de transposition; ceux qui ont émis l'avis que la composition avait été renversée et les caractères replacés n'importe comment ne s'étaient pas donné la peine de compter, car on ne déguise pas un système de transposition. Il se reconnaît à première vue.

Ce n'est pas non plus un chiffrement dans le genre du chiffre carré.

*
* *

Dans ces conditions, la conclusion est bien simple :

Balzac, ayant voulu dire que la question du confesseur et de l'amant était une question indéchiffrable, a, sans doute, laissé 2 ou 3 pages en blanc dans son manuscrit, et dit à son éditeur : « Vous remplirez cela comme vous voudrez, avec des majuscules, des minuscules, des chiffres, des signes de ponctuation, etc., soit en les plaçant naturellement, soit en les renversant, de manière à former un imbroglio quelconque où personne ne comprendra rien. »

C'est ce qui a été fait.

Donc le cryptogramme de Balzac est simplement une facétie de l'auteur et non le résultat d'un système cryptographique quelconque.

CHAPITRE IV

NOUVEAU PROCÉDÉ DE DÉCHIFFREMENT

Revenons au chiffre carré, dont nous nous sommes écarté un instant, et donnons un nouveau procédé de déchiffrement que ni Kasiski, ni Kerckhoffs, ni Josse, ni Viaris, ni Valério n'ont décrit.

Nous avons déjà établi par ailleurs [1] que le point de départ de toute reconstitution de chiffre était toujours la recherche d'un mot supposé.

Dans le chiffre carré, la recherche de ce mot supposé donnera du même coup soit la clef, soit une portion de cette clef.

C'est un moyen pratique de déchiffrement tout aussi rapide que ceux indiqués par M. Kerckhoffs ; de plus, il est infaillible, si on a affaire à une clef courte, comme celle de la dépêche Havas relative aux affaires militaires d'Egypte, donnée page 41 de la brochure de M. Aug. Kerckhoffs, et qui comporte

[1] *Le Masque de fer*, p. 262. Paris, 1893. Firmin Didot.

comme clef, d'après les calculs des répétitions, un mot de cinq lettres.

Un exemple fera mieux comprendre la façon d'opérer. On va chercher dans cette dépêche Havas le mot « *général* », que M. Kerckhoffs dit s'attendre à y trouver.

Voici la manière d'opérer :

RECHERCHE DE LA CLEF

	1 2 3 4 5	1 2 3 4 5	1 2 3 4 5	1 2 3 4 5
Cryptogramme :	R B N B J	J H G T S	P T A B G	J Z X B G, etc.

Mot supposé. . g e n e r a l
Clef. . . . . K R A R S J X

g e n e r a l
P J I F S I W

g e n e r a l
H R W F R H R

La clef est trouvée : c'est FRHRW.

En se servant de ces cinq lettres comme clef et du tableau de la page 46 de la brochure de M. Aug. Kerckhoffs, on déchiffrera tout le cryptogramme de la page 41, ce que l'on ne pourrait faire ni avec le mot *dégel*, ni avec le mot *puluy* indiqué page 45.

Voici d'ailleurs la traduction littérale et complète de cette dépêche :

« Le général Wolseley télégraphie d'Ismaïlia qu'il attend seulement que le service de transports

et de communications soit complètement organisé pour faire une nouvell *r* (e) marche en *v* (a) vant. Il avait compté sur le chemin de fer et le canal *k* (p) our tra *f* (n) sporter les a *k* (p) provisionnements des troupes, mais l'ennemi a coupé ces voies de communication en construisant des di *e w* es (digues) dans le canal et en élevant une v *f* (a) ste jetée su *e* (r) la ligne du chemin de fer. Ces obstacles sont maintenant enlevés et trois ma *e* (c) hines font le s*t* (e) rvice du camp Anglais d'Ismaïlia.

* * *

Ce cryptogramme, comme en général beaucoup d'autres non suffisamment collationnés, contenait 11 erreurs; ces erreurs peuvent dérouter pour la recherche de la clef; mais, une fois la clef trouvée, elles n'empêchent point la traduction, et on s'aperçoit vite des erreurs commises.

Bien mieux, on détermine la cause de l'erreur : erreur du chiffreur qui aura pris une ligne ou une lettre pour une autre, erreur du télégraphiste qui aura transmis ou lu une lettre ou un chiffre pour un autre.

* * *

M. Kerckhoffs, qu'il faut toujours citer en cryptographie et dont il faut savoir s'inspirer au besoin, dit dans son étude du chiffre carré :

« Lorsque le rapport des lettres de la clef à celles « des chiffres du cryptogramme est tel qu'aucune « répétition n'a pu se produire, le déchiffrement « présente des difficultés, et l'on est obligé d'avoir « recours au tâtonnement. »

Et plus loin :

« Si, dans le déchiffrement d'un cryptogramme à « alphabets intervertis, il est impossible de déter- « miner le nombre des alphabets de la clef, soit « parce que la dépêche est trop courte, soit parce « que la clef est trop longue, la solution du pro- « blème présente des difficultés, sinon insurmon- « tables, du moins capables de lasser la patience du « plus habile déchiffreur. »

On verra plus loin comment le procédé de déchiffrement qui vient d'être indiqué a donné un résultat positif pour le déchiffrement des dépêches du duc d'Orléans (Voir chapitre v).

CHAPITRE V

DÉCHIFFREMENTS DE QUELQUES CHIFFRES CARRÉS

On va dans ce chapitre donner quelques déchiffrements obtenus par différents procédés.

CRYPTOGRAMME DE JULES VERNE

En appliquant les principes énoncés au chapitre IV au cryptogramme que Jules Verne a donné dans son roman *la Jangada*, cryptogramme que le juge Jarriquez eut tant de mal à traduire, on va tout de suite pouvoir déterminer le système employé et faire ensuite, avec aisance, la traduction.

Ci-après le cryptogramme en question ; les répétitions de 3 et au dessus sont soulignées, ainsi que le bigramme PH.

PHYJS LYDDQ FDZXG ASGZZ QQEHX
GKFND RXUJU GIOCY TDXVK SBXHH
UYPOH DVYRY MHUHP UYDKJ OXPHE

TOZSL ETNPM VFFOV PDPAJ XHYYN
OJYGG AYMEQ YNFUQ LNMVL YFGSU
ZMQIZ TLBQG YUGSQ EUBVN RCRED
GRUZB LRMXY UHQHP ZDRRG CROHE
PQXUF IVVRP LPHON THVDD QFHQS
NTZHH HNFEP MQKYU UEXKT OGZGK
YUUMF VIJDQ DPZJQ SYKRP LXHXQ
RYMVK LOHHH OTOZV DKSPP SUVJH
D.

La première chose à faire est d'enregistrer les caractères employés pour établir la fréquence de leur emploi.

Ce travail donne le résultat ci-après :

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
3.	4.	3.	16.	9.	10.	13.	23.	4.	8.	9.	9.	9.	12.	16.	16.	12.	10.	8.	17.	13.	12.	19.	12	

Total : 276.

Immédiatement on constate que les vingt-cinq lettres de l'alphabet sont employées et que le rang de fréquence forme une échelle descendante de 23 à 3, sans écart brusque ; 23 H; 19 Y; 17 V; 16 DPQ; 13 GV ; 12 ORXZ ; 9 EKLMN; 8 JT ; 4 BI ; 3 AC.

C'est la caractéristique de la *cryptographie à clef.*

De plus, il existe les répétitions de RYM, RPL, KYUU. C'est encore la caractéristique du *chiffre carré.*

Ce travail d'enregistrement a donc permis d'établir sûrement que la méthode employée était celle du *chiffre carré*.

Il faut ensuite déterminer la longueur de la clef; les intervalles de 192, 60 et 12 existant entre les répétitions de RYM, RPL, KYUU indiquent comme longueur, 3, 4, 6 ou 12 sous-multiples de 192, 60 et 12.

L'examen du bigramme PH, répété à 72, puis à 114 d'intervalle fait de suite éliminer 4 et 12; reste donc comme longueur de clef 3 ou 6.

Il ne reste plus qu'à traduire, et le lecteur va constater combien c'est aisé, si on a la patience de faire ce

	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	
Première colonne verticale. . .	»	1	»	»	3	»	1	5	(2)	»	»	»	6	1	»	4	4	3	4	»	»	2	3	4	3	46
Deuxième id. . .	»	»	»	7	»	2	4	(9)	»	»	»	2	1	»	1	1	5	2	1	»	1	4	3	2	1	46
Troisième id. . .	»	»	3	2	3	1	(4)	»	1	»	9	»	»	3	2	3	2	»	»	»	4	4	2	3	»	46
Quatrième id. . .	3	»	»	»	»	3	»	1	1	(4)	»	1	1	3	»	»	4	4	3	5	1	»	1	7	4	46
Cinquième id. . .	»	3	»	1	3	(3)	»	1	»	3	»	»	»	2	8	5	»	2	2	3	7	1	1	1	1	46
Sixième id. . .	»	»	»	6	»	1	4	(7)	»	1	»	6	1	»	1	3	1	1	»	»	4	2	3	2	3	46
Totaux. . .	3	4	3	16	9	10	13	23	4	8	9	9	9	9	12	16	16	12	10	8	17	13	12	19	12	276

nouveau travail d'enregistrement des lettres.

On dispose le cryptogramme par colonnes verticales sur 6 de front et on enregistre les lettres par colonne verticale.

Ci-contre le résultat de ce travail.

La division par 6 devrait nous donner le nombre de E; mais l'examen du tableau nous fait voir que cette proportion normale est loin d'être atteinte, cela arrive quelquefois; il ne faut donc pas s'y arrêter outre mesure et examiner quel est le nombre qui, à 4 d'intervalle, donne d'autres nombres avant et après qui puissent être A et I. Les nombres entre parenthèses 2,9,4,4,3,7, répondent à cette condition. Ces nombres indiquent la lettre E.

4,4,3,4 — 1,1,5,2 — 3,2,3,2 — 4,4,3,5 — 0,2,8,5 — 1,3,1,1 correspondant aux lettres L, M, N, O et 2,3,4,3 — 1,4,3,2 — 0,4,4,2 — 1,7,4,3 — 2,3,7,1 — 4,2,3,2 correspondant aux lettres R, S, T, U, confirment dans cette hypothèse.

Il n'y a plus qu'à traduire chaque lettre du cryptogramme en lui substituant sa correspondante qui est :

Première colonne verticale. . . .		moins 4
Deuxième	id.	moins 3
Troisième	id.	moins 2
Quatrième	id.	moins 5
Cinquième	id.	moins 1
Sixième	id.	moins 3

TRADUCTION

P H Y J S L	H Y Y N O J	V D D Q F H
l e v é r i	d u v i n g	r a b l e e
Y D D Q F D	Y G G A Y M	Q S N T Z H
t a b l e a	t d e u x j	m p l o y é
Z X G A S G	E Q Y N F U	H H N F E P
u t e u r d	a n v i e r	d e l a d m
Z Z Q Q E H	Q L N M V L	M Q K Y U U
u v o l d e	m i l h u i	i n i s t r
X G K F N D	Y F G S U Z	E X K T O G
s d i a m a	t c e n t v	a t i o n d
R X U J U G	M Q I Z T L	Z G K Y U U
n t s e t d	i n g t s i	u d i s t r
I O C Y T D	B Q G Y U G	M F V I J D
e l a s s a	x n e s t d	i c t d i a
X V K S B X	S Q E U B V	Q D P Z J Q
s s i n a t	o n c p a s	m a n t i n
H H U Y P O	N R C R E D	S Y K R P L
d e s s o l	J o a m D a	o u i m o i
H D V Y R Y	G R U Z B L	X H X Q R Y
d a t s q u	c o s t a i	s e u l q u
M H U H P U	R M X Y U H	M V K L O H
i e s c o r	n j u s t e	i s i g n e
Y D K J O X	Q H P Z D R	H H O T O Z
t a i e n t	m e n t c o	d e m o n v
P H E T O Z	R G C R O H	V D K S P P
l e c o n v	n d a m n é	r a i n o m
S L E T N P	E P Q X U F	S U V J H D
o i c o m m	a m o r t c	o r t e g a
M V F F O V	I V V R P L	
i s d a n s	e s t m o i	Clef 4 3 2 5 1 3
P D P A J X	P H O N T H	
l a n u i t	l e m i s é	

Cle 4 3 2 5 1 3 Clef 4 3 2 5 1 3

Nous reconnaissons que les travaux d'enregistrement sont fort longs, qu'ils n'ont aucun attrait; mais c'est le seul moyen à employer, si l'on veut aboutir.

De plus, ces travaux ont l'avantage immense de supprimer presque complètement la période de tâtonnement, si absorbante et si fatigante.

Comme le lecteur a pu s'en convaincre, en commençant par l'enregistrement, on va droit au but, lentement, mais sûrement.

CHIFFRES DU GÉNÉRAL BOULANGER

Récemment, à Dijon, nous recevions d'un officier général, qui, au moment des affaires Schnæbelé, faisait partie du Cabinet du général Boulanger, un cryptogramme fait avec un chiffre spécial dont devait se servir le Ministre de la Guerre en tournée d'inspection dans la région de Nice, pour correspondre, en cas d'événements, avec son Cabinet.

Il paraît que Boulanger avait une telle confiance dans le chiffre de l'Etat-Major général qu'il n'avait pas voulu l'employer!!!

L'officier général qui nous envoyait ce cryptogramme ne se doutait certes pas qu'on pouvait le traduire en moins de deux heures.

Voici d'ailleurs ce cryptogramme qui, entre parenthèses, renfermait quatre erreurs :

AWAQG	KQZKG	STNVN	MWFKH
WTQRO	WQCMP	WAIFN	WZGVJ
UIQJP	AWAJG	DBBFU	JQFMW
GKSUC	KMZZC	ANTZF	KCZGU
WTGKG	JKSJU	WT	

Les lettres soulignées, par suite d'un examen rapide, se trouvant donner des intervalles de 45 et 10, la longueur de la clef — 5 — saute pour ainsi dire aux yeux, et on peut en déduire que c'est une méthode de chiffre carré.

*
* *

N'ayant pas de tableau sous la main et ne voulant pas en construire un, nous avons essayé de déchiffrer de tête, en comptant, comme pour les méthodes de Gronsfeld et du comte de Paris.

Le résultat a été complet.

Après avoir placé les lettres par colonnes verticales de 5, on a établi que W existant 6 fois dans la première colonne et G existant 4 fois dans la cinquième colonne représentaient E; pour les trois autres colonnes, il a fallu tâtonner un peu; mais cela n'a pas été long, et, en fin de compte et en moins de deux heures, nous avons traduit le cryptogramme sans tableau, de tête, en comptant sur nos doigts.

La valeur des lettres était augmentée de 8 pour la première colonne ;

Diminuée de 8 pour la deuxième ;

Augmentée de 12 pour la troisième ;

Augmentée de 9 pour la quatrième ;

Diminuée de 2 pour la cinquième.

Ci-après le déchiffrement ; les erreurs sont rectifiées par les lettres mises entre parenthèses.

Pour lire la traduction : « Les secrets les plus difficiles », etc., il faut commencer par la fin du cryptogramme et lire de droite à gauche et en remontant.

A	W	A	Q	G	
i	o	m	z	e	
K	Q	Z	K	G	
s	i	l	t	e	
S	T	N	V	N	(x)
a	l	z	e	v	
M	W	F	K	H	
u	o	r	t	f	
W	T	Q	R	O	
e	l	c	a	m	
W	Q	C	M	P	
e	i	o	v	n	
W	A	l	F	N	(x)
e	s	u	o	v	
W	Z	(R)	G	V	J
e	j	s	e	h	
U	I	Q	J	P	
c	a	c	s	n	
Clef	+	−	+	+	−
	8	8	12	9	2

A	W	A	J	G	
i	o	m	s	e	
D	B	B	F	U	
l	t	n	o	s	
J	Q	F	M	W	
r	i	r	v	u	
G	K	S	U	C	
o	c	e	d	a	
K	M	Z	Z	C	(E)
s	e	l	i	c	
A	N	T	Z	F	
i	f	f	i	d	
K	C	Z	G	U	
s	u	l	p	s	
W	T	G	K	G	
e	l	s	t	e	
J	K	S	J	U	
r	c	e	s	s	
W	T				
e	l				
Clef	+	−	+	+	−
	8	8	12	9	2

Nous n'avons pas cherché le mot clef dont le général s'était servi; mais c'est une opération extrêmement facile à faire[1].

Ce qui importait le plus dans l'espèce était de connaître la force de résistance au déchiffrement. Moins de deux heures, avec quatre erreurs dans le texte, c'est suffisant pour ne pas recommander ce système, surtout le déchiffreur ignorant la méthode employée.

Lorsque, plus tard, le général Boulanger se lança dans la politique, il adopta pour son usage personnel et pour correspondre avec ses partisans un dictionnaire existant dans le commerce (Sittler).

Pour déchiffrer ses dépêches, on n'eut pas besoin de recourir aux services d'un spécialiste. Malgré le soin avec lequel la pagination avait été faite, ses dépêches purent être facilement lues.

CHIFFRE DES ANARCHISTES FRANÇAIS EN 1892

M. Kerckhoffs, en décrivant le chiffre secret adopté par les nihilistes russes, chiffre fait d'après un système de transposition double, dit que les

[1] La recherche de ce mot-clef faite depuis, et d'après la méthode indiquée au chapitre III, a donné CROIS, renversé, soit SIORC, et a dévoilé que la méthode employée était celle de Beaufort, clef en dessus.

nihilistes ont commis la faute grave de se servir du même mot clef, pour les deux transpositions.

On va voir que les anarchistes français ont commis une faute analogue, faute qui a permis de découvrir leur chiffre.

*
* *

Le chiffre employé par les anarchistes, en 1892, était une variété peu connue du « chiffre carré ».

Les quelques spécialistes qui la connaissent lui ont donné le nom de « chiffre du comte de Paris ».

On ignore si réellement le comte de Paris l'employait.

Ce chiffre se rapproche de la méthode connue en cryptographie sous le nom de méthode de Gronsfeld.

Voici en quoi il en diffère.

Le comte de Gronsfeld a supprimé complètement le tableau cryptographique. Après avoir pris comme clef un nombre quelconque, il fait les opérations de chiffrement et de déchiffrement, de tête pour ainsi dire.

Les anarchistes opéraient de même ; mais, pour ne pas se tromper, ils avaient un tableau ne renfermant que dix alphabets au lieu de vingt-cinq.

*
* *

Deux écrits chiffrés avaient été saisis, ainsi que le tableau des dix alphabets.

La clef étant courte (première faute), la longueur a pu en être déterminée; malgré cela, les précautions prises ont tenu le déchiffreur en échec pendant une quinzaine de jours.

Voici en quoi consistaient les précautions:

1° Les six premières lettres et les six dernières des cryptogrammes étaient des lettres nulles. Cette première précaution, excellente en elle-même, avait pour effet de renfermer l'écrit secret entre deux murailles, réputées par certains comme infranchissables;

2° Des lettres nulles étaient intercalées dans le texte, de distance en distance, et chiffrées; de préférence, elles étaient placées entre chaque mot.

Cette deuxième précaution, excellente aussi, avait sans doute été prise pour rebuter un déchiffreur habile, mais peu patient.

Malgré toutes ces excellentes précautions, la clef a été trouvée. C'était le nombre 456.327, ou, en opérant par la méthode de Vigenère, les lettres EFGDCH.

*
* *

La faute grave commise par les anarchistes a été de placer en tête et en queue du cryptogramme un nombre de nulles égal à la longueur de la clef.

Comme nulles du corps de l'écrit, la lettre W avait été adoptée.

Le procès de Saint-Etienne (1892) a permis de connaître ce chiffre et la traduction des deux lettres chiffrées.

Partie chiffrée d'une lettre du 30 avril 1892 :

« Demande à Louis Ch... une lettre de ma part. »

Partie chiffrée d'une autre lettre du 5 mai 1892 :

« Sa femme et lui sont des mouchards; s'il m'ar-
« rive quelque chose, songe à les supprimer. »

Par les précautions prises on a tout simplement retardé la traduction de quelques jours; mais ces précautions indiquent chez l'auteur de ce chiffre une compétence en matière cryptographique qu'on ne devait certes pas s'attendre à trouver chez des anarchistes aussi peu instruits que Ravachol et Béala.

CHIFFRE DU DUC D'ORLÉANS EN 1898-1899

Les dépêches du duc d'Orléans étaient en chiffres arabes, transmis par groupes de quatre[1].

La première idée qui vient à l'esprit est que ces groupes de quatre chiffres arabes représentent des mots.

Mais, en enregistrant les nombres formés par ces

[1] Ces dépêches ont été publiées (Voir *la Libre Parole* du dimanche 5 novembre 1899).

groupes, afin d'en établir la fréquence et les répétitions, on constate qu'il n'y a pas de nombre inférieur à 1111, ni supérieur à 3737.

L'idée des répertoires existant dans le commerce (Sittler, Nilac, Bazeries), lesquels ont tous dix mille groupes variant de 0000 à 9999 est donc à rejeter d'emblée.

Reste l'hypothèse d'un répertoire spécial, fait pour la circonstance.

*
* *

En examinant plus attentivement les dépêches, on constate que dans les 1100, par exemple, on ne trouve pas de nombre inférieur à 1111, ni supérieur à 1137. Cette constatation, rapprochée de l'inscription des nombres 11 à 37, figurant sur le tableau du duc d'Orléans, a suffi pour abandonner complètement l'hypothèse d'un répertoire et pour pouvoir déterminer sûrement qu'on se trouve en présence d'un chiffrement lettre par lettre.

Il ne restait plus, après cette constatation, qu'à transformer les chiffres, pris deux par deux, en lettres, d'après la valeur indiquée au tableau.

Cette transformation faite, les lettres ont été enregistrées pour établir leur ordre de fréquence et eurs répétitions.

*
* *

Cet enregistrement a permis d'établir sûrement :

1° Que c'était une méthode de substitution ;

2° La fréquence des lettres indiquait une méthode à clef ;

3° Les dépêches paraissaient être faites chacune avec une clef différente.

*
* *

Les profanes pourront s'étonner que le simple enregistrement dont on vient de parler ait pu donner sûrement les trois indications ci-dessus ; il n'en sera pas de même des cryptologues : ceux-ci savent qu'avant les opérations de tâtonnement, qui font découvrir un chiffre, il y a les opérations techniques et que celles-ci, basées sur les sciences mathématiques sont très rarement en défaut.

On a donc conclu à une des nombreuses variétés du chiffre carré, et le fait s'est trouvé exact, puisque les dépêches étaient en effet chiffrées d'après la méthode de Beaufort, les unes avec la clef en dessous, les autres avec la clef en dessus.

*
* *

La première des dépêches chiffrées du duc d'Orléans qui a été déchiffrée est celle du 7 janvier 1899,

qui était en clair, sauf la fin 3630, 2924, 3626.

D'après le tableau, ces groupes de chiffres donnent : ZTSNZP.

On avait supposé le mot *urgent*, ce mot n'a rien donné.

On a supposé le mot *secret*. Voici ce qu'a donné ce mot :

Cryptogramme.	Z T S N Z P
Mot supposé.	s e c r e t
Clef. . . .	R X U E D I

Les trois dernières lettres EDI paraissant bonnes, il a fallu tâtonner pour les trois premières lettres et, après quelques essais infructueux, on a amené comme clef SAMEDI, et comme traduction, THURET.

Le 7 janvier étant un samedi, on a été tout de suite fixé sur la manière dont on formait la clef.

Cependant d'autres dépêches ne donnaient rien en appliquant comme clef, le jour.

Exemple : la dépêche du jeudi 2 février 1899 : 1933 2912 1437, etc., qui donne :

Cryptogramme.	I W S B D A, etc.
Clef. . . .	J e u d i
Texte clair	B I C C F

En présence de cet insuccès, on a essayé les trois

manières différentes d'obtenir un chiffre carré, et voici le résultat :

Cryptogramme	I W S B D A
Clef. . . .	J e u d i
Chiffre de Vigenère.	Z S Y Y V
Chiffre de Beaufort (clef en dessous). .	B I C C F
Id. id. (clef en dessus) . .	R A M E L

La dernière traduction était la bonne ; la méthode était connue ; les uns et les autres chiffraient d'après Beaufort, l'un en mettant la clef en dessous, l'autre en la mettant en dessus.

En effet le mot Ramel, chiffré avec la clef jeudi, donnait d'après :

VIGENÈRE	BEAUFORT	
	Clef en dessous	Clef en dessus
R A M E L	R A M E L	J E U D I
J E U D I	J E U D I	R A M E L
A E C H T	S E I Z X	I W S B D

Cette manière d'opérer ne donnait cependant aucun résultat pour d'autres dépêches.

Une répétition de trigramme et de tétragramme, produite par le hasard et non par la clef — (il en a été fait mention au chapitre II) — induisait forcément en erreur, et on a perdu de longues et nombreuses séances avant d'aboutir (Voir *Note* V).

*
* *

Ce qui a permis d'obtenir la traduction de ces cryptogrammes rebelles au déchiffrement a été

l'essai du mot « *Déroulède* », qui existait en effet dans la dépêche du 25 février et l'essai de la terminaison « *ement* » pour la dépêche du 24 février.

La dépêche du 23 février avait déjà donné le mot : *inutile* avec la clef : *qui donc*.

La traduction de ces trois cryptogrammes faite d'assaut, pour ainsi dire, c'est-à-dire lettre par lettre et en tâtonnant, a enfin donné comme clefs :

« Qui donc es-tu, visiteur solitaire?
« Assis dans l'ombre...
« Dis-moi pourquoi je te trouve sans cesse. »

*
* *

Ce résultat obtenu, les autres dépêches pouvaient être considérées comme traduites ; il était beaucoup plus simple de rechercher l'auteur de ces vers de grande allure que de continuer à se marteler le cerveau pour amener les autres dépêches, en tâtonnant sur chaque lettre.

La facture d'Alfred de Musset ayant été reconnue, la *Nuit de décembre* fut bientôt trouvée.

On correspondait en chiffres, en prenant comme clef un vers de la *Nuit de décembre* ; ce vers était celui donné par la date.

En janvier, on comptait à partir du premier vers de la poésie ; en février, on compta à partir du dernier vers, en remontant : c'est ce qu'on appelait la *clef inverse*.

CHAPITRE VI

CHIFFRE DONNÉ PAR LES CRYPTOGRAPHES CONCENTRIQUES

M. Kerckhoffs a donné quelques aperçus sur les appareils cryptographiques imaginés par MM. Mouilleron, Vinay et Gauvin, Rondepierre, Wheatstone et Silas.

M. de Viaris a également inventé un cryptographe concentrique, dont la description a été donnée par M. H. Léauté, ingénieur des Manufactures de l'Etat, répétiteur à l'Ecole Polytechnique, dans *le Génie Civil*, août 1888. — S'étant aperçu que les cryptogrammes donnés par son appareil étaient lus, il a eu le bon esprit de ne pas persister.

*
* *

On peut poser en principe que tout appareil concentrique donne un chiffre qui peut, en général, être déchiffré par une des méthodes du chiffre carré.

Parmi les cryptographes concentriques récemment inventés et qui ont été soumis à notre examen, nous citerons ceux de MM. Bord, de Nantes, et Gavrelle, de Paris.

Nous demandons pardon au lecteur de l'entretenir de faits tout à fait personnels ; mais il est nécessaire de les exposer pour bien démontrer que les cryptographes concentriques ne peuvent donner qu'un chiffre carré.

La question sera ainsi complètement élucidée, et on finira par reconnaître que ce chiffre, qui a joui d'une vogue extraordinaire, ne peut donner, malgré les précautions prises, qu'une sécurité illusoire.

APPAREIL BORD

L'appareil Bord, construit par Bréguet, est un bijou comme instrument. Son mécanisme est ingénieux, il imprime le chiffrement et le déchiffrement ; mais le chiffre qu'il donne n'a aucune valeur cryptographique.

Nous avons retrouvé dans nos papiers la correspondance échangée à ce sujet et des brouillons de déchiffrement ; nous les livrons à la publicité.

*
* *

Le chef d'état-major du XI[e] corps d'armée nous fit adresser, le 8 janvier 1891, par le capitaine de Cadoudal, huit cryptogrammes chiffrés d'après le système Bord. Il nous priait de vouloir bien les étudier, et nous invitait à lui adresser personnellement le résultat de nos recherches. Nous étions prévenu que l'alphabet ne comportait que 24 lettres et que le Q remplaçait à l'occasion le K, celui-ci étant supprimé. Toutes ces dépêches étaient chiffrées avec la même clef.

Ces dépêches furent traduites.

*
* *

M. Bord, ayant compliqué sa méthode, changea sa clef et nous fit remettre cinq nouveaux cryptogrammes, le 31 janvier 1891.

Ils eurent le même sort que les premiers.

M. Bord ne se tint pas pour battu et nous envoya encore six autres cryptogrammes, faits avec une nouvelle clef et une nouvelle méthode.

Nous les négligeâmes, jugeant que l'expérience avait été concluante.

*
* *

Croyant à l'infaillibilité de sa nouvelle méthode, M. Bord nous écrivait, le 12 mars 1891 :

« ..... Puisque vous étiez certain de déchiffrer « les dépêches imprimées par mon cryptographe, « je regrette fort que vous n'ayez pas profité de la « possession des six cryptogrammes que j'ai eu « l'honneur de vous adresser, pour me donner une « petite preuve à l'appui... Inutile de vous dire que « la clef n'est pas une phrase, mais un mot, deux « au plus. »

La petite preuve à l'appui demandée ainsi nous força pour ainsi dire à faire le déchiffrement que nous avions cru inutile. Ce fut vite fait. Le jour même, M. Bord reçut la traduction littérale des six dépêches, imprimées par son appareil.

Il y avait des nulles en tête et dans le corps des cryptogrammes.

Nous avions trouvé que F était l'indicatrice des nulles de la tête, et déterminé la longueur de la clef — 8 — par les calculs connus de tous les cryptologues.

*
* *

Nous avions établi un tableau et numéroté les alphabets donnés par l'appareil. Voici ce tableau :

ALPHABETS BORD

		A	B	C	D	E	F	G	H	I	J	L	M	N	O	P	Q	R	S	T	U	V	X	Y	Z
AN	n° 1	a	z	y	x	v	u	t	s	r	q	p	o	n	m	l	j	i	h	g	f	e	d	c	b
	n° 2	b	a	z	y	x	v	u	t	s	r	q	p	o	n	m	l	j	i	h	g	f	e	d	c
BO	n° 3	c	b	a	z	y	x	v	u	t	s	r	q	p	o	n	m	l	j	i	h	g	f	e	d
	n° 4	d	c	b	a	z	y	x	v	u	t	s	r	q	p	o	n	m	l	j	i	h	g	f	e
CP	n° 5	e	d	c	b	a	z	y	x	v	u	t	s	r	q	p	o	n	m	l	j	i	h	g	f
	n° 6	f	e	d	c	b	a	z	y	x	v	u	t	s	r	q	p	o	n	m	l	j	i	h	g
DQ	n° 7	g	f	e	d	c	b	a	z	y	x	v	u	t	s	r	q	p	o	n	m	l	j	i	h
	n° 8	h	g	f	e	d	c	b	a	z	y	x	v	u	t	s	r	q	p	o	n	m	l	j	i
ER	n° 9	i	h	g	f	e	d	c	b	a	z	y	x	v	u	t	s	r	q	p	o	n	m	l	j
	n° 10	j	i	h	g	f	e	d	c	b	a	z	y	x	v	u	t	s	r	q	p	o	n	m	l
FS	n° 11	l	j	i	h	g	f	e	d	c	b	a	z	y	x	v	u	t	s	r	q	p	o	n	m
	n° 12	m	l	j	i	h	g	f	e	d	c	b	a	z	y	x	v	u	t	s	r	q	p	o	n
GT	n° 13	n	m	l	j	i	h	g	f	e	d	c	b	a	z	y	x	v	u	t	s	r	q	p	o
	n° 14	o	n	m	l	j	i	h	g	f	e	d	c	b	a	z	y	x	v	u	t	s	r	q	p
HU	n° 15	p	o	n	m	l	j	i	h	g	f	e	d	c	b	a	z	y	x	v	u	t	s	r	q
	n° 16	q	p	o	n	m	l	j	i	h	g	f	e	d	c	b	a	z	y	x	v	u	t	s	r
IV	n° 17	r	q	p	o	n	m	l	j	i	h	g	f	e	d	c	b	a	z	y	x	v	u	t	s
	n° 18	s	r	q	p	o	n	m	l	j	i	h	g	f	e	d	c	b	a	z	y	x	v	u	t
JX	n° 19	t	s	r	q	p	o	n	m	l	j	i	h	g	f	e	d	c	b	a	z	y	x	v	u
	n° 20	u	t	s	r	q	p	o	n	m	l	j	i	h	g	f	e	d	c	b	a	z	y	x	v
LY	n° 21	v	u	t	s	r	q	p	o	n	m	l	j	i	h	g	f	e	d	c	b	a	z	y	x
	n° 22	x	v	u	t	s	r	q	p	o	n	m	l	j	i	h	g	f	e	d	c	b	a	z	y
MZ	n° 23	y	x	v	u	t	s	r	q	p	o	n	m	l	j	i	h	g	f	e	d	c	b	a	z
	n° 24	z	y	x	v	u	t	s	r	q	p	o	n	m	l	j	i	h	g	f	e	d	c	b	a

Avec ce tableau nous n'avions pas besoin de savoir le mot clef; la périodicité de la clef était 6, 1, 22, 21, 17, 12, 10, 7, et on va se rendre compte du système par la traduction de ces 6 cryptogrammes.

Nulles de tête — nombre indéterminé; la lettre F les terminait.

N° 1. — Toutes SS les X incertitudes D de Montaigne reposant son NNN esprit, etc.

N° 2. — Les X hommes Q médiocres XX jouent Q un rôle BBB dans Q de XX grands événements, etc., etc.

N° 3. — Ces SSS idées XXXY germèrent D d'autant PP plus PP promptement Q que tous, etc.

N° 4. — L'exemple XX de QQ Monsieur XQ de X La Fayette avait BB entraîné X toute QQ la Q partie BB brillante QRR de Q la XX nation.

N° 5. — La X jeune BB noblesse GGGG française X enrôlée pour QQ la X cause, etc., etc.

N° 6. — La G grande facilité FF plaît LL, mais XX n'inspire point QQ de CC confiance.

* * *

Ci-après le sixième cryptogramme de M. Bord. C'est le plus court. Le lecteur, s'il le désire, pourra s'exercer à le déchiffrer en se servant du tableau des alphabets Bord et en employant successivement les alphabets n^{os} 6, 1, 22, 21, 17, 12, 10, 7.

Les premières lettres sont nulles jusques et y compris F.

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

*
* *

Nous croyions, cette fois, en avoir fini ; mais il nous fallut compter avec la ténacité connue des inventeurs.

Le lendemain, 13 mars 1891, nouvelle lettre :

« .....Vous avez, je crois, cher Monsieur, oublié un « peu ce que je vous disais de mon appareil : je me « répète, je puis employer avec lui un très grand « nombre de méthodes.

« La première et la plus simple de beaucoup, mais « aussi la plus faible puisqu'elle revient exactement « au chiffre carré, consiste dans l'emploi d'un chiffre « sans nulles.

« Je ne vous ai pas fait l'injure de vous demander « de déchiffrer celle-là; c'est beaucoup trop facile « pour vous. Je vous ai donné des cryptogrammes à « mon avis de plus en plus difficiles pour bien « vous initier à ma méthode. C'eût été méconnaître votre très grande habileté que de supposer « que vous n'arriveriez pas à me lire... Après ces « cryptogrammes, je vous en donnerai d'autres en « augmentant graduellement la difficulté jusqu'à « l'indéchiffrabilité absolue, à moins que vous ne « vouliez que je commence par où j'aurais voulu « finir. »

*
* *

Pour terminer ces exercices, qui n'avaient plus aucun attrait pour nous, nous le priâmes de nous envoyer un seul cryptogramme, mais de sa dernière méthode cette fois, celle qu'il donnait comme étant d'une indéchiffrabilité absolue.

Nous reçûmes ce cryptogramme, le 16 mars 1891. Il portait en annotation : « Composé selon la méthode définitivement adoptée pour le cryptographe Bord ».

Ce dernier cryptogramme fut traduit. Autant que nos souvenirs peuvent nous servir, le texte clair était : « Je veux bien être pendu si vous déchiffrez celui-là. »

*
* *

Nous accusâmes réception à M. Bord de son dernier cryptogramme, en lui disant qu'il ne serait pas pendu pour cette fois, mais que nous considérions les expériences comme absolument terminées.

Nous ne l'avons plus revu, non plus qu'entendu parler de son cryptographe. Il en aura pris son parti, sans fausse honte et ne se sera pas pendu. Si tous ceux dont on lit les chiffres devaient se pendre, la corde de pendu n'aurait plus aucune vertu : il y en aurait trop.

APPAREIL GAVRELLE

De tous les cryptographes concentriques qui ont vu le jour, celui de M. Charles Gavrelle est, sans conteste, le mieux compris et le plus étudié.

Inventé en 1892, ce cryptographe fut présenté, en 1894, à la Société d'encouragement pour l'Industrie nationale, 44, rue de Rennes, à Paris.

M. le général Sebert, au nom du Comité des Arts économiques, en fit un rapport élogieux. Nous croyons utile de donner ici la description du cryptographe chiffreur de M. Gavrelle.

*
* *

L'instrument, en métal, présente d'un côté deux alphabets, de l'autre, trois alphabets concentriques dont les lettres concordent (*fig.* 1 et 2).

Le premier côté est destiné au chiffrement et au déchiffrement ; le second est destiné à la mise en position des alphabets suivant la clé convenue.

Le boîtier (*fig.* 4) se compose d'une couronne *a*, montée sur un étrier *b*, dans lequel est pratiquée une ouverture destinée à recevoir une lettre de chacun des trois alphabets (*fig.* 2).

La couronne *a* est percée de 13 ouvertures entre

chacune desquelles est gravée une lettre (*fig.* 4). Un cercle mobile *a'* (*fig.* 5) s'emboîte sous la couronne *a*, et les lettres qu'il porte, visibles par les ouvertures, constituent, avec celles de la couronne *a*, un alphabet complet dont l'ordre varie à chaque déplacement du cercle *a'* (*fig.* 1). Une vis de serrage *i* immobilise ce cercle (*fig.* 3 et 4), et rend cet alphabet fixe.

A l'intérieur de ce cercle se trouvent une couronne *c* et un autre cercle *c'* (*fig.* 1 et 5), présentant la même disposition, c'est-à-dire un alphabet mobile intérieur, lequel pivote autour de l'axe *j*, au moyen de la vis *e* (*fig.* 1 et 3); il peut ainsi occuper 26 positions différentes par rapport à l'alphabet extérieur.

La couronne *c* est fixée à un disque central *d* (*fig.* 1 et 3), à l'aide de quatre vis, et entraîne dans son mouvement de rotation, ou laisse en place, le cercle *c'* intérieur, suivant que la vis *v* (*fig.* 1 et 3) est serrée ou non.

Le contour du cercle *c'* est taillé en dents de rochet, qui viennent successivement buter contre le ressort *f*, ne permettant ainsi que le mouvement de gauche à droite de la couronne *c* et du cercle *c'*, quand la vis *e* est serrée, et seulement le mouvement inverse pour la couronne *c*, quand cette vis est desserrée, puisque le ressort arrête le cercle *c'*.

Un alphabet complet dans son ordre normal est gravé sur chacun des côtés opposés des cercles *a'*, *c'*,

et du disque *d*, chacun de ces alphabets ne pouvant présenter qu'une lettre à la fois dans l'ouverture de l'étrier *b*.

L'usage de l'instrument exige une clé formée de deux mots quelconques. Le premier mot sert au montage de l'instrument, qui s'opère de la façon suivante : les vis *e* et *i* étant desserrés, on amène, dans l'ouverture de l'étrier *b*, les trois premières lettres du premier mot, puis on serre les deux vis *e* et *i*.

*
* *

Pour chiffrer, on tourne, de gauche à droite, à l'aide de la vis *e*, l'alphabet mobile; on amène ainsi successivement en regard de l'étoile les différentes lettres du second mot de la clé, et, chaque fois, on remplace une lettre du texte clair, prise dans l'alphabet fixe, par celle qui lui correspond dans l'alphabet mobile. On répète ainsi le second mot de la clé autant de fois que cela est nécessaire pour épuiser toutes les lettres du texte clair.

Pour éviter les répétitions des lettres dans le texte chiffré, l'instrument permet: 1° le fractionnement de la clé, c'est-à-dire la possibilité de dissimuler le nombre réel des lettres qui composent cette clé; 2° le changement des lettres de l'alphabet mobile, c'est-à-dire la modification dans leur ordre.

Dans le premier cas, on inscrit non la lettre

indiquée par l'ordre de succession des lettres du deuxième mot de la clé, mais celle qui se trouve en regard de l'étoile et qui, dans le cryptogramme, devient une nulle. On reprend ensuite le chiffrement avec la lettre initiale de la clé.

Dans le second cas, pour modifier l'ordre des lettres de l'alphabet mobile, on inscrit immédiatement une seconde nulle, après l'inscription de la première (cette seconde nulle sera nécessairement la première lettre du second mot de la clé). Desserrant ensuite la vis *e*, on tourne de droite à gauche la couronne *c*, et l'on amène la lettre A en regard de l'étoile. En resserrant la vis *e*, on reprend le chiffrement, comme plus haut, avec le nouveau chiffre carré que l'on a ainsi constitué.

*
* *

Pour déchiffrer, connaissant les deux mots formant la clé, on n'a qu'à répéter les opérations précédentes en sens inverse, c'est-à-dire que les lettres du texte chiffré, prises sur l'alphabet mobile, sont remplacées par celles qui leur correspondent dans l'alphabet fixe. Quand le déchiffreur rencontre des nulles, il les passe en répétant à ces endroits exactement les mêmes opérations que le chiffreur.

En résumé, le cryptographe chiffreur permet de modifier le texte chiffré, c'est-à-dire l'ordre de suc-

cession des chiffres qui le composent, chaque fois que la disposition de ces chiffres paraît fournir une indication compromettante. Celui qui chiffre peut varier à l'infini la disposition de son texte chiffré, et cela, sans convention préalable avec son correspondant, à qui la connaissance des deux mots constituant la clé suffit toujours pour rétablir, sans difficulté, le texte clair.

On remarquera que cet instrument, qui se met à une clef donnée par un mot de trois lettres (PAR, — *fig.* 2), a une lettre sur deux de chacun de ses alphabets extérieur et intérieur, qui est variable à volonté (*fig.* 1).

*
* *

M. Charles Gravelle expose sa méthode dans un fascicule autographié de 17 pages. Dans sa conclusion, il lui donne le nom de : Procédé à clef et à chiffre carré variables.

L'inventeur s'était parfaitement rendu compte que son cryptographe et le chiffre carré étaient cousins germains; aussi tend-il à faire employer son appareil suivant les procédés de clef autoclave et indéfinie.

*
* *

De tous les cryptographes que nous avons été appelé à examiner, c'est certainement celui qui nous a donné le plus de mal à traduire.

FIG. 1.

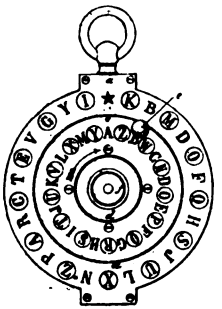


FIG. 2.

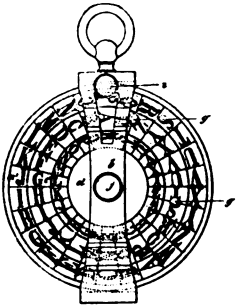


FIG. 3.

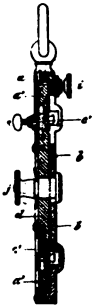


FIG. 4.

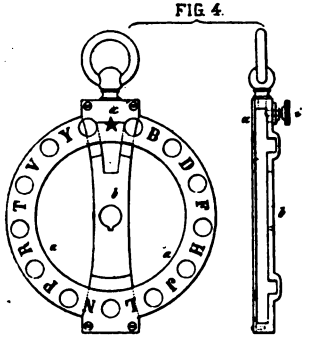


FIG. 5.

Fig. 1 à 5. — Cryptographe chiffreur de M. Gavrelle.

Il nous a fallu chercher un procédé de déchiffrement. Nous l'avons enfin trouvé dans l'étude du bigramme NT, et par la série des alphabets que pouvait donner l'appareil, soit pour les lettres mobiles, soit pour les lettres fixes.

Ci-après ces alphabets au nombre de 91 : 52 pour les lettres mobiles et 39 pour les lettres fixes.

ALPHABETS DONNÉS PAR L'APPAREIL GAVRELLE

1° *Pour les lettres mobiles du cadran extérieur.* — Ces lettres sont : ECAZXUSQOMKIG.

N°s	E C A Z X U S Q O M K I G
1	w n o p q r s t u v x y z
2	z w n o p q r s t u v x y
3	y z w n o p q r s t u v x
4	x y z w n o p q r s t u v
5	v x y z w n o p q r s t u
6	u v x y z w n o p q r s t
7	t u v x y z w n o p q r s
8	s t u v x y z w n o p q r
9	r s t u v x y z w n o p q
10	q r s t u v x y z w n o p
11	p q r s t u v x y z w n o
12	o p q r s t u v x y z w n
13	n o p q r s t u v x y z w
14	m l k j i h g f e d c b a
15	l k j i h g f e d c b a m
16	k j i h g f e d c b a m l
17	j i h g f e d c b a m l k
18	i h g f e d c b a m l k j
19	h g f e d c b a m l k j i
20	g f e d c b a m l k j i h
21	f e d c b a m l k j i h g
22	e d c b a m l k j i h g f
23	d c b a m l k j i h g f e
24	c b a m l k j i h g f e d
25	b a m l k j i h g f e d c
26	a m l k j i h g f e d c b

N°s	E C A Z X U S Q O M K I G
27	w z y x v u t s r q p o n
28	z y x v u t s r q p o n w
29	y x v u t s r q p o n w z
30	x v u t s r q p o n w z y
31	v u t s r q p o n w z y x
32	u t s r q p o n w z y x v
33	t s r q p o n w z y x v u
34	s r q p o n w z y x v u t
35	r p p o n w z y x v u t s
36	q q o n w z y x v u t s r
37	p o n w z y x v u t s r q
38	o n w z y x v u t s r q p
39	n w z y x v u t s r q p o
40	m a b c d e f g h i j k l
41	l m a b c d e f g h i j k
42	k l m a b c d e e g h i j
43	j k l m a b c d f f g h i
44	i j k l m a b c d e f g h
45	h i j k l m a b c d e f g
46	g h i j k l m a b c d e f
47	f g h i j k l m a b c d e
48	e f g h i j k l m a b c d
49	d e f g h i j k l m a b c
50	c d e f g h i j k l m a b
51	b c d e f g h i j k l m a
52	a b c d e f g h i j k l m

Observations. — Les alphabets de 1 à 13 et de 27 à 39 sont des *chiffres* mobiles; la lettre-clef, comprise de A à M, est fixe, mais essentiellement variable.

Les alphabets de 14 à 26 et de 40 à 52 sont des *chiffres* fixes ; la lettre-clef, comprise de N à W, est une lettre mobile essentiellement variable.

2° *Pour les lettres fixes du cadran extérieur.* — Ces lettres sont: BDFHJLNPRTVY.

B D F H J L N P R T V Y	Clef
m a b c d e f g h i j k	L
l m a b c d e f g h i j	K
k l m a b c d e f g h i	J
j k l m a b c d e f g h	I
i j k l m a b c d e f g	H
h i j k l m a b c d e f	G
g h i j k l m a b c d e	F
f g h i j k l m a b c d	E
e f g h i j k l m a b c	D
d e f g h i j k l m a b	C
c d e f g h i j k l m a	B
b c d e f g h i j k l m	A
a b c d e f g h i j k l	M

Observations. — Les *chiffres* sont des lettres fixes; la lettre-clef est fixe et invariable.

B D F H J L N P R T V Y	Clef
w z y x v u t s r q p o	N
z y x v u t s r q p o n	W
y x v u t s r q p o n w	Z
x v u t s r q p o n w z	Y
v u t s r q p o n w z y	X
u t s r q p o n w z y x	V
t s r q p o n w z y x v	U
s r q p o n w z y x v u	T
r q p o n w z y x v u t	S
q p o n w z y x v u t s	R
p o n w z y x v u t s r	Q
o n w z y x v u t s r q	P
n w z y x v u t s r q p	O

B D F H J L N P R T V V	Clef
w n o p q r s t u v x y	Z
z w n o p q r s t u v x	Y
y z w n o p q r s t u v	X
x y z w n o p q r s t u	V
v x y z w n o p q r s t	U
u v x y z w n o p q r s	T
t u v x y z w n o p q r	S
s t u v x y z w n o p q	R
r s t u v x y z w n o p	Q
q r s t u v x y z w n o	P
p q r s t u v x y z w n	O
o p q r s t u v x y z w	N
n o p q r s t u v x y z	W

Observations. — Les *chiffres* sont des lettres mobiles; la lettre-clef est mobile et invariable.

En examinant le dessin de l'appareil, on constatera que la figure 1 donne notre alphabet n° 31

pour les lettres mobiles et notre alphabet A pour les lettres fixes.

*
* *

M. Gavrelle nous envoya plusieurs cryptogrammes à déchiffrer; ils étaient d'une certaine longueur et chiffrés avec des clefs différentes.

Par les calculs habituels, le nombre de lettres de la clef du cryptogramme n° 1 fut déterminé : — 8.

Le mot clef fut ensuite trouvé : VICTOIRE, ou 24, 30, 36, 26, 18, 30, 15, 34.

Quatre erreurs existant dans le texte chiffré n'empêchèrent point la traduction.

*
* *

Ci-après quelques lignes du cryptogramme n° 1 et la manière de le déchiffrer.

CRYPTOGRAMME	TRADUCTION
	Clef 24 30 36 26 18 30 15 34
	V I C T O I R E
N X U L K C O U	J e m a i N T i
C C Y A V F D N	e N s e N T o u
J D V C V F F K	s P o i N T s L
C Q S N C F N N	e s i N s T R u
B F S F V Q T Y	c T i o N s D o
etc.	etc.

Nota. — Les lettres minuscules sont traduites avec les alphabets numérotés de 1 à 52 ; celles majuscules, avec les lettres-clefs.

M. Gavrelle fut fort surpris de cette traduction; mais il avait sa grande méthode en réserve :

Ruptures de la clef et nulles.

Il nous envoya un nouveau cryptogramme, qu'il considérait comme absolument indéchiffrable.

La longueur de la clef fut vite déterminée — 7; il en fut de même du mot clef: JOURNAL, ou 37, 19, 26, 16, 20, 33, 35.

*
* *

Ci-après quelques lignes de ce nouveau cryptogramme et leur déchiffrement.

TEXTE CHIFFRE	DÉCHIFFREMENT
	Clef { J O U R N A L 37 19 26 16 20 33 35
	— — — — — — —
Z U U	X L »
P O	e »
M F R I T T J	F a T a L e V
P V A B G H I	e N e m e N T
V C A R	q u e »
D M I E X T A	N o u s R e D
U C R M L H Z	o u T i o N s
G O	T »
U C H K Y C L	o u s e T D »
U V R Y E I H	o N T L a P R
etc.	etc.

Nota. — Les lettres minuscules sont traduites avec les alphabets numérotés et les majuscules avec les lettres-clefs.

Cette fois M. Charles Gavrelle fut convaincu que son chiffre n'était pas indéchiffrable, et il en prit bravement son parti.

Le 10 janvier 1895, il nous écrivait : « La clé est « bien « Journal », et le début du cryptogramme est « bien tel que vous me l'indiquez. Tous mes com- « pliments. Je vous avoue que ce résultat me paraît « réellement très savant.

« Quant aux fautes ou, du moins, à celle que vous « m'indiquez, elle est exacte ; en revoyant mon « texte, j'ai constaté que j'avais fait une erreur de « copie; c'est bien UKQ et non UKP qu'il fallait.

« ... En tous cas, dès à présent je vous remercie « de vos observations; vos critiques me sont pré- « cieuses et seront pour moi le point de départ de « nouvelles recherches. Je ne désespère pas d'ar- « river à un maniement plus simple de mon ins- « trument et surtout à ce résultat, qui me paraît dès « à présent indispensable : échapper aux erreurs « et, s'il s'en produit, faire en sorte qu'elles ne dé- « truisent pas le sens de la phrase en clair. Il y a « là encore, sur vos indications, un vaste champ « d'études à faire.

« C'est vous dire que je suis très heureux « d'avoir votre appréciation et que j'en ferai mon « profit... »

APPAREIL KRONBERG

Un autre cryptographe concentrique, en carton, imaginé par M. Kronberg, a été soumis à notre examen.

Cet appareil, trop sujet à se déplacer, ne méritait pas un examen approfondi.

Nous avons su, d'ailleurs, que M. Félix Jean d'Olivet (Loiret) avait déchiffré des dépêches que M. Kronberg lui avait données, et cela malgré des indications erronées qui l'avaient un instant dérouté.

CHAPITRE VII

DICTIONNAIRES CHIFFRÉS DU COMMERCE

Ce mode de cryptographie est de beaucoup le plus usité. Depuis l'installation des téléphones, on s'en sert moins, la communication téléphonique étant beaucoup plus rapide et bien moins coûteuse. Cependant commerçants, industriels, financiers, particuliers, etc., s'en servant pour leurs affaires, on ne peut moins faire que d'en toucher un mot.

*
* *

Les répertoires les plus connus et les plus usités sont :

En langue française : Sittler, Nilac, Bazeries ;
En langue allemande : Katscher ;
En langue italienne : Baravelli.

Pour la langue anglaise, on emploie plus généralement des *Codes*, fort complets. Mais, ceux-ci ne visant pas à l'obtention du secret des correspondances, on n'a pas à s'en occuper ici.

*
* *

Pour bien montrer au lecteur combien le secret est difficile à obtenir avec certains de ces dictionnaires, nous ne pouvons que reproduire ci-après ce que nous disions à ce sujet, en 1893[1] :

*
* *

« Lorsque le dictionnaire est bien établi, c'est le système de cryptographie le plus commode, le plus rapide et le plus facile; mais il exige le secret le plus absolu du dictionnaire dont on fait usage.

« Dès qu'on est en possession du dictionnaire dont on s'est servi, la clef se trouve avec aisance et facilité.

« Nous allons en donner une preuve, tout en indiquant la marche à suivre pour aboutir rapidement.

« Ci-après une dépêche chiffrée avec le dictionnaire abréviatif de Sittler, qui nous a été donnée à déchiffrer par une personne convaincue que l'on ne pouvait pas lire ces chiffres sans en posséder la clef:

2213	2379	2836	5034	6360	9051
1302	1086	7131	2394	7514	1933

« Ayant demandé de quoi traitait cette dépêche, il nous a été répondu : c'est une dépêche financière.

[1] *Tables chiffrantes et déchiffrantes* (A. Hermann, 8, rue de la Sorbonne, Paris, 1893 (*Introduction et usage*, page 5).

« C'était un peu vague ; aucune répétition n'existe dans cette dépêche ; elle est, de plus, fort courte. C'est donc la plus grosse difficulté qui puisse se présenter.

*
* *

« La supposition d'un mot qui, dans les systèmes de chiffrement lettre par lettre, donne toujours de bons résultats, nous donnera ici la clef du chiffre.

« Du moment que la dépêche est financière, il doit y être question de *bourse*, de *titres*, de *millions*, etc., etc.

« Essayons le mot **million.**

« Million, dans le Sittler, est à la page réelle 57 et à la ligne 04 ; la page de convention nous est inconnue ; mais la ligne, nous la connaissons, elle est invariable ; quelle que soit la clef, si **million** est dans la dépêche, il ne peut être représenté comme ligne que par 0 et 4.

« En examinant les groupes, il n'y a que le 4e qui possède un 0 et un 4 (5034) ; si 5034 représente **million,** la clef serait donc :

1er et 3e chiffre, la page 53.
2e et 4e chiffre, la ligne 04.

« Si 5034 est **million,** le groupe avant, 2836, doit représenter un nombre ; il faut chercher dans les lignes 86 la signification voulue. Si on a eu la pré-

caution de décomposer le Sittler par lignes, comme nous l'avons fait, c'est vite fait; deux solutions sautent aux yeux, et il n'y en a pas d'autres: 17, page réelle 27, et 41, page réelle 74. 17 ou 41 répondent donc à la question.

« Nous remarquons que **million**, page convenue 53, est à la page réelle 57, écart 4; que 17, page convenue 23, est à la page réelle 27, écart 4.

« La constance de cet écart nous frappe, et nous essayons aussitôt si le groupe qui précède **17 millions**, 2379, ce qui indique page convenue 27, ligne 39, ne nous donnera pas un résultat à la page réelle 31. Cet essai nous donne **emprunter.** Il n'y plus aucun doute, nous tenons la clef; car **emprunter 17 millions** ne peut être produit par le hasard.

« La clef est donc de commencer la pagination par 96, 97, 98, 99, 00, 01, etc., et d'indiquer la page convenue par le 1er et le 3^{e} chiffre du groupe transmis, et la ligne par le 2^{e} et le 4^{e} chiffre.

« La traduction de la dépêche nous donne : **Je désire emprunter 17 millions, pouvez-vous vous charger de les réaliser et à quelles conditions ?**

*
* *

« Évidemment, si la pagination n'est pas continue, c'est beaucoup plus difficile à déchiffrer; mais on y arrive tout de même, lorsque les dépêches sont

longues ou qu'on en possède plusieurs faites avec le même chiffre.

« De plus, des déchiffreurs habiles peuvent, lorsqu'ils ne possèdent pas le dictionnaire, arriver à le reconstituer. Ces travaux sont longs et laborieux, il est vrai ; mais enfin ils peuvent aboutir.

« En résumé, tels qu'ils sont établis, les dictionnaires chiffrés n'offrent aucune sécurité, au point de vue *secret*. »

*
* *

Nous n'avons rien à changer à nos appréciations antérieures.

Un récent déchiffrement retentissant va les confirmer, et le lecteur pourra constater, sans aucun doute possible, que c'est la fixité des deux chiffres indiquant la ligne qui a dû permettre la traduction de la fameuse dépêche Panizzardi, qui a fait et fait encore tant de bruit.

CHIFFRE PANIZZARDI

Au récent procès de Rennes (août-septembre 1899) il a beaucoup été parlé du télégramme en chiffres envoyé de Paris à Rome, le 2 novembre 1894[1], par le colonel Panizzardi, attaché militaire italien.

On a dit par ailleurs[2] : « De même que c'est dans les ratures d'un écrit qu'il faut chercher la pensée première de l'auteur, c'est dans les parties chiffrées d'une pièce qu'il faut trouver la note juste et le fait historique certain. »

En effet, ceux qui correspondent secrètement avec un chiffre fait par eux-mêmes ne peuvent se figurer que des spécialistes puissent quelquefois parvenir à lire leurs cryptogrammes; aussi ne dissimulent-ils pas leur pensée et disent-ils à cœur ouvert tout ce qu'ils ont à se dire.

*
* *

Le texte chiffré de la dépêche Panizzardi n'a pas été publié. La traduction vraie n'a été donnée, en audience publique, qu'en bribes dispersées.

[1] *Nota : La Libre Parole* venait de divulguer l'arrestation du capitaine Dreyfus.

[2] *Les chiffres de Napoléon Ier pendant la Campagne de* 1813, déjà cité, p. 12.

Tout ce que nous en savons nous a été appris par le compte rendu sténographique du *Figaro*[1].

Cependant il en a été assez dit, en audience publique, au cours du procès de Rennes, pour pouvoir déterminer sûrement de quel chiffre se servait l'attaché militaire italien, à Paris, pour sa correspondance secrète avec le chef d'État-Major de l'armée italienne.

En effet, il a été dit que le mot *preuve* excluait le mot *relations* et que les mots *émissaire prévenu* et *commentaires de la presse* s'excluaient également.

Il n'en fallait pas autant pour découvrir et affirmer que le colonel Panizzardi faisait usage d'un *Baravelli*.

*
* *

Comme le lecteur le sait, le *Baravelli* est un dictionnaire chiffré, en langue italienne, existant dans le commerce.

En ouvrant ce livre, on trouve *relazione* à la ligne 88 de la page 75, et *provi* à la ligne 88 de la page 71; *prevenuto emissario* aux lignes 91 et 65 des pages 69 et 30, et *commentare stampa* aux lignes 91 et 65 des pages 17 et 88.

Comme on peut s'en convaincre, les mots : *relazioni*, *provi*, *prevenuto*, *commentare*, *emissario*,

[1] Voir principalement les nos 224 *bis* et 236 *bis* des 12 et 24 août 1899.

stampa, s'excluent l'un l'autre; il n'y a donc aucun doute à avoir lorsqu'on affirme que Panizzardi se servait d'un *Baravelli*. C'est aussi clair que la lumière du jour.

*
* *

De tout ce qui précède, il se dégage que le *Paolo Baravelli* ne vaut pas mieux pour la sécurité d'un chiffre que le *Sittler* français[1].

Le *Baravelli* se divise en quatre parties :

1re partie. — Voyelles et signes de ponctuation;
2e partie. — Consonnes, terminaisons, etc.;
3e partie. — Syllabes;
4e partie. — Mots usuels.

Cette dernière partie est composée, comme les dictionnaires français existant dans le commerce, de 100 pages contenant chacune 100 lignes.

Comme au *Sittler*, les deux chiffres représentant la ligne sont fixes; c'est une première faute au point de vue : *secret*.

En outre, si, pour transmettre un mot, on emploie un groupe de quatre chiffres, deux représentant la page convenue et les deux autres la ligne où se

[1] *Nota*. — On traite ici une question technique de déchiffrement; le lecteur n'a pas à y chercher ce qui n'existe pas dans la pensée de l'auteur.

trouve le mot à transmettre, avec le *Baravelli*, lorsqu'il faut chiffrer une voyelle ou un signe de ponctuation, une consonne ou une terminaison, une syllabe, on n'emploie que des groupes de 1, 2 et 3 chiffres seulement.

Cette différence dans le groupement saute aux yeux; c'est un indice révélateur. Si, de plus, on a la mauvaise idée de chiffrer la ponctuation, la traduction en clair n'est plus qu'un jeu, pour un cryptologue un peu exercé, et en peu de temps il trouve la loi qui a présidé à la pagination du dictionnaire.

Cette loi trouvée, la traduction n'est plus discutable.

FIN DE LA DEUXIÈME PARTIE

TROISIÈME PARTIE

ÉTUDE SUR LES CHIFFRES MILITAIRES FRANÇAIS

CHAPITRE PREMIER

CHIFFRES DE NAPOLÉON Ier

Les chiffres de Louis XIV, réputés indéchiffrables, ont été déchiffrés[1] ; ces chiffres étaient, en général, fort bien établis; on sentait la main d'un cryptologue, et dans la confection du chiffre, et dans la manière de s'en servir.

En effet, il n'était point fait usage de séries alphabétiques, lesquelles sont toujours désastreuses; on employait plusieurs chiffres pour les lettres et mots les plus usités, de manière à éviter la fréquence et les répétitions qui trahissent le secret; il n'y avait pas de mots en clair dans les correspondances pour ne pas indiquer le sujet traité, etc., etc.

[1] *Le Masque de Fer*, par E. Burgaud et le commandant Bazeries. Paris, 1893, Firmin Didot.

*
* *

Cent ans se passent; la cryptographie est délaissée; nous arrivons à Napoléon Ier, et nous constatons que le chiffre militaire est de beaucoup inférieur à celui de Louis XIV.

Les précautions prises par le Grand Roi ont été perdues de vue par le Grand Empereur; il y a bien encore un *grand chiffre* et un *petit chiffre*, mais il n'y a plus de chiffre de réserve sous pli cacheté; on trouve du clair en abondance au milieu des chiffres, etc., etc.

Les généraux de Napoléon étaient bons pour battre l'ennemi et gagner des batailles, ce qui d'ailleurs était leur rôle et dans leur tempérament, mais ils étaient nuls en fait de cryptographie. Cela se conçoit aisément: les guerriers ne sont pas faits pour faire de la cryptographie; ils marchent droit au but et ne s'entortillent pas dans les subtilités d'une science de casse-tête.

Il faut donc leur donner un *chiffre* facile à employer, et c'est à ceux qui l'établissent qu'il incombe d'en connaître la force et la faiblesse.

*
* *

Nous pourrions citer quantité d'exemples de la faiblesse du chiffre de Napoléon Ier et de l'inhabi-

leté à s'en servir des généraux de l'époque, voire même du major général Alexandre Berthier. Nous n'en donnerons que deux; ils édifieront le lecteur [1].

[1] Les dépôts d'archives ne mettant pas encore à la disposition du public les papiers des règnes de Louis XVIII, Charles X, Louis-Philippe, 2e République et Napoléon III, il ne nous a pas été possible de parler des chiffres de ces époques.

Les cryptologues de l'avenir constateront assurément que la faiblesse des chiffres n'a fait que s'accentuer.

PREMIER EXEMPLE

Dépêches chiffrées de Berthier et d'Augereau
Marche du corps d'observation de Bavière sur Leipzig

Nous avons trouvé aux *Archives nationales* et au *Dépôt de la Guerre* quelques documents chiffrés prescrivant la marche du corps d'Augereau sur Leipzig.

Ces documents étant inédits, il nous a paru intéressant de les publier, non seulement parce qu'ils se rapportent à la période de marche qui a précédé la bataille de Leipzig — bataille de quatre jours qui a décidé du sort du monde, d'après le *Bulletin prussien* du 19 octobre 1813, — mais surtout en vue de bien faire voir les erreurs commises par Augereau en chiffrant.

Si Augereau battait facilement Lichtenstein et Thielmann, les chiffres avaient le don de l'embrouiller; à tout instant, il se trompait; le lecteur pourra en juger.

*
* *

Nous commençons par donner la dépêche chiffrée qui prescrivait à Augereau de marcher en droite ligne sur Iéna par Cobourg.

Elle existe en primata et en duplicata au *Dépôt de la Guerre*[1]; elle est faite avec le petit chiffre, et la traduction en manque.

La manière de chiffrer n'ayant pas été la même pour le duplicata, nous donnons les deux textes chiffrés avec la traduction littérale sous chaque groupe.

Péterswald, ce 17 septembre 1813.

Monsieur le Maréchal, duc de Castiglione, l'Empereur ordonne que vous vous portiez le plutôt possible 167, 138, 169, 106, 171, 15, 117, avec son infan-
s u r la sa a le
terie, sa cavalerie et son artillerie, en ne laissant 15, 164, 138, 169, 176, 166, 35 138, 169, 81, que ce que Sa
a v u r t z bo u r g
Majesté a désigné pour 106, 78. Son principal but
la garnison
sera de rester 107, 87, 176, 169, 53, 52, 167, 52, 35. 138, 6
ma i t r e de s de bo u c
85, 82, 52, 106, 171, 15, 117 et de chasser 117, 167, 156 169,
h es de la sa a le le s pa r
145, 171, 115, 167, 68 qui manœuvrent dans 20, 176, 131,
ti sa n s ennemis ce t te
75. Vous pouvez vous rendre en droite ligne, 156,
direction pa
169, 40, 35, 138, 169, 81, 167, 138, 169, 87, 53, 91.
r co bo u r g s u r l é na

Le prince vice-connétable,
Major général,

Signé : ALEXANDRE.

[1] Correspondance de Napoléon Ier, non publiée.

Duplicata.

Péterswald, le 17 septembre 1813.

Monsieur le Maréchal, duc de Castiglione, l'Em-
pereur ordonne que 175, 138, 167, 164, 9', 138, 167, 152,
vo u s v o u s po
169, 145, 53, 166, 117, 137, 103, 157, 176, 152, 167, 134, 37, 117,
r ti e z le p lu to t po s si b le
174, 169, 106, 171, 15, 117, 15, 132, 6, 175, 176, 126, 48,
su r la sa a le a ve c vo t re infanterie
164, 153, 126, 32, 50, 175, 176, 126, 25, 68, 94,
v ot re cavalerie et vo t re artillerie en ne
106, 122, 171, 115, 176, 15, 164, 138, 169, 166, 35, 138, 169, 81,
la is sa n t a V u r z bo u r g
136, 20, 173, 138, 53, 171, 107, 87, 82, 131, 15, 52, 134, 81, 94
que ce q u e Sa Ma j es te a de si g ne
137, 90, 138, 169, 106, 51, 169, 116, 168, 115, 175, 176, 126, 137,
p o u r la ga r ni so n vo t re p
148, 115, 6, 119, 156, 96, 3, 176, 177, 146, 52, 169, 82, 131, 169,
ri n c i pa l bu t se ra de r es te r
107, 92, 126, 52, 167, 23, 53, 35, 138, 6, 61, 167, 52, 106, 171, 39,
ma it re de s d e bo u c he s de la sa al
53, 50, 52, 6, 72, 167, 177, 169, 117, 167, 137, 22, 145, 171, 115,
e et de c ha s se r le s p ar ti sa n
167, 68, 154, 107, 94, 138, 164, 126, 115, 176, 16, 115,
s ennemis qui ma ne u v re n t da n
167, 20, 176, 131, 67, 126, 6, 145, 175, 138, 167, 152, 138, 132
s ce t te di re c tion vo u s po u ve
166, 164, 90, 138, 167, 126, 115, 23, 126, 68, 23, 159, 92, 53, 93,
z v o u s re n d re en d ro it e li
81, 94, 137, 22, 6, 90, 35, 138, 169, 81, 174, 169, 119, 53, 115, 15.
g ne p ar C o bo u r g su r l e n a.

Le prince vice-connétable,
Major général,

Signé : ALEXANDRE.

Les personnes appelées à faire usage d'un *chiffre* pourront faire des réflexions salutaires en examinant les deux textes chiffrés du major général Berthier.

Supposons que ces deux dépêches soient tombées entre les mains de l'ennemi.

L'examen sommaire des deux textes montre aussitôt que c'est la même dépêche; d'ailleurs on a eu soin de l'indiquer en mettant en clair « duplicata ».

Le primata contenant du clair et du chiffre et le duplicata étant entièrement en chiffres, il est on ne peut plus facile de retrouver dans les chiffres du duplicata le clair du primata.

Ce chiffre est immédiatement perdu, surtout si c'est un petit chiffre.

Si c'est un grand chiffre, fût-il de 2 ou 3.000 groupes, il est bien malade. Cela peut paraître extraordinaire, mais c'est cependant la vérité absolue, et tous les cryptologues seront de notre avis, à ce sujet.

* * *

Augereau marchait sur Leipzig; ci-après quatre lettres inédites de sa correspondance.

PREMIÈRE LETTRE

—

Naumbourg, le 9 octobre 1813,
à 4 heures 1/2 après midi.

« Monsieur le duc, malgré la bonne volonté de « la troupe, il est impossible qu'elle aille aujourd'hui plus loin que cette ville, il fait un temps si « affreux que les trois quarts des soldats sont restés « en arrière, et si je poussais plus loin dans cette « journée, j'arriverais presque seul sans infanterie « à Leipzig. Je vous prie de faire ce rapport à Sa « Majesté.

« Je désirerais savoir si je dois après-demain « entrer dans Leipzig ou m'arrêter au dehors de « la ville.

« J'ai rencontré de nombreuses évacuations de « malades esclopés, et je ne sais comment ces « hommes pourront passer, l'ennemi m'accompagnant à petite distance de mon arrière-garde ; il « a bivouaqué à deux lieues de moi cette nuit.

« Recevez, Monsieur le duc, l'assurance de ma « parfaite considération. »

Le Maréchal d'Empire,

Signé : AUGEREAU,
DUC DE CASTIGLIONE.

DEUXIÈME LETTRE

Stöhsen, le 10 octobre 1813,
6 heures 1/2 du soir.

SIRE,

« Ainsi que j'ai eu l'honneur d'en rendre compte « hier à Votre Majesté que l'ennemi m'avait tou- « jours suivi ; aujourd'hui il a retardé ma marche. Je « l'ai trouvé occupant le pont de Vétau, la position « presque inexpugnable qu'il avait pris a été enlevée « à la bayonnette, les troupes se sont battues à mer- « veille surtout la jeune infanterie; dans la plaine « de Stöhsen, route de Zeitz, la cavalerie a exécuté « des charges sanglantes et aussi belles que j'en « aye jamais vu. Chacun a fait son devoir; le com- « bat a duré depuis 4 heures du matin jusqu'à « 4 heures du soir. L'ennemi a été mis en déroute « *complette* et poursuivi pendant quatre heures; « sa perte est considérable, la notre est de très peu « d'hommes tués, il y a quelques blessés. Nous « avons fait des prisonniers, je n'en sais point « encore le nombre précis.

« Le prince de Lichtenstein, les généraux Thiel- « mann et Biron étaient présents, ils avaient tout « réuni. Demain je reprends la route si l'ennemi

« ne veut pas recommencer, ce que je ne crois pas,
« il a été trop bien mené par la cavalerie.

« Lorsque tous les rapports me seront parvenus,
« j'aurai l'honneur d'en adresser un général à
« Votre Majesté.

Je suis, Sire, de Votre Majesté,
Le très fidèle sujet,
Le Maréchal d'Empire,

Signé : AUGEREAU,
DUC DE CASTIGLIONE.

TROISIÈME LETTRE

—

(*Chiffrée par Augereau lui-même*)

164, 53, 87, 167, 87, 115, 58, 96, 167, le 11 octobre, dix h. du soir.
V e i s i n fe l s

123, 169, 53, 6, 138, 167, 53, 138, 96, 53, 114, 53, 115, 176, 52, 138,
J'ai r e c u s e u l e m e n t de u
151, 52, 175, 167, 137, 15, 142, 157, 15, 115, 157, 87, 53, 175, 138,
x de vo s p a y to a n to j e vo u
167, 15, 87, 107, 115, 10, 29, 173, 138, 53, 87, 15, 175, 87, 167, 37,
s a i ma n d bi q u e j a vo i s b
15, 176, 176, 138, 77, 53, 169, 96, 87, 6, 85, 131, 87, 115, 50, 176,
a t t u hi c r l i c h te i n et t
85, 87, 53, 96, 107, 115, 173, 138, 53, 87, 53, 58, 169, 15, 87, 167,
h i e l ma n q u e j e fe r a i s
68, 167, 90, 169, 176, 53, 52, 114, 53, 169, 53, 115, 10, 169, 53, 52,
en s o r t e de me r e n d r e de
107, 87, 115, 15, 117, 87, 137, 141, 81, 167, 87, 96, 68 115,
ma i n a le i p si g s i l ennemi n
53, 114, 53, 71, 137, 15, 167, 15, 169, 53, 176, 169, 90, 81, 146,
e m e force p a s a r e t r o g ra
52, 169, 87, 53, 175, 138, 167, 15, 87, 107, 115, 175, 142, 53, 169,
de r j e vo u s a i ma n vo y e r
138, 115, 6, 90, 169, 137, 167, 15, 138, 10, 53, 170, 115, 176, 52,
u n c o r p s a u d e va n t de
114, 90, 87, 15, 96, 138, 176, 166, 53, 115.
m o i a l u t z e n.

Signé : Ml. A.

Cette dépêche est si mal chiffrée, les erreurs sont si nombreuses, qu'il y a lieu d'en rectifier le déchiffrement.

Weiszenfels, le 11 octobre, à 10 heures du soir.

« J'ai reçu seulement deux de vos pay[1].

« Tantôt, je vous ai mandé que j'avais battu « Lichtein[2] et Thielmann, que je ferais en sorte de « me rendre demain à Leipzig si l'ennemi ne me « force pas à rétrograder.

« Je vous ai[3] m'envoyer un corps au devant de « moi à Lutzen. »

[1] Sans doute *paquets* ou *paysans*.
[2] *Lichtenstein*.
[3] Sans doute, *prié de*.

QUATRIÈME LETTRE

—

Leipzig, le 12 octobre 1813, 5 h. 1/2 du soir.

« SIRE,

« J'ai l'honneur de rendre compte à Votre Majesté « que je suis arrivé ici il y a deux heures, avec « environ 8.000 hommes d'infanterie et 3.000 che- « vaux ; l'ennemi qui était venu avec 6.000 chevaux « occuper Lutzen, l'a abandonné à mon approche. « J'aurai l'honneur d'observer à Votre Majesté qu'il « me sera difficile d'exécuter de grands mouve- « ments avec 8.000 hommes d'infanterie. J'attends « les ordres de Votre Majesté. »

Je suis, Sire, de Votre Majesté,
Le très fidèle sujet,
Le Maréchal d'Empire,

Signé : AUGEREAU,
DUC DE CASTIGLIONE.

*
* *

Nous croyons utile de placer ici un document inédit, sans signature, daté du 13 octobre 1813. Il se trouve aux *Archives nationales*, carton AF IV 1666, et renferme quelques chiffres non traduits :

« Le affaires vont toujours au mieux.

« Le roi de Naples avait battu le 10, à Borna, le « général Vittgenstein qui s'était retiré sur Froh- « bourg; mais, ce général ayant été joint par le « prince de Schwarsenberg, le roi de Naples qui « attendait la jonction du duc de Castiglione a pris « une position en avant de Leipzig.

« Le duc de Castiglione a rencontré, du côté « de Weissenfels, les généraux Thielmann et « Lichtenstein, leur a fait un millier de prisonniers, « leur a tué et blessé beaucoup de monde. Trois « régiments, parmi lesquels sont celui de La Tour « et un régiment de hussards noirs prussiens ont été « presque entièrement détruits. Le duc de Casti- « glione a fait sa jonction hier, en avant de Leipzig.

« Sur notre droite, nous nous sommes emparés « des ponts et de la tête de pont de Wartembourg. « Nous avons enlevé avec une telle rapidité les « ouvrages de l'ennemi sur la Mulde, qu'il n'a « pas eu le temps de détruire ses ponts. Nous « sommes entrés à Dessau. Nous y avons fait

« 3.000 prisonniers, dont 1 colonel, 2 majors et « 50 officiers, tous prussiens. Le général Yorck a « été blessé mortellement. On a remarqué pour la « première fois, parmi les prisonniers, un grand « nombre de cosaques. Le bataillon de la Vengeance « a été détruit. On lui a pris ses deux pièces de « canon.

« Le général Regnier, qui avait passé l'Elbe à « Wittemberg, a marché sur Roslau dont il a « trouvé le pont levé. Il y a eu hier une canonnade « de deux heures. Il a fait 600 prisonniers. Il a « continué sa marche sur Aken, pour détruire le « seul pont qui reste à l'ennemi sur l'Elbe.

« Il paroit qu'une cinquantaine de mille hommes, « y compris les Suédois, se voyant coupés, ont « passé sur la rive droite.

« L'Empereur se porte à merveille; le Roi, la « Reine et la princesse de Saxe se portent égale- « ment bien.

441, 201, 711, 402, 45, 516, 33, 351, 1125, 18, 1136, 759, 330, 277, 564, 351, 1069, 597, 622, 389, 1140, 1135, 638, 261, 912, 893, 1117, 625, 488, 1013, 597.	*Aujourd'hui nous sommes* avec le roi, la reine et la princesse de Saxe, à Eilenbourg, l'Empereur est encore cette nuit à Duben[1].

[1] *Nota.* — Le déchiffrement est certain, sauf pour les trois premiers mots en italique, qui, faute d'éléments suffisants, n'ont pu être contrôlés.

« L'interruption des communications est un effet « inévitable des grands mouvements qui s'opèrent « et qui ont tous été prévus. On ne doit pas croire « les bruits que les ennemis ne manqueront pas de « répandre. »

13 octobre 1813.

« *P.-S.* — Les lettres de Dresde, datées d'hier 12, « annoncent que l'ennemi, qui n'a pas des forces « assez considérables disponibles, n'a rien tenté « contre cette ville. »

DEUXIÈME EXEMPLE.

Dépêche chiffrée du général Rapp. — Siège et défense de Danzig[1]

La relation de la défense de Danzig, en 1813, *par le Xe corps de l'armée française contre l'armée combinée russe et prussienne* a été publiée en 1820 par P.-H. d'Artois, capitaine du génie.

Cette relation complète un ouvrage publié à ce sujet, en 1814, par M. M***, attrayant par la pureté et la grâce d'un style fleuri, mais fort incomplet, d'après le capitaine d'Artois.

Celui-ci a rédigé sa relation d'après les rapports et journaux officiels de l'Etat-Major général, de l'artillerie et du génie. M. le lieutenant Rommeru, chargé de la correspondance particulière du général Rapp à Danzig, lui a fourni une grande quantité de notes.

Le général Chasseloup a aussi écrit sur le siège de Danzig; son manuscrit est à la Bibliothèque de la Guerre[2].

D'après d'Artois, peu de jours après l'incendie des magasins de vivres, le gouverneur avait expé-

[1] Nous avons conservé à Danzig l'orthographe de l'époque.

[2] A. 2.
d. 588

dié par mer son aide de camp, le capitaine Marnier, pour faire part à Napoléon de sa pénible situation.

Sa lettre commençait ainsi :

« Notre position, Sire, est des plus affligeantes et « si vos armes ne vous mettent en état de faire « lever bientôt le siège, la seule perspective de « cette garnison, qui s'est immortalisée par de longs « et continuels succès, est de terminer, par la cap- « tivité, une défense aussi glorieuse. »

« Venait ensuite la décomposition de l'effectif.

« Le général Rapp exposait les pertes en vivres « qu'il avait éprouvées par les incendies et le peu « de ressources qui lui restaient. Enfin il dépeignait « l'esprit dont était animée la plus grande partie « de la garnison : les Polonais vivement sollicités, « les Bavarois rappelés par leurs souverains, incer- « tains jusqu'à ce qu'ils fussent suffisamment éclai- « rés sur l'authenticité des ordres qui leur étaient « parvenus; toutes les troupes de la Confédération « désertant en détail et prêtes à nous abandonner en « masse.

« Le général, inquiet sur le sort du capitaine Mar- « nier qui pouvait si facilement tomber entre les « mains de l'ennemi, et ne recevant aucune nou- « velle, se décida à envoyer le duplicata de ses « dépêches par un espion.

« Cet homme profita, pour sortir de la ville, du « départ d'une vingtaine d'habitants qui s'embar-

« quèrent à Neufahrwasser, dans la nuit du 15 au « 16 novembre, pour se rendre à Pillau. »

*
* *

La lettre chiffrée du général Rapp, datée du 6 novembre 1813, existe au *Dépôt de la Guerre*. Elle provient de la succession Marnier. Elle ne parvint donc pas à destination, pas plus que le duplicata envoyé par un espion. Cette lettre n'avait jamais été déchiffrée; elle n'est pas tout à fait telle que le capitaine d'Artois l'a donnée ou analysée.

Le lecteur va en juger.

Danzig, le 6 novembre 1813.

SIRE,

J'envoye près de Votre Majesté un de mes aides de camp pour lui rendre compte

52, 106, 167, 119, 150, 15, 145 52, 106
137, 106, 20 de 12, 46, 107, 96, 61, 138
169, 119, 169, 126, 156, 146, 37, 117, 82. 176
22, 148, 132, 119, 6, 119 dans la 104, 119
176, 76, 137, 126, 95, 62, 15, 138, 52, 138
151 de ce 111, 119, 167, 117, 58, 15, 6, 149, 174
99, 117, 167, 45, 145,53, 169, 167 de 121, 167
19, 137, 137, 159, 161, 167, 119, 90, 94, 99, 115
167, 50, 134 les 22, 114, 53, 167 de V. M.
94. 106, 99, 176, 176, 68, 176, 68, 50, 34, 52.
69, 119, 126, 37, 119, 68. 157, 176, 117, 132, 169.
117, 167, 119, 53, 60, 106, 177, 138, 117, 165, 169

de la situation de la place de Danzig. Un malheur irréparable est arrivé ici dans la nuit du premier au deux de ce mois. Le feu a consumé les quartiers de nos approvisionnements et si les armes de Votre Majesté ne la mettent en état de faire bientôt lever le siège la seule perspective de cette place qui

167, 165, 6, 145, 132, 52, 20, 176, 176, 53, 78
qui s'est 97, 111, 169, 158, 93, 177, 53 par 52
110, 115, 81, 167 et continuels 174, 6, 6, 53, 167
82, 176 de 176, 62, 95, 94, 169 par la 4, 137
145, 161, 131, 46, 53, 52, 134 glorieuse.

119, 53, 119, 139, 115, 167, 15, 20, 146, 137
137, 90, 169, 176 les 53, 158, 176, 167 de
134, 150, 15, 145 des 176, 159, 138, 137, 137
53, 167 tant 9, 142, 90, 115, 115, 53, 176
176, 53, 167 que 107, 106, 52, 167 et 6
149, 170, 117, 167, 20, 115, 178, 167 ;
117, 167, 53, 158, 176, 167 :

Du service dans la place 71, 169, 176, 167
53, 151, 131, 148, 53, 138, 139, 167 et 15
170, 115, 176 - 137, 90, 167, 131, 167 :
52, 167, 23, 53, 177, 169, 131, 138, 169. 167 ;
du 107, 131, 148, 63 de 96' 25 ;
les 99, 169, 6, 138, 148, 15, 117, 167 ;
des 15, 137, 137, 150, 161, 134, 90, 115
115, 53, 99, 115, 167 et des 165, 167, faites
par 96' 74, 52, 96' 118 ;
de la 40, 114, 152. 134, 145 successive de
la 146, 145 et celle 21, 150, 53, 96, 96, 53 ;
de la 4, 119, 167, 167, 53.

Par le 1er 53, 158, 176 Votre Majesté 132
169, 169, 15, combien est 126, 76, 119, 176, 117, 67
151, 119, 53, 114, 53, 40, 169, 137, 137 et elle jugera
23, 53, 96' 97, 152, 134, 29, 93, 131
qu'une 78, 15, 138, 167, 167, 119, 73
90, 119, 37, 117 put 52, 73, 73, 68, 23, 126, 12
jusques 15, 138, 111, 119, 167, 52, 114, 15, 119, 15
119, 115, 134 que V. M. 96', 15, 175, 119, 176

s'est immortalisée par de longs et continuels succès est de terminer par la captivité une défense si glorieuse.

Je joins à ce rapport les états de situation des troupes tant bayonnettes que malades et convalescents

les états

Du service dans la place
forts extérieurs et avant-postes ;
des déserteurs ;
du matériel de l'artillerie ;
les mercuriales :
des approvisionnements et
des pertes faites
par l'effet de l'incendie,
de la composition succes sive de la ration et celle actuelle ; de la caisse.

Par le premier état Votre Majesté verra combien est réduit le dixième corps et elle jugera de l'impossibilité qu'une garnison aussi faible pût défendre Danzig jusques au mois de mai ainsi que Votre Majesté

52, 134, 126 quand on 86, 176, 137, 15, 169 13', 104 à 171, 138, 132, 169 les 174, 37, 134 167, 158, 115, 20, 167. Elle daignera d'ailleurs ne pas 165, 169, 23, 126, 52, 124, 53, 136, 20 176, 176, 53, 78, 167', 15, 73, 73, 139, 37, 96, 119 176, 6, 85, 15, 136, 119, 90, 138, 169, non seulement 156, 169, 117, 58, 52, 96' 68, 107 119, 167, 68, 40, 126, 156, 169 la 52, 177, 169 145 et 156, 169, par 117, 167, 107, 106, 67, 53 167 qui 15, 138, 81, 141, 53, 115, 131, 159, 115 176 de 137, 103, 167 en 137, 103, 167, tant par l'effet de la 107, 138, 170, 122, 53, 171 122, 149 et de la 148, 54, 53, 138, 169 du 6 93, 107, 176 que par le 177, 169, 161, 20 très 69, 145, 51, 115, 176 qu'elle a à faire. Je 174, 137, 137, 93, 53, 68, 40, 126, V. M. de remarquer que toutes 20, 167, 176, 159 138, 165, 167, ne 138, 115, 176, 156, 167 également 176, 126, 167 et que le 177, 169, 161, 20 le plus 165, 116, 37, 117 doit 94, 20, 167, 171, 87, 126 99, 115, 176, 126, 157, 114, 37, 62 sur les 99, 108 117, 138, 126, 167.

J'ai fait pour 145, 126, 169, 156, 145, des 126, 167, 168, 138, 169, 20, 167 en 66, 114, 99 167, tout ce que mon 155, 117 pour le 177 169, 161, 20 de V. M. a pu me dicter. J'ai fait 68, 176, 126, 169 successivement dans les 4, 23, 126, 167 des 40, 114, 9, 176, 158, 115, 167 tout les 66, 114, 99, 167 français 90, 138, 39 93, 82 en 50, 34 de 152, 169, 131, 169, 117, 167

l'aurait désiré quand on eut parvenu à sauver les subsistances. Elle daignera d'ailleurs ne pas perdre de vue que cette garnison s'affaiblissait chaque jour non seulement par le feu de l'ennemi, mais encore par la désertion et par les maladies qui augmenteront de plus en plus, tant par l'effet de la mauvaise saison et de la rigueur du climat que par le service très fatigant qu'elle a à faire. Je supplie encore Votre Majesté de remarquer que toutes ces troupes ne sont pas également très [1] et que le service le plus pénible doit nécessairement retomber sur les meilleures.

J'ai fait pour tirer parti des ressources en hommes tout ce que mon zèle pour le service de Votre Majesté a pu me dicter. J'ai fait entrer successivement dans les cadres des combattants tous les hommes français

[1] Manque un mot, non chiffré, qui doit être *sûres*.

22, 99, 167.

J'ai 71, 169, 99 sous 117, 121, 114 de Bataillons 76, 159, 87, 52, 159, 99, 46, 126, 79, 99, 115, 176 dont les 44, 137, 126, 95, 62, 167, 13 se composent de 128, 87, 6, 87 62, 167, et S. 128, 87. 6, 87, 62, 167 et le 26me, 52, 167, 55, 137, 110, 142, 82, 52, 96'22 dont on pourrait absolument 67, 152, 177, 169 sans 22, 126, 131, 169, le service de 96'24, 95, 116, 167, 176, 146, 145. J'ai également 6, 126, 53, un 9 158, 108, 110, 115 de 56, 138, 15, 94, 167 composé 68, 156, 169, 145, 53 de 60, 115, 167 du 156, 142, 167, une 40, 114, 156, 81, 116, 53 de 152, 114, 127, 62, 137 choisis dans nos 90, 138, 164, 148, 62, 167, 95, 93, 158, 87, 169, 167 de 107, 148, 94 et dans ceux du 156, 142, 167 existe 59, 39, 117, 99, 115, 176. Enfin je 115, 36, 148, 68, 94, 81, 93, 60 pour augmenter 117, 121, 114, 37, 126, 52 52' 73 68, 177, 138, 169, 167.

96, 50, 34 du service 58, 146, 40, 115, 91, 92, 126 à Votre Majesté, comment 117, 167, 176, 159, 138, 165, 167, 168, 115, 176, 55, 137, 110, 142, 82 et combien 63, 117, 167, 149, 176, 52, 69, 145, 54, 82, 15, 174, 137, 152, 169, 131, 169, 69, 145, 54, 82, 154, 94, 58, 159, 115, 176, 136, 167', 21, 6, 159, 92, 126.

Celui 52, 167, 52, 167. 62, 131, 138, 169, 167,

ou alliés en état de porter les armes.

J'ai formé sous le nom de Bataillons du Roi de Rome un régiment dont les deux premiers bataillons se composent d'officiers et sous-officiers et le troisième des employés de l'armée dont on pouvait absolument disposer sans arrêter le service de l'administration. J'ai également créé un bataillon de douanes composé en partie de gens du pays. Une compagnie de pompiers choisis dans nos ouvriers militaires de marine et dans ceux du pays existe également. Enfin je n'ai rien négligé pour augmenter le nombre des défenseurs.

L'état du service fera connaître à Votre Majesté comment les troupes sont employées et combien elles ont de fatigues à supporter, fatigues qui ne feront que s'accroître.

Celui des déserteurs in-

indiquera d'abord à Votre majesté par le nombre de ceux de chaque 176, 159, 138, 165 qu'elles sont celles de ces 176, 159, 138, 165, 167 174, 169, 117, 167, 136, 149, 165, 138, 176, 117, 137, 103, 167, 90, 138, 111, 118, 167, 40, 114, 137, 131, 169, il n'est pas douteux que la 52, 177. 169, 145, 149, 167, 15, 138, 81, 99, 115, 131, 146 et par raison des 69, 145, 54, 182, 53, 151, 20, 137, 134, 132, 167 et par la 177, 76, 6, 145, 154, a toujours 93, 53, 138, 131, 96, 167 moyens 173, 138, 149, 137, 126, 115, 94, pour 96'55. 165, 6, 61, 169; 68, 83, 115, 156, 169, 106, 52, 58, 6, 145, 52, 167, 39, 93, 82. 154, 94 paraît 136, 176, 159, 137, 20, 169, 158, 118, 53.

diquera d'abord à Votre Majesté par le nombre de ceux de chaque troupe qu'elles sont celles de ces troupes sur lesquelles on peut plus ou moins compter, il n'est pas douteux que la désertion s'augmentera et par raison des fatigues excessives et par la séduction qui a toujours lieu tels moyens qu'on prenne pour l'empêcher; enfin par la défection des alliés qui ne paraît que trop certaine.

L'état des 66, 74, 99, 167, 15, 96'66, 127, 158, 96, 115', 82, 176, 156, 167, 68, 40, 169 bien 40, 115, 134, 52, 146, 37, 117, 107, 122, 108, 167, 15 138, 81, 99, 115, 131 chaque 119, 90, 138, 169 et le 107, 96, viendra tout 15, 40, 138, 137-52, 119, 15 la 83, 54, 126, 76, 168, 15, 165, 169, 76 cet 36, 169, 52, 171, 115, 131 que la belle 171, 122, 149, 103, 87 avait 126, 115, 76, et l'on remarque chaque 87, 90, 138, 169, qu'il sera 29, 68, 157, 176, 34, 131, 118, 176, 52, 106, 107, 106, 67, 53, qui le 99, 91, 20.

L'état des hommes à l'hôpital n'est pas encore bien considérable, mais il s'augmente chaque jour et le mal viendra tout à coup. déjà la figure du soldat a perdu cet air de santé que la belle saison lui avait rendu et l'on remarque chaque jour qu'il sera bientôt atteint de la maladie qui le menace.

Le 107, 131, 148, 63, 52, 96',25, 168, 138, 73, 73, 126 beaucoup par le 145, 169, 52, 96', 68 et surtout par le 121, 176, 126 mais il se 126, 156, 126, continuellement: nos 152, 138, 23, 126, 167, 67, 95,

Le matériel de l'artillerie souffre beaucoup par le tir de l'ennemi et surtout par le nôtre, mais se

104, 68, 176 aussi 40, 115, 134, 52, 146, 37, 117, 99, 115, 176. Cependant ce n'est pas 20, 154, 121, 138, 167, 107, 115, 136, 146, 117, 137, 103, 157, ainsi que Votre Majesté le verra par les 50, 34, 167, 76, 60, 117, 127, 115.

répare continuellement ; nos poudres diminuent aussi considérablement. Cependant ce n'est pas ce qui nous manquera le plus ainsi que Votre Majesté le verra par les états du général Lepin.

Le 50, 34, 52, 106, 4, 122, 177, 115, 82, 176, 156, 167, 137, 103, 167, 171, 145, 167, 58, 171, 115, 176, que le 126, 167, 131, il est 76 actuellement 26, 111, 122, 52, 168, 96, 52 à la 176, 159, 138, 165 et 1, 111, 122, 15, 138, 151 aux 128, 87, 6, 87, 62, 167 cependant tout est 87, 6, 119 à des 137, 148, 151, 53, 151, 20, 167, 134, 73, 167, 20, 136, Votre Majesté pense bien 107, 122, 136, 117, 167, 99, 169, 6, 138, 169, 87, 15, 96, 82 lui 53, 151, 137, 93, 136, 159, 115, 176 avec 52, 158, 108. — 96'55, 137, 140, 115. 176, 71, 169, 20, 15, 137, 159, 76, 92, 15, 165, 118, 53, 67, 151, 2, 20, 115, 176, 95, 96, 117, 73, 146, 115, 6, 167 et toutes 117, 167, 126, 167, 168, 138, 169, 20, 167, 168, 115, 176, 53, 162, 122, 53, 82.

L'état de la caisse n'est pas plus satisfaisant que le reste, il est dû actuellement trois mois de solde à la troupe et cinq mois aux officiers, cependant tout est ici à des prix excessifs, ce que Votre Majesté pense bien, mais que les mercuriales lui expliqueront en détail.

L'emprunt forcé a produit à peine dix-neuf cent mille francs et toutes les ressources sont épuisées.

La composition des 146, 145 actuelles est bien 118, 174, 73, 83, 171, 115, 131, elle est au 52, 167, 168, 138, 167 de celle 21, 40, 169, 52, 53 en temps de 126, 152, 167, je l'ai 123, 76, 92, 53 aux plus 165, 145, 131, 82, 173, 138, 15, 115, 145, 131, 167, 152, 167, 134, 37, 117, 167, mais une plus forte 126, 76, 6, 145 conduirait plus 23', 66, 114, 99, 167, 15, 96'66, 127, 158, 96, en ferait 52, 177, 169, 131, 169, 23'15. 138, 276, 126, 167, 50,

La composition des rations actuelles est bien insuffisante, elle est au-dessous de celle accordée en temps de repos, je l'ai réduite aux plus petites quantités possibles, mais une plus forte réduction conduirait plus d'hommes

121, 138, 167, 165, 169, 23, 148, 149, 167 ainsi beaucoup 52, 52, 138, 169, 157 pour 99, 91, 60, 169, 136, 136, 161, 164, 126, 167.

Votre Majesté remarquera sans doute que nous sommes 90, 37, 93, 60, 167, 52, 23, 90, 115, 115, 62, 76, 177, 87, 81, 117 aux 6, 61, 170, 138, 151, c'est un moyen qui m'a 167, 118, 54, 93, 53, 126, 99, 115, 176, 126, 162, 81, 94, 107, 87, 167, il faut considérer que ces 15, 116, 107, 138, 151, 167, 90, 115, 176, 118, 67, 167, 165, 115, 167, 15, 37, 117, 167, puisque depuis longtemps nous 115', 15, 175, 115, 167, 137, 103, 167, 23', 15, 138, 176, 126, 167, 37, 82, 145, 15, 138, 151, 137, 90, 138, 169, 106, 121, 138, 148, 150, 126, 52, 167, 176, 159, 138, 137, 82, 137, 90, 87, 115, 176, 23, 53, 177, 96 pour les 40, 115, 20, 169, 132, 169, 15'9, 150, 167, 96'25 doit d'ailleurs en 126, 177, 169 132, 169, une 20, 169, 158, 87, 94, 173, 138, 15, 115, 145, 131 pour son 177, 169, 161, 20, cette, 22, 99, devant conduire son 107, 131, 148, 63, 174, 169, des 152 très 53, 117, 132, 82; nos 111, 138, 93, 115, 167 à 107, 94, 60 et nos 107, 6, 85, 87, 115, 82, 85, 142, 23, 169, 15, 138, 93 ques en 94, 20, 167, 167, 87, 131, 115, 176 aussi, il en 69, 138, 176, 68, 40, 126 pour les 176, 146, 115, 167, 152, 169, 176, 167, 90, 37, 93. 60, 167 de la 71, 169, 145, 83, 4, 145, enfin pour 20. 138, 151, 52, 96'15, 23, 95, 116, 167, 176, 146, 145. Votre Majesté verra au surplus 173, 138', 15, 138, 157. 158, 96, la 146, 145 est 17, 169, 176, 118, 58, 148, 53, 138, 126 à celle 21, 40, 169, 52, 53 aux 6, 61, 170, 138, 151, 52, 176, 159,

à l'hôpital, en ferait déserter d'autres et nous perdrions ainsi beaucoup de défenseurs pour ménager quelques vivres.

nous sommes obligés de donner du seigle aux chevaux, c'est un moyen qui m'a singulièrement répugné, mais il faut considérer que ces animaux sont indispensables puisque depuis longtemps nous n'avons plus d'autres bestiaux pour la nourriture des troupes, point de sel pour les conserver abattus. L'artillerie doit d'ailleurs en réserver une certaine quantité pour son service, cette arme devant conduire son matériel sur des positions très élevées ; nos moulins à manège et nos machines hydrauliques en nécessitent aussi, il en faut encore pour les transports obligés de la fortification, enfin pour ceux de l'administration. Votre

138, 165, 167.

Nos 165, 167, 16, 115, 167, 96'118, 76, 46, 15, 138, 44 sont 97 et telle chose 173, 138, 90, 115, 162, 87, 137, 167, 53, 69, 87, 126, 63, 117, 167, 126, 76, 87, 177, 115, 176, 106, 52, 15. 45, 11, 87, 167, 15, 138, 137, 103, 167.

Toutes les 137, 126, 4, 138, 145, 152, 167, 167, 87, 37, 117, 167, 15, 175, 87, 68, 176, 53, 131, 137, 148, 177, 1 7, 152, 138, 169, 137, 126, 132, 116, 169, 117, 52, 171, 167, 176, 126 dont nous sommes 117, 137, 161, 6, 145, 99, 167, 107, 87, 167 elles ont 53, 6, 66, 138, 53, contre 96' 74, 52, 167, 37, 90, 114, 37, 82 et 86, 177, 53', 167, 118 aires 52, 167, 37, 90, 138, 117, 176, 167, 159 138, 60, 167, 68, 73, 118 de tous les moyens de 52, 167, 176, 140, 6, 145 imaginables que 96' 68, 105, 96, 145, 137, 93. 53. 68, 40, 126 chaque 119, 90, 138, 169 vers tout les 152, 87, 115, 176, 167, 76, 6, 90, 169, 137, 167 de la 137, 106, 20.

Les 107, 95, 93, 158, 87, 126, 167 qui auraient $\hat{76}$, $\hat{53}$, 176, 126, 6, 149, 167, 176, 140, 87, 176, 167 de manière 15, 174, 137. 137, 90, 169, 131, 169, 52, 167, 37, 93, 115, 16, 60, 167 n'étaient que les 81, 146, 115, 23, 167, 107 dans lesquels 117, 167, 107, 169, 6, 85, 15, 115, 23. 167. 52, 12, 126, 115, 58, 169, 107, 87, 53, 115, 176, 117, 138. 169, 167, 81, 146, 87, 115, 167 aucun 71,

Majesté verra au surplus qu'au total la ration est fort inférieure à celle accordée aux chevaux de troupes.

Nos pertes dans l'incendie du 1er au 2 sont immenses et telle chose qu'on puisse faire elles réduisent la défense à quatre mois au plus.

Toutes les précautions possibles avaient été prises pour prévenir le désastre dont nous sommes les victimes, mais elles ont échoué contre l'effet des bombes et fusées incendiaires des boulets rouges, enfin de tous les moyens de destruction imaginables que l'ennemi multiplie encore chaque jour vers tous les points du corps de la place.

Les magasins militaires qui auraient dû être construits de manière à supporter des blindages n'étaient que les grands magasins dans lesquels les marchands de Danzig ren-

115, 23. 167, 115', 15, 142, 15, 115, 176, 53, 131. 69, 87, 176, pour la 40, 115, 167, 176, 140, 6, 145 des 15, 37, 148, 167, 118. 67, 167, 165, 115, 171, 37, 117, 167 dans un 134, 53, 60, 119', 15, 175, 87, 167, 137, 126, 124, 96' 53, 132, 94, 99, 115, 176 qui nous est 22, 148, 132 et l'on avait 176, 146, 115 167, 137, 90, 169 176 par mes ordres 46, 53, 137, 15. 169, 176, 89, 53, une 137, 15, 169, 176, 89, 53 de 121, 167, 81, 146, 89. 115, 167 dans des 59, 93, 177, 167 que 119, 15, 175, 87, 167 fait 89, 169, 117, 139, 15, 20, 176, 74, l'une de 20, 167, 59, 93, 177, 167 est continuellement 176, 146, 132. 169, 177, 53, 156, 169, 117, 167, 37, 133, 37, 53, 167. mais pourtant les 81, 146, 87, 115, 167, 167', 142, 40, 115, 20, 169, 132, 115, 176 ; 96' 15, 138, 176, 126 est 68, 40, 126, 118, 158, 6, 131.

96' 119, 167, 117. 52, 106, 111, 176, 176, 106, 138, (67, 176, 167, 165, 87, 6, 85, 62) qui 126, 115, 58, 169, 107, 87, 176, 106, 107, 119, 53, 138, 126, 156, 169, 145, 53, de nos 15, 137, 137, 159, 161, 134, 90, 94, 99, 115, 167, 71, 169, 107, 81, 176, un commandement particulier aux ordres d'un 40, 110, 94, 96, 23, 25, 40, 176, 176, 87, 115, il avait pour 24, 119, 90, 87, 115, 176, un chef de bataillon 50, 26, 24, 119, 90, 87, 115, 176, 167 un nombre suffisant de 152, 167, 131, 167, 15, 175, 87, 176, 53, 131, 137, 106, 20, aux 122 174, 53, 167, des 60, 115, 167, 23, 22, 99, 167, étaient également aux ordres du commandant de 106, 137, 106, 20, 46, 53, 40, 114, 156, 81, 116, 53 de 20, 115, 176, 1, 15, 115, 176, 53, 152, 114, 127, fermaient leurs grains, aucun fonds n'ayant été fait pour la construction des abris indispensables dans un siège. J'avais prévu l'événement qui nous est arrivé et l'on avait transporté par mes ordres une partie de nos grains dans des églises que j'avais fait irler [1] à cet effet, l'une de ces églises est continuellement traversée par les bombes mais pourtant les grains s'y conservent: l'autre est encore intacte.

L'isle de la Mottlau (ditspeicher) qui renfermait la majeure partie de nos approvisionnements formait un commandement particulier aux ordres d'un colonel d'artillerie Cottin il avait pour adjoint un chef de bataillon et trois adjoints, un nombre suffisant de postes avait été placé aux issues, des gens d'armes étaient également aux ordres du

[1] *Fermer*, sans doute.

53, 169, 167, bien 90, 169, 51, 116, 177, 53 étaient aussi 34, 158, 6, 85, 82, avec 5, 152, 114, 165, 167, à cette 119, 167, 117 pour la sureté de la 173, 138' 63, 117, 119, 15, 175, 87, 167, 137, 169, 87, 167, 46, 22, 126, 131, très 148, 65, 138, 126, 138, 151, Tout a été 87, 104, 145, 117. 117, 137, 126, 95, 53, 169, 121, 132, 114, 37, 126, 15, 41, 61, 138, 126, 167, 76, 167, 139, 169, 46, 118, 90, 6, 6, 15, 134, 90, 94 par 46 53, 37, 133, 37, 53, 118 aire, 177, 107, 116, 58, 167, 158 dans le 107, 23' 46, 72, 29, 158, 115, 176, 20, 107, 86, 176, bientôt, 90, 138, 132, 139, 176, 107, 87, 167 les 73, 106, 99, 167, 167', 50, 68, 67, 126, 115, 176 avec une 131, 96, 117, 146, 127, 67, 131, 173, 138' 108, 69, 96, 103, 176, 167, 90, 6, 6, 138, 137, 165, 169 à 40, 138, 137, 53, 169, 96, 118. On 52, 137, 110, 142, 15, tous les 111, 112, 68, 167, 119, 107, 79, 91, 37, 117, 167, pour y 156, 169, 132, 116, 169, 107, 87, 176, 46, 132, 115, 176, des plus 161, 90, 117, 115, 176. 126, 81, 115, 15, jusques au 117, 115, 52, 107, 87, 115, 50, 126, 115, 67, 176, 89, 104, 145, 117 tous les 177, 40, 138, 169, 167 que nous 152, 169, 158, 99, 167, 15, 121, 167, 53, 158, 37, 93, 167, 177, 99, 115, 176, 167. Avant ce même 118, c'est à dire vers 26, 61, 138, 126, 167, 46, 15, 138, 176, 126, 58, 176, 126, 167 considérable 167', 53, 158, 89, 176, 107, 116, 58, 167, 131, à la pointe de 96. 122, 117, 108, 6, 149, 174, 107, aussi beaucoup de 107 mais il ne méritait plus d'attention puisqu'il était 53, 110, 87, 81, 94 de nos 81, 169, 53, 116, 53, 169, 167, au moment ou 96', 118 était le plus animé 96' 68, 15, 176, 158, 173, 138, 15, 101, 132, 99, 115, 176, nos avant postes 15, 90, 85, 169, 15 et 167, commandant de la place une compagnie de cent cinquante pompiers bien organisée étaient aussi attachés avec 5 pompes à cette isle pour la sûreté de laquelle j'avais pris un arrêté très rigoureux. Tout a été inutile; le 1er novembre à 6 heures du soir un incendie occasionné par une bombe incendiaire se manifesta dans le magasin d'un habitant, ce magasin est bientôt ouvert mais les flammes s'étendirent avec une telle rapidité qu'il fallut s'occuper à couper l'incendie. On déploya tous les moyens imaginables pour y parvenir mais un vent des plus violents régna jusqu'au lendemain et rendit inutiles tous les secours que nous portâmes à nos établissements. Avant ce même incendie, c'est à dire vers trois heures un autre feu très considérable s'était manifesté à la pointe de l'isle, il consuma

6, 85, 87, 23, 93, 176, 166, il fallut y 152, 169, 131, 169, 52, 167, 176, 159, 138, 165, 169 et cela 67, 95, 104, 15, d'autant 121, 167, 111, 142, 68, 167, d'arrêter 96', 118.

Je dois faire remarquer d'ailleurs à Votre Majesté que depuis le bombardement, 149, 94, 165, 138, 176, 104, 96, 117, 99, 115, 176, 40, 114, 137, 131, 169, sur le 177, 40, 138, 169, 167, 52, 167, 72, 29, 158, 115, 167 qui 6, 146, 113, 94, 115, 176, 50, 117, 167, projectiles 50, 106, 52, 167, 176, 140, 6, 145, de leurs 107, 87, 168, 115, 167, ou de leurs 74, 167 pendant qu'ils seraient 18, 177, 115, 176, 167.

Un premier incendie très considérable avait eu lieu déjà dans la nuit du 19 au 20 octobre dans l'Isle de la Motlau, 46, 5, 4, 177, 169, 94, 167, 149, 176, 53, 131, 106, 137, 159, 87, 53, 52, 167, 73, 106, 114, 99, 167, mais on était 156, 169, 132, 194, 15, 22, 126, 131, 169, 117, 58, 15, 138, 111, 99 115. 176 où 108, 52, 170, 92, 51, 81, 94, 169, 120, 167, 107, il n'y avait pas 52, 87, 90, 138, 169, où

aussi beaucoup de magasins ; mais il ne méritait plus d'attention puisqu'il était éloigné de nos greniers, au moment où l'incendie était le plus animé l'ennemi attaqua vivement nos avant postes à Ohra et Schidlitz, il fallut y porter des troupes et cela diminua d'autant nos moyens d'arrêter l'incendie.

Je dois faire remarquer d'ailleurs à Votre Majesté que depuis le bombardement on ne peut nullement compter sur le secours des habitants qui craignent et les projectiles et la destruction de leurs maisons ou de leurs effets pendant qu'ils seraient absents.

1 — casernes ont été la proie des flammes, mais on était parvenu à arrêter le feu au moment où il devait gagner nos magasins, il n'y avait pas de

149, 115, 50, 70, 81, 91, 92, 117, 58, plusieurs fois dans cette 122, 117, d'autres 118, 177, 107, 116, 58, 167, 158, 87, 68, 176 à tous 111, 99, 115, 167 dans les différentes 156, 169, 145, 82, 52, 106, 161, 96, 117, et 96 ' 68, les rend toujours 137, 103, 167, 161, 147, 117, 115, 176, 167 en 106, 115, 4, 115, 176 sur les lieux où ils se 52, 6, 106, 126, 115, 131, 115, 176, toutes sortes de 137, 159, 119, 53, 6, 145, 117, 167. Enfin, Sire, je le répète le 107, 96, 61, 138, 169, qui nous 21, 4, 37, 117 aujourd'hui devait 22, 148, 132, 169, 137, 103, 167, 158, 169, 23, et il était impossible de 117, 137, 126, 132, 116, 169, sans aucune 15, 37, 148, contre un bombardement 167, 90, 138' 31, 104.

jour où on n'éteignait le feu plusieurs fois dans cette isle, d'autres incendies se manifestaient à tous moments dans les différentes parties de la ville et l'ennemi les rend toujours plus violents en lançant sur les lieux où ils se déclarent toutes sortes de projectiles. Enfin, Sire, je le répète le malheur qui nous accable aujourd'hui devait arriver plus tard et il était impossible de le prévenir sans aucun abri contre un bombardement soutenu.

J'adresse à Votre Majesté, un mémoire que j'ai fait r édiger par le général Campredon, je n'entre donc dans aucun détail sur l'objet de ce mémoire, j'ai e mpli les lacunes que ce rapport laisse sur l'état de otre défense.

J'ai lieu d'être satisfait de toutes les armes, c'est à ui se distinguera le plus et il n'y a pas de jours que nous n'ayons de traits honorables à citer. Le général Breissand a été frappé d'une balle à la tête il y a quelques jours, il est douteux qu'il survive à cette blessure. Les généraux Grandjean, d'Handelet, Bachelu, ont rendu de grands services, le général Campredon joue un rôle bien distingué dans notre défense, le colonel Richemont le seconde comme à l'or-

dinaire, le génie prend des peines infinies, le général Lepin sert avec la plus grande distinction et son arme acquiert chaque jour plus de droits à la bienveillance de Votre Majesté.

Le général Cavaignac a fait des grenadiers de sa cavalerie que nous avons mis à pied, il leur donne le plus bel exemple ainsi que le général Farine. Le général Dumanoir tire aussi bon parti des marins sous ses ordres, et j'ai beaucoup à me louer de son zèle.

J'ai lieu d'être satisfait aussi de la division Napolitaine commandée par le général Detrès qui est parvenu à l'acclimater, le général Pepé qui a perdu la moitié du pied lors de la retraite de Moscou a voulu partager les fatigues de ses camarades quoique ses plaies ne soient pas encore cicatrisées.

Je ne dois pas finir sans faire observer à Votre Majesté, que 106, 78, 94, 177, 40, 114, 152, 177 en parti que 23, 39, 93, 82, 50, qu'il n'y a 52, 73, 146, 115, 4, 122, 136, 106, 44, 2me, 67, 106, 111, 92, 53, 52, 106, 44, 23me, 50, 96, 82, 44 régiments 52, 32, à peu près 106, 111, 92, 53, 52, 96', 25, 117, 60, 116, 53, 106, 107, 148, 94, 50, 106, 44, 22me, 67, 174, 169, laquelle je 6, 159, 122, 136, 96, 149, 165, 138, 176, 40, 114, 137, 176, 62.

la garnison ne se compose en partie que d'alliés et qu'il n'y a de français que la 2me division, la moitié de la 23me et les deux régiments de cavalerie, à peu près la moitié de l'artillerie, le génie, la marine et la 22me division sur laquelle je crois que l'on peut compter.

Je suis avec le plus profond respect, Sire, de Votre Majesté Impériale et Royale, le très humble et fidèle sujet.

Signé : RAPP.

Le lecteur constatera que, par les clairs qui existent en aussi grande quantité dans cette dépêche, on peut trouver facilement le chiffre.

En effet le passage : « Tant par l'effet de la 107, 138, 170, 122, 53, 171, 122, 149 et de la 148, 54, 53, 138, 169, du 6, 95, 107, 176, que par le 177, 169, 161, 20 très 69, 145, 51, 115, 176 qu'elle a à faire », permet sans grands efforts d'imagination de supposer comme fin de phrase : « que par le service très pénible ou fatigant qu'elle a à faire. »

Donc 177	égale	se		
169	—	r		
161	—	vi		
20	—	ce		
et 69	—	pe	ou	fa
145	—	ni	—	ti
51	—	b	—	ga
115	—	l	—	n
176	—	e	—	t

Ce point de départ est largement suffisant pour reconstituer un chiffre de 200 groupes.

Si la dépêche avait été bien chiffrée, le cryptologue aurait peiné un peu pour cette reconstitution, mais il y serait parvenu tout de même.

Telle qu'elle a été chiffrée, avec des clairs, des apostrophes, des accents circonflexes, des terminaisons, etc. — ce qui dénote chez le chiffreur une ignorance complète des règles cryptographiques — la reconstitution du chiffre devient un simple amusement.

*
* *

Il paraît intéressant de donner ici la décomposition de l'effectif du Xe corps, à la date du 6 novembre 1813 :

Malades	aux hôpitaux.	1.182	4.097	17.597
	à la chambre.	2.915		
Gendarmerie, employés des administrations, travailleurs non armés			600	
Combattants.			12.900	

Les 12.900 combattants se décomposaient comme il suit :

Artillerie :	français.	900	1.600	12.900
	allemands et polonais.	700		
Génie :	français.	240	320	
	polonais.	80		
Dépôt de la garde impériale			250	
Marine.			480	
Cavalerie :	français.	700	950	
	polonais.	250		
Infanterie :	français.	3.500	9.300	
	polonais.	3.300		
	napolitains.	1.300		
	allemands	1.200		

*
* *

Par suite de nouveaux désastres occasionnés par le bombardement, la capitulation de Danzig eut lieu le 17 novembre 1813. Elle fut signée par Alexandre, duc de Wurtemberg, général de cavalerie et géné-

ral en chef de l'armée combinée devant Danzig, et par le comte Rapp.

La garnison devait être renvoyée en France sur parole de ne pas servir avant échange; mais la convention ne fut pas approuvée par l'Empereur de Russie.

L'évacuation de Danzig n'eut lieu que le 2 janvier 1814. Les Français furent emmenés prisonniers de guerre en Russie; les Allemands, les Polonais et les Napolitains qui faisaient partie de la garnison furent renvoyés dans leurs foyers.

*
* *

Nous donnons à l'*Appendice*, *note IX*, la table déchiffrante du petit chiffre de Napoléon Ier, en 1813.

*
* *

Pour reposer le lecteur de l'aridité des chiffres, il nous paraît intéressant de publier un rapport du capitaine Marnier, aide de camp du général Rapp, rapport peu connu et ayant toutes les allures d'un roman d'aventures.

RAPPORT du chef d'escadron Marnier, aide de camp du général en chef comte Rapp, sur la mission qu'il eut à remplir vers la fin du siège de Danzig, en 1813.

Nous étions en novembre 1813, et le siège durait depuis dix mois; bloqués par terre et par mer, nous avions épuisé une partie de nos munitions; l'Empereur était à 300 lieues de nous, et les communications, même par espionnage, étaient absolument impossibles. Nous tenions toujours, nous luttions contre le danger et contre les besoins de toute espèce.

Sur ces entrefaites, un incendie nous consuma quatre mois de provisions. Cet événement, qui rendait notre situation affreuse, décida le général en chef, comte Rapp, à tenter un dernier effort pour apprendre à l'Empereur l'extrémité où la garnison était réduite. Une légère embarcation reçut l'ordre de mettre à la voile. Je m'offris pour la commander et j'obtins cet honneur. L'expédition était extrêmement périlleuse; il fallait braver la flotte anglo-russe qui observait Danzig, avertie par des transfuges de ce qui se préparait et tromper ensuite la vigilance des nombreux vaisseaux dont nos ennemis couvraient la mer.

Le navire qu'on mit à ma disposition se nommait *l'Heureuse Tonton*, capitaine Dumoutier; il portait

cinq petits pierriers et dix fusils. L'équipage était composé d'une manière assez bizarre : sur huit matelots, il y avait deux français, un espagnol, deux allemands, un danzigois et une espèce de cosmopolite qui ne parlait que le jargon des gens de mer, et comprenait cependant toutes les langues, chacun de ces hommes était marin depuis son enfance. Je les avais choisis, et, quoiqu'ils fussent de nations différentes, je pouvais compter sur eux. Quant au capitaine, c'était un jeune homme aussi courageux qu'habile.

Le 7, je me rendis à Fahrwaser; j'y trouve mes hommes et mon bâtiment prêts à mettre à la voile. J'attendis le vent. Le 8 au soir, il souffla dans une direction favorable. La clarté de la lune, qui était d'abord dans son plein, permettait à la flotte anglo-russe de suivre tous nos mouvements.

Nous partîmes, et contre toutes les probabilités, nous eûmes le bonheur d'échapper aux vaisseaux ennemis, dont la plupart étaient sous voiles; bientôt nous fûmes hors de leur portée.

Nous avions à peine doublé la pointe d'Héba (six lieues de Danzig) que les vents nous devinrent totalement contraires; notre goëlette fatigua considérablement.

Cependant les Anglais, instruits de mon départ, avaient envoyé dix bâtiments à ma poursuite. Le 9, vers les dix heures du matin, nous en aperçûmes

cinq qui se dirigeaient sur nous; mais il survint un coup de vent si terrible, que chacun d'eux songea plutôt à sa propre sûreté qu'à continuer la chasse, et bientôt nous cessâmes de les voir. Nous n'échappâmes à un danger que pour en courir un autre. Quoique nous fussions à la cape, une bourrasque nous poussa avec une effroyable rapidité vers les côtes de Suède, et nous reçûmes une telle secousse que le lest fut jeté de babord à tribord, et que, pendant plusieurs minutes, notre bâtiment avait cessé d'obéir au gouvernail. Il penchait tellement que l'eau entrait dans la cale par les écoutilles; nous coupâmes aussitôt les écoutes et nous parvînmes à remettre le bâtiment en équilibre, en nous portant tous à babord et en vidant l'eau avec des seaux, car la pompe était engagée.

A l'entrée de la nuit, le vent se calma, sans que nous puissions néanmoins nous en rendre maîtres. L'orage avait été si violent qu'il nous avait été impossible de calculer notre route; et sans savoir au juste où nous étions, nous avions l'horrible certitude que nous approchions des côtes de Suède, qui sont hérissées d'écueils.

Le moment où les flots nous laissèrent plus tranquilles nous livra à nos propres pensées; elles étaient affreuses, comme notre position. Portés au milieu d'une mer orageuse par un frêle navire, incapables, désormais, de résister au premier coup de

vent, nous avions, pour toute perspective, trois maux différents : les Anglais, les Suédois ou les flots; mais notre courage ne nous abandonna pas, et, résignés à tout, nous attendîmes les événements.

A onze heures, nous fûmes poussés sur la côte, et nous périssions infailliblement, si notre bâtiment n'eût été enclavé entre deux rochers qui le soutinrent.

Nous jetâmes à la mer tout notre lest ainsi que nos pierriers, excepté un seul, et après huit heures de travaux, pendant lesquels le vent se calma un peu, nous parvînmes à nous dégager. Nous mîmes aussitôt à l'ancre, mais il nous fut impossible d'arrêter totalement une voie d'eau considérable, formée dans ce dernier choc.

Le lendemain 10, au point du jour, nous aperçûmes la terre dont nous n'étions éloignés que de 400 toises environ; c'était l'île suédoise d'Œland; quelques barques de pêcheurs vinrent nous voir. Nous nous dîmes Prussiens. Elles nous apportèrent du poisson, du beurre, des œufs et quelques autres provisions. Nous employâmes toute la journée à réparer nos avaries.

Le 11, notre position resta la même; le 12, deux officiers suédois se rendirent à notre bord pour visiter nos papiers. Comme ils ne parlaient pas allemand, nous feignîmes de ne pas les entendre, et leur montrâmes un pavillon prussien. Notre con-

duite ne parut pas les satisfaire, et nous nous séparâmes, eux mécontents et nous fort inquiets.

Le 13, plusieurs barques, sur l'une desquelles était le pasteur de Kerglosa, s'approchèrent de nous; nous ne voulûmes recevoir que ce dernier. Il parut surpris de notre défiance, et nous apprit que, d'après les lois, les officiers, que nous avions vu la veille, avaient droit à la moitié des bâtiments naufragés; bien qu'il nous parla comme à des alliés, il nous quitta, entièrement convaincu que nous étions Français. Dès ce moment, nous vîmes bien que nous avions tout à redouter. Pendant le reste de la journée, des rassemblements eurent lieu en divers endroits sur le rivage, et nous remarquâmes un grand mouvement d'hommes à pied et à cheval. Bien certains que nous étions l'objet de ce tumulte, nous aurions voulu nous éloigner de ces parages; mais un calme plat nous en empêchait. Nous passâmes la nuit dans des transes mortelles et sous les armes, décidés à vendre cher notre liberté.

Le 14, un canot vint à bord avec une lettre du pasteur; il invitait le commandant à se rendre à terre avec quelques hommes de sa suite, pour y assister au service divin et dîner chez lui. Je devinai facilement ses intentions; je lui fis, en allemand, une réponse fort polie, et donnai quelques pièces de monnaie à ses messagers.

Cependant notre situation devenait de jour en

jour plus pénible. Nous ne pouvions douter de ce que les Suédois méditaient contre nous; nos petites provisions s'épuisaient; point d'espérance de les remplacer et presque aucune de nous éloigner des côtes; car, ayant jeté tout notre lest, nous ne pouvions plus tenir la mer, que dans le cas seulement où nous aurions été favorisés par une légère brise d'est.

Dans cette cruelle extrémité, après de mûres réflexions, je m'arrêtai à une résolution qui me parut la seule digne de dix soldats de la garnison de Dantzig. J'assemblai mon petit équipage et je leur déclarai que nous débarquerions la nuit suivante, et qu'après avoir transporté à terre nos munitions et nos vivres, et coulé notre bâtiment nous irions nous emparer de vive force d'une des tours qui servent pour les signaux; que de là nous irions faire une incursion dans la ferme la plus voisine, y prendre des vivres pour un mois, nous retrancher ensuite et forcer le commandant de l'île à nous accorder une capitulation honorable. Le jeune Dumoutier, plein d'enthousiasme, ordonna à l'instant les préparatifs, et chacun de mes matelots travailla sans relâche en attendant le moment favorable pour mettre notre projet à exécution, mais un nouveau danger qui nous survint nous empêcha de l'exécuter.

Le lendemain matin 15, vers les 8 heures, nous eûmes en vue deux bâtiments que nous reconnûmes

pour anglais et qui semblaient se diriger vers nous.

La mer commençait à devenir houleuse et tout présageait un gros temps. Nous remarquâmes bientôt que des deux bricks un seul venait à nous. La situation affreuse dans laquelle nous nous trouvions nous faisait une loi de tout oser, je me décidai à l'attaquer.

Je fais donner à mes matelots double ration d'eau-de-vie, et nous courons sur les Anglais, ils nous laissent approcher sans défiance. Arrivés près d'eux, nous hissons pavillon français et faisons une décharge de notre pierrier et de notre mousqueton. Ils ripostent, la fusillade s'engage. Pendant trois quarts d'heure on se bat avec acharnement de part et d'autre. Cependant l'eau continuait de pénétrer dans notre navire, et comme nos gens avaient été contraints d'abandonner la pompe, nous étions au moment d'être submergés. A cette vue je prends mon parti, j'ordonne de monter à l'abordage, nous accrochons le bâtiment ennemi et, au moment où nous nous en rendions maîtres, le nôtre aussitôt disparaît sans même que nous ayons le temps de sauver nos effets.

Tout mon équipage fit preuve en cette affaire d'une rare intrépidité et mérita les plus grands éloges, notamment le jeune capitaine Dumoutier.

Le brick capturé s'appelait *les Deux Jumeaux*, capitaine Williams Beel, du port de 290 tonneaux, portant 25 hommes d'équipage et 4 canons. Il

retournait de Riga à Londres, chargé de graine de lin, de caviar, etc. Il faisait partie d'un nombreux convoi, escorté par des bâtiments de guerre, et s'en trouvait séparé depuis les derniers coups de vent. Lorsque je connus ces détails, je sentis que ma position était encore fort équivoque et d'autant plus que le second brick qui se trouvait en arrière et sous le vent à nous était resté spectateur du combat; à la vue de notre succès, il parut chercher à nous joindre; mais exténués comme nous l'étions, et nous trouvant en trop petit nombre pour surveiller nos prisonniers, manœuvrer notre nouveau vaisseau et courir la chance d'un second combat, nous forçâmes de voiles pour l'éviter, et, comme le vent nous était favorable, nous fûmes bientôt hors de sa portée.

Nous continuâmes notre route, et ne fîmes ce jour-là aucune rencontre fâcheuse; mais le 16 au matin à la hauteur de Gothland, nous fûmes tout étonnés de nous trouver au milieu du convoi anglais dont notre vaisseau avait fait partie.

Nous étions infailliblement perdus, si l'on avait pu nous reconnaître; heureusement on ne savait rien de ce qui s'était passé la veille. Pendant quatre jours nous voguâmes sans qu'il leur vint le moindre soupçon à notre égard. Durant cet intervalle nous essuyâmes une tempête épouvantable; elle fut si terrible que, d'après les journaux du temps, trois cents bâtiments échouèrent alors sur les côtes de Suède.

Le 20, poussés par un vent d'ouest, nous avions dépassé la hauteur de Riga et nous nous trouvions à l'entrée du golfe de Finlande.

Le 21, la mer se calma un peu et nous cessâmes de dériver. Cependant la situation de mon petit équipage devenait de plus en plus critique. Depuis le 10, nous étions à la demi-ration, et même, en continuant à donner les vivres sur ce pied-là, il ne nous en restait que pour six jours. L'eau nous manquait totalement et nous avions épuisé notre eau-de-vie. D'un autre côté, à mesure que les distributions diminuaient, le service devenait plus pénible. Obligés d'être jour et nuit sur le pont, de faire la manœuvre par des temps affreux et sans sécher leurs vêtements, privés de tout, exténués de fatigue, mes matelots maigrissaient à vue d'œil, et je prévoyais le moment ou leurs forces cesseraient de répondre à leur courage. Je redoutais en outre d'être engagé dans les glaces.

Les 22 et 23, le vent ayant varié de l'ouest au sud, nous fîmes petite route, mais toujours avec le convoi anglais.

Le 24, le vent se fixa à l'est, et nous eûmes connaissance de l'île de Gothland. Pendant la nuit, il s'éleva une brise et toute la journée du 25 nous courumes vers Bornholm ; sur le soir le vent fraîchit et nous n'étions plus qu'à 12 lieues de cette île désirée, mais comme alors nous faisions une lieue à

l'heure, nous fûmes obligés de diminuer de voiles pour ne pas terrer avant le jour.

Le 26, deux chaloupes danoises vinrent nous reconnaître et nous allâmes mouiller sous la protection des batteries de Bornholm.

Je me rendis auprès du gouverneur qui me fit l'accueil le plus distingué. Je voulais sur le champ partir pour Copenhague, mais il m'en empêcha. Il me fit observer qu'à moins de traverser le détroit la nuit et par un bon vent, on risquait d'être pris par les croiseurs suédois qui infestaient ces parages. Il m'engagea même à ne pas continuer ma route sur le bâtiment capturé dont la marche était fort lente et mit à ma disposition un paquebot et un officier de son état-major.

Je laissai au capitaine Dumoutier la liberté de partir quand il le jugerait convenable, et je lui enjoignis de vendre à Copenhague le bâtiment que nous avions pris.

Le 2 décembre, le vent soufflant dans une bonne direction, mais avec violence, je voulus mettre à la voile. Deux obstacles s'y opposaient, le clair de lune et quelques croiseurs suédois en observation devant le port de Roenne. Le gouverneur que ces dangers effrayaient voulut me retenir, mais dans ma position je crus devoir résister à ses instances et tenter encore une fois la fortune.

Lorsque je pris congé de ce brave officier (M. de

Rœter, commandant de la marine), il eut l'attention de me promettre que dans le cas où l'on se disposerait à me donner la chasse, il m'en préviendrait par un signal.

A peine étais-je à une portée de canon du port, que j'entendis le signal convenu. Cependant je ne voulus pas rétrograder. La mer était très houleuse, j'espérais que l'ennemi nous perdrait de vue. Le succès justifia mon attente.

Nous passâmes la nuit à craindre les attaques, à lutter contre les vagues. Cette nuit fut affreuse et nous courûmes les plus grands dangers.

Le lendemain à midi nous entrâmes dans le Sund et à onze heures du soir nous arrivâmes à Copenhague. Après avoir remis à notre ambassadeur (M. le baron Alquier) les lettres que j'avais pour lui, je me disposais à partir lorsque le roi instruit de mon arrivée par l'officier venu de Bornholm avec moi me fit dire qu'il désirait me voir. Je me rendis sur le champ auprès de sa Majesté qui me reçut de la manière la plus gracieuse, voulut connaître jusqu'aux plus petits détails de mon voyage, et m'offrit tous les secours dont je pouvais avoir besoin.

Je quittais Copenhague immédiatement après l'audience du Roi, et me dirigeai sur Hambourg.

J'appris en route les événements qui avaient eu lieu, l'invasion de la France et le blocus d'Hambourg, je fus témoin de la retraite de l'armée danoise.

Forcé de revenir sur mes pas, je retournai à Copenhague, après avoir tenté vainement de m'embarquer dans les principaux ports du Holstein et du Jutland.

J'appris enfin les malheurs de l'armée française, l'abdication de l'Empereur et l'entrée du Roi à Paris. C'est alors que je rentrai en France.

Le capitaine Dumoutier resté à Bornholm d'après mes instructions, profita d'un coup de vent pour traverser le Sund; mais, aperçu et poursuivi précisément par l'un des dix bâtiments de guerre partis de Danzig, ce brave jeune homme eut l'audace d'assurer le pavillon français et d'engager un combat dont l'issue ne pouvait être douteuse. Sa témérité étonna le commandant anglais, qui, sur la demande du capitaine Dumoutier, le déposa, ainsi que ses matelots, sur les côtes de Suède au lieu de les emmener en Angleterre.

CHAPITRE II

MANIÈRE DE JUGER LA VALEUR D'UNE MÉTHODE CRYPTOGRAPHIQUE

On pourrait dénommer ce chapitre : *Dynamométrie de la cryptographie.*

Tout se mesure et se pèse.

La cryptographie ne fait pas exception à la règle commune.

*
* *

Une méthode cryptographique quelconque a, comme valeur, le nombre de combinaisons qu'elle renferme ; mais — il y a aussi un mais — cette valeur est absolue ou illusoire.

C'est par le déchiffrement sans clef d'une méthode qu'on peut établir si les combinaisons de cette méthode ont une valeur absolue ou n'ont qu'une valeur d'illusion.

*
* *

On peut admettre comme un principe que, connaissant un mot et la méthode employée, tout cryptogramme peut être déchiffré sans qu'on en ait la clef.

La valeur réelle de la méthode ne sera pas donnée par son plus ou moins de combinaisons, mais bien par la durée de la résistance que le cryptogramme opposera au déchiffrement sans clef.

*
* *

En conséquence, il n'est pas difficile de se prononcer sur la valeur d'une méthode, quelle qu'elle soit.

Donnez un cryptogramme à un déchiffreur, avec toutes les indications de la méthode suivie, avec les appareils, si la méthode en comporte; livrez-lui un mot de sept ou huit lettres, mot n'existant qu'une seule fois dans le cryptogramme, et attendez qu'il ait fait la traduction.

Si un déchiffreur habile, muni de ces renseignements, déchiffre le cryptogramme en peu de temps, — et, par peu de temps, nous entendons une demi-heure aussi bien qu'un jour, — la méthode est jugée; elle ne vaut rien.

Si, au contraire, ledit déchiffreur habile passe

plusieurs jours, ou plusieurs mois, en travaillant sans relâche, pour parvenir à arracher son secret à un cryptogramme, la méthode est bonne ; vous pouvez l'employer en toute sécurité.

*
* *

En bonne logique, toute méthode rapidement déchiffrée doit rigoureusement être éliminée, surtout lorsque les dépêches chiffrées peuvent tomber entre les mains de l'ennemi.

Évidemment certains chiffres, reposant sur le secret de l'appareil qui les donne (tables chiffrantes, livres, etc.) offrent, tant que le secret est gardé, une très grande garantie de sécurité ; mais il ne faut pas perdre de vue qu'aucun mystère n'est durable et que, soit par ruse, soit autrement, les intéressés viennent toujours à bout de se procurer les appareils en question, à moins que, par des travaux spéciaux, souvent fort longs, ils ne parviennent à les reconstituer.

La sécurité alors disparaît pour toujours. Tous les changements de clef qu'on pourra faire seront impuissants à la ramener.

C'est l'appareil livré ou reconstitué, qu'il faut abandonner complètement.

*
* *

Conclusion logique et forcée : faire reposer la sécurité d'un chiffre sur le secret de la méthode ou d'un appareil (et par appareil nous entendons aussi bien un cryptographe qu'un dictionnaire ou un tableau) est une chose illogique au premier chef.

VALEUR DES MÉTHODES OFFICIELLES

Par les quelques déchiffrements que nous avons faits — (chiffres officiels de la guerre, — chiffres proposés par MM. Bord, La Feuillade et d'autres, — chiffres de François I^er^, de François II, de Henri IV, de Louis XIV, de Mirabeau, de Napoléon I^er^, — chiffres inventés par MM. de Viaris, Hermann, d'Ocagne, etc.), — nous avons vu les points faibles des différents systèmes.

Nous avons prouvé, dans la première et la deuxième partie de cet ouvrage, que l'on arrive toujours à trouver le secret de la méthode employée, sans en rien connaître.

Nous avons presque toujours réussi à faire la traduction des cryptogrammes qui nous ont été

soumis, et certes ils sont nombreux; certains même étaient faussement chiffrés, et les erreurs étaient *voulues*, pour nous empêcher d'aboutir; d'autres, au lieu de traiter de choses militaires, parlaient des Bakoko et des Batanga, de la géographie d'Elysée Reclus, etc., etc.

*
* *

Depuis 1890, le Ministère de la Guerre a eu le temps de se convaincre de l'insuffisance de ces chiffres. Les preuves ont été faites à Nantes d'abord, à Paris ensuite, puis à Constantine, où le général commandant l'artillerie mettait en doute la traduction *sans clef* des chiffres militaires. Ce général nous adressa un cryptogramme qui fut déchiffré le jour de sa réception et, — circonstance peu favorable, — en chemin de fer dans le trajet de Constantine à Philippeville. *Matifou* était le mot clef.

On doit donc être fixé, en haut lieu, sur la valeur des méthodes officielles en usage et en faveur.

CHAPITRE III

MÉTHODES PROPOSÉES ET OBJECTIONS FAITES

Prouver qu'un chiffre dont on fait usage ne vaut rien, c'est bien; mais encore faut-il proposer quelque chose de mieux à la place.

C'est ce que nous avons fait, en pure perte d'ailleurs, à maintes et maintes reprises.

Nous étions même, à un moment donné, littéralement emballé sur le sujet. Encouragé par les uns, — les esprits droits et loyaux, — enterré par les autres, — les esprits tortueux et mystérieux, — toujours bien accueilli par tous, recevant, à chaque présentation nouvelle, des éloges et de l'eau bénite de cour, nous avions fini par renoncer à cette ingrate science, et il a fallu le procès de la Haute-Cour pour nous donner une nouvelle cryptographite aiguë, maladie dont, paraît-il, nous sommes fortement atteint.

*
* *

Ceci expliqué, nous allons donner, par ordre chronologique, les méthodes que nous avons proposées à la *Guerre* en remplacement de celles employées et que nous avions démolies.

Nous donnerons aussi les objections faites et les motifs officiels de la non-acceptation. Le lecteur jugera.

En nous inspirant des trois conditions énumérées au chapitre II de la deuxième partie :

Indéchiffrabilité absolue ;

Simplicité et rapidité ;

Non-nécessité du secret de la méthode et de l'appareil ;

Nous avons cherché à supprimer les points faibles des systèmes étudiés, et nous avons soumis au Ministre de la Guerre à différentes reprises, depuis 1890, des méthodes cryptographiques, réunissant ces trois conditions essentielles.

*
* *

Voici ces méthodes :

1890. — Méthode du chiffre carré perfectionné.

On répondit : « Le système présenté, malgré des « qualités assez sérieuses, n'est pas assez simple,

« ni assez rapide pour pouvoir être utilisé pour la « correspondance chiffrée militaire. »

* * *

1891. — Méthode du chiffre carré combiné avec plusieurs tables cryptographiques, et les nombres premiers.

Les tables cryptographiques étaient au nombre de 20, et à ordre interverti.

Pour pouvoir se les rappeler en cas de besoin, elles dérivaient pour la plupart d'une devise formant souche.

Table n° 1. — Ordre normal de A à Z.
— 2. — Les consonnes de B à Z, suivies des voyelles de A à B.
— 3. — Les voyelles de A à Y intercalées par séries de 2 entre des séries de 6 consonnes de B à Z.
— 4. — Ordre normal retourné de Z à A.
— 5. — Les voyelles dans l'ordre retourné de Y à Z, intercalées par séries de 2 entre des séries de 6 consonnes retournées également de Z à B.
— 6. — Les consonnes dans l'ordre retourné de Z à B, suivies des voyelles dans le même ordre de Y à A.
— 7 ou table A. — Devise, — Allons enfants de la patrie, le jour de gloire est arrivé.
— 8 — B. — Bienheureux les pauvres d'esprit, le royaume des Cieux.
— 9 — C. — Charybde et Scylla.
— 10 — D. — Dieu protège la France.
— 11 — E. — Evitez les courants d'air.
— 12 — F. — Formez les faisceaux.
— 13 — G. — Gloire immortelle de nos aïeux.

Table n° 14 ou table H. — Honneur et Patrie.
— 15 — I. — Instruisez la jeunesse.
— 16 — J. — J'aime l'oignon frit à l'huile.
— 17 — K. — Kyrie eleison.
— 18 — L. — L'homme propose et Dieu dispose.
— 19 — M. — Montez à cheval.
— 20 — N. — Nous tenons la clef.

Les tables ne comportaient pas le double V, les appareils Hughes et Baudot ne possédant pas cette lettre, et employant deux V, l'un à la suite de l'autre, pour transmettre W.

On nous répondit : « Le système est combiné « avec grand soin, entouré de précautions nom- « breuses, et, en général, bien choisies, et la sécu- « rité égale à celle des meilleurs systèmes connus.

« Toutefois une méthode aussi minutieuse dans « ses détails, qui pourrait, à la rigueur, servir en « temps de paix, ne pourrait, sans de graves in- « convénients, être utilisée en temps de guerre.

« En conséquence, le système, ne répondant pas « complètement aux besoins militaires, ne saurait « être mis en service dans l'armée. »

Ceci se passait en janvier 1891.

*
* *

La méthode avait été envoyée en décembre 1890; trente cryptogrammes, faits avec la même clef, l'accompagnaient. Ils ne furent pas déchiffrés.

Pourquoi donc dire que la méthode égalait en

sécurité celle des meilleurs systèmes connus, alors que les chiffres de ces derniers étaient lus, et qu'on ne pouvait pas lire les nôtres?

La fin de l'exposé de notre méthode disait : « Les « cryptogrammes sont chiffrés sans aucune malice; « le mot clef est un mot dans le genre de Indes « Portugal. Nous sommes tellement convaincu que « les changements de tables sont suffisants pour « empêcher de déchiffrer sans clef, quel que soit le « nombre de dépêches que l'on puisse posséder, « que ces chiffrements ont été faits pour ainsi « dire au courant de la plume.

« Nous avons une manière qui nous est propre « de déchiffrer sans clef les cryptogrammes obte- « nus au moyen du chiffre carré ordinaire; du « moins nous le pensons, car cette façon de procé- « der (infaillible, d'après les expériences que nous « avons faites) ne se trouve indiquée dans aucun « des ouvrages traitant de la matière, que nous « avons consultés. Nous avons essayé de cette mé- « thode de déchiffrement avec des cryptogrammes « chiffrés par plusieurs tables; les changements « inconnus de table nous ont toujours dépisté et « empêché d'aboutir.

« Il peut se faire que de plus habiles puissent « aboutir à déchiffrer sans clef; mais ce que nous « affirmons hautement, c'est qu'ils ne réussiront « que si le mot clef est un mot réel; si le mot est

« une combinaison de lettres n'ayant aucun sens,
« telles que, par exemple, BIKVDXLP, etc., etc.,
« le déchiffrement sans clef est une chose impos-
« sible. »

Ce qui précède était écrit en décembre 1890. Nous n'avons rien à y changer.

*
* *

Cependant nous avons reconnu que l'observation du Ministre était fondée, lorsqu'il disait que cette méthode était trop minutieuse dans ses détails, et nous avons cherché à faire plus simple, comme nous y étions encouragé.

Un officier de l'État-Major de Nantes, qui s'intéressait à nos travaux, nous dit alors que ce qui avait le plus de chance d'être adopté par la *Guerre* était un appareil avec lequel on pût lire la dépêche, sans cassement de tête.

C'est ainsi que fut inventé notre cryptographe cylindrique. On conserva les mêmes alphabets que ceux de la méthode précédente (chiffre carré par plusieurs tables).

*
* *

Le cryptographe cylindrique, qui est bien un appareil avec lequel on peut lire la dépêche sans aucun cassement de tête, et sans aucune

attention soutenue, fut présenté à la Guerre, le 12 février 1891.

Le général Fay, commandant le XI[e] corps d'armée, fit cette présentation, et, à la suite d'un rapport fait sur cet appareil par son état-major, il ajouta de sa main, avant de le signer et de l'envoyer au Ministre :

« Je n'ai aucune aptitude pour la cryptographie,
« mais j'ai été séduit par la vue de cet appareil
« ingénieux et ai pu chiffrer et déchiffrer en moins
« d'une demi-heure une dépêche, ce que je n'avais
« jamais pu faire avec les systèmes précédents.

« Si les personnes plus compétentes ne trouvent
« pas de défaut à ce système, je doute que l'on
« puisse en trouver de plus ingénieux et de plus
« pratique.

« Il fait grand honneur, etc., etc.

*
* *

Le cryptographe cylindrique inaugure une méthode nouvelle en cryptographie. Le principe est le suivant : Emploi simultané de plusieurs alphabets différents pour le chiffrement d'une même dépêche. L'appareil n'a pas à être tenu caché, il ne livre pas le secret, à condition qu'il soit démonté, bien entendu. L'emploi en est simple et rapide et l'indéchiffrabilité absolue.

Il n'y a de secret que le mot-clef.

*
* *

On répondit en critiquant d'abord la construction de l'appareil : exiguité des chiffres, difficulté dans le jeu de la broche, inconvénient pour la lecture à la lumière de lettres gravées en creux sur métal poli.

La manipulation fut trouvée facile, mais exigeant toutefois une assez grande attention, et il ne fut pas trouvé que le système présentât d'avantage, au point de vue de la rapidité du chiffrement ou du déchiffrement, sur le procédé alors en usage.

Pour la question d'indéchiffrabilité, il résultait d'un rapport fourni au Ministre qu'à défaut d'un changement complet de clef des dépêches saisies pouvaient être lues.

*
* *

L'auteur de ce rapport s'était placé dans l'hypothèse d'un appareil saisi monté à la clef.

Nous avions indiqué de prendre comme clef un mot et d'ajouter à ce mot la date de l'envoi du cryptogramme, ce qui, par le fait, faisait une clef journalière.

Avec énormément d'ingéniosité, l'auteur du rapport a démontré que l'appareil qu'il avait supposé saisi monté à la clef : *guerre dix-sept avril* per-

metfait la lecture d'une dépêche saisie faite avec la clef : *guerre dix-huit avril.*

L'exposé de la méthode recommandait cependant de démonter l'appareil après s'en être servi.

* * *

L'opération du démontage et du remontage du cryptographe à une clef quelconque ne demande que deux minutes, montre en main, sans se presser.

Elle était si longuement exposée dans ce rapport que rien qu'à la lecture on sentait que c'était tout un travail.

Le lecteur va en juger. Nous citons en entier le paragraphe du rapport en question.

« Donc si les anneaux ne sont nullement disposés « d'après la clef, on peut considérer la sécurité « comme assurée; mais ce ne sont pas tout à fait « là les conditions de l'emploi pratique. S'il fallait, « chaque fois qu'on a une dépêche à lire ou à écrire, « constituer la clef en lettres, la transformer en « chiffres, démonter l'appareil, enlever les anneaux, « les ranger d'après l'ordre donné par la clef, les « remettre en place, rajuster la fenêtre mobile et « le disque de fermeture, on n'en finirait pas. Il faut « pour cela n'être pas pressé, avoir une table à sa « disposition, etc. »

Bref, et quoique les cryptogrammes qui accompagnaient l'appareil n'aient pu être lus, le Ministre concluait ainsi :

« Dès lors le système proposé ne présente pas « des garanties de sécurité supérieures à celui actuel- « lement en usage [1], et comme son emploi présente, « au moins actuellement, certaines difficultés incon- « testables, je ne juge pas qu'il réalise un progrès « justifiant son adoption pour les usages militaires. »

* * *

En 1892, après avoir perfectionné le cryptographe, supprimé la fenêtre mobile, compartimenté la trousse qui le renfermait, de manière à obliger l'officier négligent à démonter son appareil après s'en être servi, simplifié encore la méthode, on fit une nouvelle présentation, et c'est par un nouveau refus d'adoption qu'il nous fut répondu.

* * *

En 1893, le général Saussier, gouverneur militaire de Paris, s'étant intéressé à cet appareil, qui lui plaisait fort, qu'il manœuvrait avec aisance et sans cassement de tête, écrivit au Ministre. Il lui demandait, à la suite d'une lettre fort élogieuse pour nos travaux

[1] On lisait le chiffre officiel sans clef, souvent en moins d une heure.

et qu'il nous fit communiquer, de vouloir bien réunir la Commission cryptographique — que nous nous étions fait fort de convaincre *de visu* du danger de la méthode en usage — pour nous entendre en nos explications.

On nous convoqua pour le jeudi 9 février à 3 heures du soir, au 3e bureau de l'État-Major de l'Armée.

Au lieu de la Commission devant laquelle nous nous attendions à comparaître, nous nous sommes trouvé en présence d'un capitaine. Ce capitaine était l'inventeur du système alors en usage, système que nous lisions sans clef.

Surpris de voir que la demande du général Saussier tournait en plaisanterie, nous nous sommes retiré en déclarant à ce capitaine que nous n'avions rien à lui confier, à lui personnellement.

Nous savions que, de parti pris, il était hostile à tous les inventeurs de systèmes cryptographiques.

* * *

Enfin, en 1898, rentrant dans les vues de l'État-Major — un crayon et du papier — nous avons présenté une méthode dans cet ordre d'idées, mais sans enthousiasme.

Cependant les cryptogrammes donnés n'ont pas été lus.

On nous a demandé notre méthode, que nous

n'avions pas indiquée, parce qu'elle était forcément secrète. En la donnant, nous avions indiqué une modification qui, sans en détruire la forme originale, permettrait peut-être de n'en point craindre la divulgation. Un nouveau cryptogramme avec le seul secret de la clef accompagnait l'exposé de la méthode. Ce cryptogramme n'a pas été lu.

Voici la réponse du Ministre ; elle est du 19 avril 1899 :

« Il a été reconnu que la méthode ne présentait « pas les garanties de sécurité suffisantes pour être « adoptée. »

*
* *

Nous donnons à l'*Appendice*, *notes VII* et *VIII*, les deux dernières méthodes présentées à la *Guerre :* le cryptographe cylindrique et le système n'exigeant qu'un crayon et du papier ; nous abandonnons comme trop compliquée la méthode du chiffre carré, combiné avec plusieurs tables et les nombres premiers.

*
* *

Le lecteur sera peut-être surpris que, de toutes les méthodes que nous venons d'exposer et qui ont été soumises au Ministre (*toutes accompagnées de cryptogrammes, dont aucun n'a été déchiffré*), on ait dit : les garanties de sécurité ne sont pas suffisantes.

Il trouvera aussi extraordinaire que les méthodes adoptées par des *compétents* (?) (si difficiles pour les autres) n'aient jusqu'ici donné que des chiffres que nous avons toujours déchiffrés en quelques heures, ne sachant même pas comment ils étaient établis.

Il se demandera enfin pourquoi on persiste dans ces errements. Nous ne savons que répondre. On a dit qu'il fallait ménager l'amour-propre des *compétents* (?).

* * *

Si les chiffres de l'état-major général français étaient destinés, en cas de guerre, à communiquer des banalités, nous en ririons et nous admirerions ce bel exemple d'esprit de routine et de chapelle ; mais, ces chiffres étant faits pour transmettre des ordres de toute importance, leur faiblesse peut compromettre le sort d'une armée, l'avenir du Pays peut-être.

Sait-on si ce cas ne s'est déjà pas produit?

La série de revers subie par Napoléon Ier, à partir de 1813, ne serait-elle pas, en partie, due à la faiblesse de son chiffre lu par les Russes?

Rappelons ce que dit le maréchal Macdonald dans ses *Souvenirs :*

* * *

C'était en 1814 ; l'Empereur de Russie avait invité à dîner les Maréchaux présents à Paris, le

Ministre de la Guerre et le duc de Vicence (général de Caulaincourt). On parla pendant le dîner de choses et autres, et aussi *chiffres*.

Écoutons Macdonald (p. 308) :

« L'Empereur nous parla ensuite de nos correspondances officielles et particulières qui avaient « été interceptées et déchiffrées de sorte qu'il avait « pu les lire.....

« Pour en revenir à la correspondance officielle, « je dis, en souriant : « Il n'est pas surprenant que « Votre Majesté ait pu la déchiffrer, on lui en « avait donné la clef[1]. » Il prit alors un air solennel, une main sur son cœur et l'autre étendue : « Non, répondit-il, je vous en donne ma parole « d'honneur. »

* * *

Le fait est acquis. On ne peut mettre en doute la parole d'honneur de l'empereur Alexandre Ier ; les déchiffreurs russes lisaient les chiffres militaires de Napoléon Ier.

* * *

On est en droit de supposer qu'en 1870 il en a été de même, et que les déchiffreurs allemands ont lu les chiffres de Napoléon III.

[1] Le duc de Tarente faisait allusion à la désertion du général Jomini, chef d'État-Major du maréchal Ney, qui avait passé à l'ennemi en août 1813, emportant tous les papiers.

La génération future pourra s'en assurer, lorsque le Dépôt de la guerre à Berlin mettra les papiers de l'année 1870 à la disposition du public.

*
* *

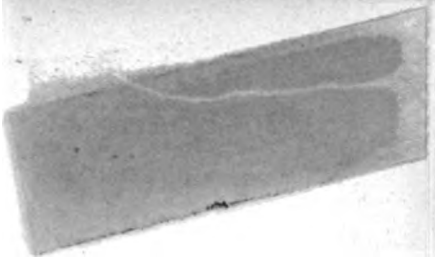
Puisse le cri d'alarme que nous poussons être entendu !

Puisse la réforme des chiffres militaires français que nous désirons si ardemment être enfin ordonnée !

C'est dans cet espoir que nous écrivons :

Divulguer des faits qui, tenus secrets, peuvent compromettre la défense nationale, c'est faire acte de bon Français.

FIN DE LA TROISIÈME PARTIE



APPENDICE

NOTE I

DÉCHIFFREMENT FAIT PAR VIÈTE

Lettre de Viète[1] au Roy, datée de Tours, le 5 mars 1590, faisant l'envoi de la traduction d'une lettre chiffrée du commandeur Juan de Moreo à Philippe II, roi d'Espagne.

Cette lettre chiffrée était datée d'Anvers, le 28 octobre 1589, et écrite en langue espagnole.

La traduction française donnée en regard est due au gracieux concours de M. Joseph Soubielle, professeur d'espagnol au collège de Perpignan.

Pour mieux saisir l'importance historique de cette lettre chiffrée, nous rappelons par une notice succincte les faits antérieurs au 28 octobre 1589 et que tout le monde connaît.

[1] Bibliothèque nationale. Manuscrits. Les 500 de Colbert, 33.

Le 1er août 1589, Henri III était assassiné, sous les murs de Paris, par le moine dominicain Jacques Clément.

Paris était alors au pouvoir des ligueurs, commandés par le duc de Mayenne.

Les chefs catholiques de l'armée de Henri III, réunis à Saint-Cloud, proclamèrent roi, sous le nom de Henri IV, Henri de Bourbon, roi de Navarre.

La Ligue, de son côté, proclama roi, sous le nom de Charles X, Charles de Bourbon, cardinal de Rouen oncle de Henri IV.

Comme le cardinal était prisonnier de l'armée royale qui assiégeait Paris, le duc de Mayenne reçut de la Ligue le titre de lieutenant-général du royaume.

Chacun sait que la dignité de lieutenant-général du royaume n'était créée que dans les circonstances difficiles ou pendant la minorité des rois. Le titulaire de cette dignité possédait et exerçait toute l'autorité du roi.

Henri IV abandonna le siège de Paris pour se porter sur la Normandie, où il devait recevoir un renfort de troupes de 5.000 hommes, venant d'Angleterre.

Les ligueurs le poursuivirent et l'atteignirent aux environs de Dieppe.

Henri IV avait 10.000 hommes; Mayenne en avait 30.000; après douze jours d'engagements assez vifs, un dernier combat, livré au château d'Arques, le 21 septembre 1589, assura la victoire à Henri IV.

Ayant reçu les 5.000 hommes de renfort, Henri IV revint sur Paris et s'empara de quelques faubourgs; des barricades élevées à la hâte par les Parisiens et l'arrivée de l'armée de Mayenne l'empêchèrent d'en faire le siège.

* * *

C'est ici que se placent l'intérêt historique et l'importance de la lettre chiffrée de Juan de Moreo, datée du 28 octobre 1589, et déchiffrée par Viète en 1590.

On fera remarquer que Charles de Bourbon, proclamé roi par la Ligue, vivait encore (mort en 1590).

Le duc de Mayenne qui, d'après cette lettre, ambitionnait la couronne de France, trahissait donc la Ligue et son Roi.

(Inédit) **LETTRE DE VIÈTE[1] AU ROY**

Sire, j'envoye présentement les traductions de mot à mot des ordres dont ces jours passés, je peu seulement envoyer les extraits. Les lettres et instructions du Roy d'Espagne envoyez à l'ambassadeur Mandosse et au commandeur Moreo y sont insérées au long, et l'escrit de Mandosse, où il respond à certains points dont Sa Majesté Espagnole désiroit estre éclaircie singulièrement de ceux qui doivent succéder à votre couronne française[2]. Mais cela est peu consequencieus, au regard de la lettre que lui avait escrit Moreo, tant sur les conseils du duc de Parme que les desseins du duc de Mayne[3], qui s'est déclaré vouloir estre Roy, et y aspirer, et a traitté des moyens pour y parvenir à la désolation et dissipation de l'Estat de votre France.

Sire, je m'advanceray de vous dire que je ne puis estimer que les villes de la Picardie, que le duc de Mayne voulait livrer à l'Espagnol et retenir à soy la

[1] On a respecté l'orthographe de l'époque.

[2] Renseignements obtenus par des déchiffrements antérieurs.

[3] Charles de Lorraine, duc de Mayenne, deuxième fils de François de Guise, succéda, comme chef des catholiques, à son frère Henri le Balafré (1588) : il ne fit sa soumission à Henri IV qu'en 1596, après avoir été battu, en 1595 à Fontaine-Française, dans son gouvernement de Bourgogne.

Bourgongne, pour puis après tous deux, et chacun pour soy, conquérir le surplus de vos estats, ne se rengent sous vostre obéissance, quand ils auront cognoissance de la visée ou l'on tend pour les piper; les gouverneurs les premiers, qu'on s'attend tirer des villes peu à peu pour y introduire l'Espagnol. Ce n'est point par presens, cõme dit Moreo, que prétend le duc de Mayne, que se gaigne le cœur de vostre Noblesse Françoise. C'est elle qui n'a jamais defailly au besoing à leur Roy naturel. Et pour ce, Sire, il me semble point mal à propos, que ces villes et gouverneurs, et généralement tous voz peuples, qui trempent encor en la ligue, sceussent ceste vérité. Car ce ne sont point lettres appostées que je présente. J'en tiens et garde soigneusement les originaux, que je recongnois en bonne forme, et bien scellez et signez, lesquels je representeray toujours avecques mes traductions, et les alphabets et dictionnaires que j'ay compris pour y parvenir, à qui, et quand de par vous il me sera ordonné. Et ne doit esmouvoir que cela sera occasion à voz ennemis de changer leurs chiffres, et se tenir plus couverts, et à nous voz officiers plus empeschez à vous y servir. Ils en ont changé et rechangé, et néantmoins ont esté et seront toujours surpris en leurs finesses. Car vostre cause est juste et la leur inique. Et pour ce Dieu dissipera leurs conseils pour bénir les vostres, illuminant les esprits à ce

qui fera de vostre service auquel s'affectionnera à jamais selon son devoir

Vostre très humble et très obéissant subjet et serviteur.

F. V. (François Viète).

De Tours, le 15 mars 1590.

Déchiffrement de Viète[1]

Al Rey nuestro Sennor

En manos de Don Martin de Idiaquez su secretario d'Estado.

Sennor,

De Ruan despache un correo à V. M. con el despacho, cuyo duplicado va con esta. Despues boluiendo adonde estava el Duque Deumeyna le halle en el aprieto y al resolucion que me forzo à dexallo todo y venir a qui por el remedio y a dar cuenta del estado de las cosas al Duque de Parma.

Como V. M. mandara veer por los puntos que le he dado por escrito, firmados de mi mano, cuya copia va con esta. Haviendo me para ello aprovechado de algunos extremos para atraelle a lo que tanto importa al servicio de Dios y de V. M. Que no hiziendo

1 Viète ne connaissait pas à fond la langue espagnole. La traduction qu'il a obtenue syllabe par syllabe peut présenter quelques légères erreurs, mais le fond du sujet reste exact. On fait remarquer que c'est l'espagnol de l'époque.

Traduction en français

Au Roi notre Seigneur

Aux bons soins de M. Martin de Idiaquez son secrétaire d'Etat.

Seigneur,

De Rouen j'ai envoyé un courrier à Votre Majesté avec la dépêche dont je vous donne le duplicata.

Revenant ensuite où se trouvait le Duc de Mayenne, je le trouvai en danger et dans une telle résolution que j'ai été forcé de tout laisser et de venir ici pour y remédier et rendre compte de l'état des choses au duc de Parme[1].

Comme Votre Majesté voudra bien voir par les points que je lui ai mandés par écrit, signés de moi et dont la copie est ci-jointe.

Pour l'amener à ce qui importe tant au service de Dieu et de Votre Majesté je me suis servi

1 Le prince Farnèse, duc de Parme, était le plus habile des généraux de Philippe II. Il était gouverneur des Flandres.

se tengo por perdido y despiertado el mayor negocio que se ha visto en el mundo, como se dexa considerar.

Y a todo lo que tengo dicho al Duque de Parma me tiene respondido hasta el presente.

Que el no tiene à cargo sino de conservar estos estados, y que lo de mas pues se le ha quitado las ocasiones.

Que no tiene con que podelles socorrer de gente, y que ansi no le piensa hazer hasta que tenga otra orden de V. M.

Cosa que me ha espantado que pagando V. M. 66.000 hombres en estos estados no haya con que poder dar 6.000 a tan extrema necessidad.

Que tambien llegada dicha nueva ya todo estara perdido.

Y visto semejante als resolucion le replique que hiziendo se lo que dezia, no havia para que yo volviese alla, ni havia para que dalles los 300 mil escudos, pues no servirian de nada y se podian ahorrar à V. M.

Pues assi como asy no dexaria de concertarse, y hazer la paz general en biendo que dicho socorro de gente les falta, y que V. M. no se quiere declarar por los Catolicos como han hecho la Reyna de Ynglaterra y principes protestantes por los hereges, y quando no haya sino una suspension de armas V. M. vera quan pre udizial sera a la religion.

de quelques moyens extrêmes et si cela ne se fait pas je considère comme perdue et éventée la plus grande négociation qu'on ait vue au monde, comme on peut en juger.

Et à tout ce que j'ai dit au duc de Parme il m'a répondu jusqu'à présent.

Que lui n'est chargé que de conserver ces Etats, et que pour le reste, puisque les occasions lui ont été ôtees, il n'a pas de quoi pouvoir les secourir avec des troupes et qu'ainsi il ne pense pas le faire à moins d'avoir un autre ordre de Votre Majesté.

J'ai été étonné que Votre Majesté entretenant 66.000 hommes dans ces Etats, il n'y ait pas de quoi pouvoir en consacrer 6.000 à un si pressant besoin.

Qu'aussitôt ce refus connu, tout sera perdu.

Et ayant vu une semblable résolution je lui répondis que si l'on faisait ce qu'il disait, il n'y avait aucune raison pour que je revinsse là-bas et pour leur donner les 300 mille écus, car ils ne serviraient à rien et on pouvait les économiser à Votre Majesté.

En effet de toutes les manières on ne laisserait pas de traiter et de faire la paix générale en voyant que ledit secours de troupes leur manque et que Votre Majesté ne veut pas se déclarer pour les catholiques comme l'ont fait pour les hérétiques la reine d'Angleterre et les princes protestants, et quand même il n'y aurait qu'une sus-

Dios lo quiera remediar.

A lo que yo tengo entendido y puedo pensar de discursos y palabras que el duque de Parma me ha dicho, es desear el mismo en persona entrar con exercito formado en Francia, y obligar a V. M. a que por este als camino le de larga la mano. De que esta muy sentido al presente.

Y esto de entrar el en Francia entiende que V. M. lo havra de hazer por fuerza quando vea despintado el juego que ahora tiene entablado en dicho Reyno.

Y no considera los grandes males que dello se seguira.

Porque quanto a lo primero al presente, en el mismo punto que veran campo de V. M. se juntaran hereges y catoliços contra el, y esto sin ninguna duda por buenos protestos que se tomen y a la fin nos quedara entre manos muy poca *onada* [1].

Lo que V. M. puede remediar sacando mayores provechos entrando en Francia de la manéra que ellos piden y ruegan y yo tengo dicho que les teniendo ganados los estrangeros y cargar fuerza a fuerza por una y otra parte de gente asegurada y criados de V. M. y con esto y poco a poco ganando voluntades de la

pension d'armes, Votre Majesté reconnaîtra combien ce sera préjudiciable à la religion. Que Dieu veuille y remédier!

D'après ce que j'ai compris et ce que je puis penser des discours et des paroles du duc de Parme, il désire entrer lui-même en personne, avec une armée formée en France et obliger ainsi Votre Majesté à lui donner de cette manière pleins pouvoirs; il y tient beaucoup en ce moment [2].

Pour ce qui est d'entrer lui-même en France, il est d'avis que Votre Majesté y sera forcément amenée quand Elle verra que le jeu qu'elle a maintenant commencé dans ledit royaume est brouillé.

Et il ne considère pas les grands maux qui en résulteront.

En effet, dès que les desseins de Votre Majesté seront connus, hérétiques et catholiques s'uniront contre lui, et cela sans aucun doute quelque bons que soient les prétextes que l'on donnera et à la fin il nous en reviendra bien peu d'honneur.

Votre Majesté peut remédier à cela et retirer de plus grands profits en entrant en France de la manière qu'ils le demandent et qu'ils vous en prient et moi j'ai dit que si on gagne les étrangers, si on introduit en nombre de part et d'autre des gens sûrs et des serviteurs de Votre Majesté et si on se concilie ainsi peu

[1] Probablement : honra.

[2] Le duc de Parme arriva à ses fins, puisqu'il vint en France, après le combat d'Ivry et força Henri IV à lever le siège de Paris, en 1590.

nobleza francesa, y del pueblo, que viendo buenos protestos y pulizia vendran a rogar con el tiempo, y mas viendo tan buen defensor y para mi de lo que tengo comprehendido y calado del humor presente si otro medio se toma, sera hazer grandes gastos y sin provechos.

Y para que V. M. quede informado de todo lo que por aca passa y mejor pueda resolver lo que fuere de su real servicio, dire lo que despues de la larga platica he passado con el d'Eumayna al tiempo de mi partida para venir aqui. De todo lo qual no he dicho nada al duque de Parma aun.

Y es que tambien dicho duque me dixo su voluntad y me declaro que era de venir a ser Rey con el tiempo, yo no pude detenerme de suerte que el hecho de ver que no quede con seguridad dello, y despues en algunas platicas que hemos tenido los dos y Villerroy me he mostrado un poco frio en dicho punto, aunque no le he querido quitar las esperanzas, antes bien le he animado a ello, dandole muy buenas palabras por no gastar el negocio y como digo, ultimamente me dijo (zerrando nos en un apossento solos) que de todo punto se echaria en los brazos de V. M. y para que entendiese con quanta fidelidad le serviria, sacandole del trabajo y aprieto en que se veia,

à peu les esprits de la noblesse française et du peuple, lorsqu'ils verront de bonnes promesses et de la courtoisie ils en viendront à prier, avec le temps, surtout en voyant un si bon défenseur et pour moi d'après ce que j'ai compris et saisi de l'humeur présente, si on prend un autre moyen ce sera risquer de grands frais sans profit.

Et pour que V. M. soit informée de tout ce qui se passe ici et puisse mieux décider ce qui touche à son royal service, je dirai ce que j'ai appris après le long entretien que j'ai eu avec le duc de Mayenne au moment de partir pour venir ici. De tout cela je n'ai rien dit au duc de Parme.

Ledit duc de Mayenne me déclara que sa volonté était d'arriver avec le temps à être Roi ; moi je ne pus retenir ma surprise, de sorte qu'il s'aperçut que nous ne lui en donnons pas l'assurance ; depuis, dans quelques entretiens que nous avons eu nous deux et Villeroy, je me suis montré un peu froid sur ledit point, mais je n'ai pas voulu lui ôter toute espérance ; au contraire, je l'y ai encouragé lui donnant de bonnes paroles pour ne pas gâter la négociation et comme je dis, en dernier lieu il me dit (nous étions enfermés dans un appartement, seuls) qu'il se jetterait tout à fait dans les bras de V. M. et pour qu'elle comprît avec quelle fidélité il la servirait, si on le tirait de l'em-

que lo primero que haria seria jurar de jamas hazer paz, ni tregua, ni suspension de armas.

Porque el era verdadero catolico y morira por la religion, ayudandole porque todo lo demas bien veia que era su perdicion y de la religion catolica, y que asi no lo haria, si no a mas no poder, viendose desamparado de V. M. y que como cosa que tanto yva en ello havia pensado de unirse de suerte con V. M. que todo el poder del mundo no seria bastante para estorbar que no se saliesse con lo que se puede dessear.

En esta forma, que entrando el socorro de gente[1] que espera de V. M. de lo que el haze su principal fundamento y caudal y con los demas estrangeros piensa acariziar la nobleza.

Lo qual no han hecho agora por lo qual se vee oy en aprieto.

Y retirarse la mas que pudiere lo qual sera fazil dandoles algun dinero y cargos:

Introduziendo los en las villas.

Cosa que les conviene por no estar siempre a la misericordia de pueblo.

barras et du danger où il se voyait, que la première chose qu'il ferait serait de jurer de ne jamais faire ni paix, ni trêve, ni suspension d'armes.

Parce qu'il était un vrai catholique et il mourra pour la religion si on l'aide, parce qu'il voyait bien que tout le reste était sa perte et celle de la religion catholique, et qu'il ne le ferait pas, à moins de ne pouvoir faire autrement, s'il se voyait abandonné de V. M. et que comme c'est une chose de si grande importance, il avait songé à s'unir avec V. M. de telle manière que tout le pouvoir du monde ne pût suffire à empêcher d'arriver au but qu'on peut désirer.

En cette forme, lorsqu'on aura fait entrer le secours de troupes[1] qu'il attend de V. M. et qui est à ses yeux son appui et sa ressource principales avec les autres étrangers, il pense caresser la noblesse.

Ce qui ne s'est pas fait encore et c'est pourquoi il se voit aujourd'hui en danger.

Et de la retirer le plus qu'on pourra, ce qui sera facile en lui donnant quelque argent et des charges

Les introduisant dans les villes (les nobles).

Chose qui leur convient (aux nobles) pour n'être pas toujours à la merci du peuple.

[1] Philippe II accéda à la demande de Mayenne et envoya les 6.000 hommes qu'il demandait. Ce secours n'empêcha point Mayenne d'être battu à Ivry (Eure), le 14 mars 1590. Le général flamand, comte d'Egmont, qui commandait le secours espagnol, fut tué dans ce combat.

Y de dos inconvenientes se halla ser el menor, y por la esperiencia se vee que sera mas fazil de contentar a uno que a un millon.

Y por este medio terna[1] mas mano en poder satisfazer a V. M., no solo en dar villas, pero aun provincias, lo qual al presente le es impossible sin seguirse grandisimo danno a la Religion, y en duda de poderse salir con ello.

Dize agora que aunque el me dixo que su pretension era de ser Rey de Francia, que viendo ser imposible que V. M. no quiera gastar tanto dinero, como se ofrece para provecho y honra de otro, ni es justo, y que aunque la religion catolica sea el fin principal que a V. M. y a el les mueve, que a cadauno le es lizito procurarlo que le estuviere bien, y con justizia y razon.

Y asi que para salir con ello V. M. no hara nada sin el, ni el sin V. M.

Pero estando conformes y dexandole V. M. el duquado de Borgonna, que oy posee, el poco a poco se introduzira y se assegurara en alguna otra provincia, y a V. M. le estara mejor la Picardia que mas le importa, en esta forma, que es con buen color meter gente en las villas principales para governar de la que fuere de V. M. como es de

Et de deux inconvénients, il se trouve être le moindre, et, par l'expérience, on voit qu'il sera plus facile d'en contenter un que un million.

Et par ce moyen, il interviendra plus efficacement pour pouvoir satisfaire Votre Majesté, non seulement lui donnant des villes, mais même des provinces, ce qui, en ce moment, est impossible sans qu'il s'en suive un très grand préjudice pour la religion, et il est douteux qu'on puisse réussir.

Bien qu'il m'ait dit que sa prétention était d'être roi de France, il dit maintenant qu'il voit qu'il est impossible que Votre Majesté consente à dépenser autant d'argent qu'Elle lui en offre pour le profit et l'honneur d'un autre, et que ce n'est pas juste, et que quoique la religion catholique soit le but principal qui fait agir Votre Majesté et lui, il est permis à chacun de vous de chercher son avantage avec justice et raison.

Et qu'ainsi, pour y réussir, Votre Majesté ne ferait rien sans lui, ni lui sans Votre Majesté.

Mais étant d'accord, et Votre Majesté lui laissant le duché de Bourgogne qu'il possède aujourd'hui, lui peu à peu s'introduira et se fortifiera dans quelque autre province, et Votre Majesté prendra de préférence la Picardie, qui est pour Elle si importante, de la manière suivante : sous un bon prétexte, on mettrait dans les villes principales,

[1] Terna, vieille forme de tendrá.

la que pide, y esto con titulo de salvallos del de Bearne, dexando los governadores que oy estan por el presente, y poco a poco yr llamando, oy uno y mannana otro, y acomodando los el en otra parte, vernan [1] a quedar en poder de V. M. absolutamente; y con el mismo tiempo hazer lo mismo en otras provincias.

Y que pensar que se pueda hazer por otro medio es enganno, ni se podra salir con ello, ni es en su poder de dar oy una villa aun por otra via.

Que aunque le intente, no saldra con ello, y sera dannar a lo de porvenir.

Dize que hiziendose esto V. M. se hallara con un exercito suyo en Francia, y con la provincia que mejor le esta.

Y el con poder teniendo otras de suerte que con esto asseguraran la Fe catolica, y poco a poco conquistaran lo demas tocandole a cadauno su parte, sin haver en que se les pueda impedir por este medio.

Y si por dicha viniese dicho duque a morir en tanto que esto se va hiziendo, V. M. se hallara dentro en Francia con lo dicho, y con haver ganado voluntades, tomando el protesto de la Fe, y de su muger, y con conservalle lo que tuviere.

pour gouverner, des gens dévoués à Votre Majesté comme s'ils l'étaient à ceux qui les demandent, et cela sous prétexte de les sauver du Béarnais. On laisserait les gouverneurs qui y sont aujourd'hui, mais peu à peu, aujourd'hui l'un, demain l'autre, on les retirerait, et lui les placerait ailleurs; ces villes en arriveraient ainsi à rester au pouvoir absolu de Votre Majesté; avec la même lenteur on en ferait autant dans d'autres provinces.

Et que penser que cela puisse se faire par un autre moyen est une erreur; on ne pourrait y réussir, et il n'est pas en son pouvoir de donner aujourd'hui une ville même par un autre moyen.

Que bien qu'il l'essayât, il n'y parviendrait pas, et ce serait compromettre l'avenir.

Il dit que si cela se fait, Votre Majesté se trouvera avoir une armée à Elle, en France, et la province qui lui convient le mieux.

Et lui sera puissant et en aura d'autres, de sorte qu'ainsi vous affermirez la foi catholique, et peu à peu vous conquerrez le reste, chacun prenant sa part, sans que, grâce à ce moyen, rien puisse vous en empêcher.

Et si par hasard ledit duc venait à mourir pendant que cela se fera, Votre Majesté se trouvera avoir en France ce qui a été dit et aura gagné les cœurs en prenant le prétexte de la foi et de sa femme [2] et lui conservera ce qui sera acquis.

[1] Vernan, vieille forme de vendrán.

[2] Philippe II, veuf deux fois, avait épousé une princesse française, Isabelle de Valois.

Hallara otros muchos que le sirvan, deseando ser grandes con seguridad.

Este es el medio que halla mejor y mas seguro para el bien de la religion, y de cada parte, y el que seguio el rey de Inglaterra a los principios, y salio con ser Rey de casi toda Francia.

Y considere V. M. que en estos payses donde obedescen a V. M. y es su Rey y señor natural, si quisiese meter en las villas guarnicion d'españoles ay duda si se saldria con ello al menos lo tomarian cuesta arriba, segun dize el duque de Parma.

Y en fin no se intenta otra cosa.

Quanto mas diferente lo tomaran Franceses hiziendose por medio de la fuerza a los principios.

Y asi lo entiendo, y lo represento a V. M.

Y de que dudo que se salga con ello, y pareciendo me que agora als bien va el Deumayne por el derecho, y buen medio, y que trata con mas llaneza y seguri dad en lo de por venir.

Y que el darnos villas no lo podra hazer si no es teniendo gente de V. M. dentro en Francia.

Y esto ha de ser con mucho artificio y destreza, y con titulo del bien y salvacion d'ellas.

Elle (Votre Majesté) en trouvera beaucoup d'autres qui, désirant être grands, la serviront assurément.

Tel est le moyen qu'il trouve le meilleur et le plus sûr pour le bien de la religion et de chacun de vous; c'est celui qu'au début employa le roi d'Angleterre, et il réussit à être roi de presque toute la France.

Et que Votre Majesté considère que dans ces pays où l'on obéit à Votre Majesté et dont elle est le Roi et Seigneur naturel, si Elle voulait mettre une garnison espagnole dans les villes, il est douteux que l'on réussît, tout au moins ne l'accepterait-on qu'à contre-cœur, au dire du duc de Parme.

Et enfin on ne tente pas autre chose.

De quelle façon bien différente prendraient la chose les Français si, au début, l'on agissait par la force!

Et c'est ainsi que je l'entends et le représente à Votre Majesté.

Et je doute qu'on y arrive, et il me paraît que maintenant le duc de Mayenne prend le droit et bon moyen et qu'il traite avec plus de franchise et d'assurance en ce qui concerne l'avenir.

Et quant à vous donner des villes, il ne pourra le faire qu'en ayant des troupes de Votre Majesté en France.

Et cela doit se faire avec beaucoup d'artifice et d'adresse et sous prétexte de leur bien et de leur salut.

He venido aqui a procurallo, sin haver declarado aun al de Parma mas misterio del riesgo que corre de despintarse todo, si V. M. no se declara desde luego en embiar la gente.

Y viendo aun que aqui hay poca gana de hazello, determino de boluer alla con el socorro del dinero, y con el descargar a V. M. de que no es su voluntad de no embialles gente y que los inconvenientes proceden del duque de Parma solo, y que llegando a notizia de V. M. asegurarles que metera remedio con gran diligencia.

Que en el entretanto tengan paciencia, con entretenerse lo mejor que se pudiere, sin resolverse a cosa de que tanto danno vernia a ellos y a la religion, y confio mucho en la buena voluntad del dicho Deumayne, y que me dara credito en lo que le dixere, dandole a entender no ser la falta de V. M. pues les socorre en lo que mas importa que es dineros.

Y para mejor podello hazer y que en el negocio se mire y se haga todo lo que humanamente se puede para que salga bien a satisfacion de V. M. que es a que sobre todo tengo puesta la mira, siendo de la importancia que es;

He determinado de dar parte

Je suis venu ici pour y pourvoir, n'ayant encore déclaré au duc de Parme d'autre mystère que le risque que l'on court de tout manquer, si Votre Majesté ne se déclare pas aussitôt en envoyant des troupes.

Et voyant encore qu'ici on n'a guère envie de le faire, je décide de revenir là-bas avec le secours en argent, et pour disculper Votre Majesté en disant que votre volonté n'est pas de ne point leur envoyer des troupes et que les difficultés viennent du duc de Parme seul, et pour leur assurer que dès que Votre Majesté en aura connaissance elle y mettra remède en grande diligence.

Que pendant ce temps ils prennent patience en se maintenant le mieux qu'ils pourront, sans se résoudre à une chose dont il résulterait tant de préjudice et pour eux et pour la religion. Et je compte beaucoup sur la bonne volonté dudit de Mayenne, et qu'il me croira en ce que je lui dirai, lui donnant à entendre que ce n'est pas la faute de Votre Majesté puisqu'Elle les secourt avec ce qui est le plus important : l'argent.

Et afin de pouvoir mieux faire et pour que, dans cette négociation, on considère et l'on fasse tout ce qui se peut humainement afin que cela tourne bien à la satisfaction de Votre Majesté, et c'est surtout ce à quoi je vise, cela étant d'une telle importance;

J'ai résolu de faire part de tout

de todo à Juan Bautista de Tassis, y pedille por lo que toca al servicio de V. M. quiera venir conmigo hasta donde está el duque d'Eumeyna pues está tan cerca de la contrada para que juntos apuremos alli todas las cosas, y se haga la capitulacion todo lo mas cumplido que sea posible.

A lo qual se ha dispuesto con la aficion y zelo que siempre tuvo al servicio de V. M. que por aca ne se perdera tiempo, como seria fuerza que se hiciese quando ello se huviese de remitir a que pudiese hallarse en ello Don Bernardino, que esta lejos, sino que se podra acavar luego.

Que es lo que importa, pues son cosas estas tan subjettas à mudanza haviendo dilacion de tiempo:

Quanto se dexa considerar de mas de no estar Don Bernardino muy en gusto del Deu mayne haviendoseme quexado de que con los de Paris trata cosas que se las podria excusar, pordo podria caer en sospechas de que se trata con el doblez, que no es medio dacomodar sino antes de gastar las cosas.

Y ansi lo tengo escrito a don Bernardino, para que se vaya a la mano, y no se arroje tanto, ni se fide con quien trata.

Porque no hazen sino descubrillo el pecho, y luego lo cuen-

à Jean-Baptiste de Tassis, et de lui demander pour ce qui concerne le service de Votre Majesté, de vouloir bien venir avec moi jusqu'à l'endroit où est le duc de Mayenne, puisqu'il est si près de la contrée, afin que, ensemble, là-bas, nous examinions à fond toutes choses, et pour que le pacte se fasse de la façon la plus parfaite possible.

A quoi il s'est préparé avec le dévouement et le zèle qu'il a toujours eus pour le service de Votre Majesté, car de notre côté nous ne perdrons pas de temps, on en prendrait forcément, s'il fallait attendre que don Bernardino qui est loin, pût s'y trouver; sans lui, cela pourra bientôt être terminé.

C'est ce qui est important, car ce sont là choses sujettes à changement, s'il y a des retards.

D'autant plus qu'il faut considérer encore que don Bernardino ne plait pas beaucoup au duc de Mayenne, celui-ci s'est plaint à moi qu'il traite avec ceux de Paris de choses dont il pourrait se dispenser; par là, il pourrait soupçonner que l'on traite avec dissimulation, ce qui ne serait pas le moyen d'arranger, mais plutôt de gâter les choses.

Et ainsi j'ai écrit à don Bernardino, pour qu'il se surveille et ne se hasarde pas tant, et ne se fie pas à celui avec qui il traite.

Car ils ne font que lui tirer des secrets, et ensuite ils les

tan a este otro el qual esta muy sentido; que entiendo lo escriviria à V. M.

Y la que con esta va es la duplicada de la suya que de Ruan embie.

Dios garde a V. M.

De Anveres a veinte y ocho de octubre.

Juan de Moreo.

racontent à l'autre qui est très fâché, et je crois qu'il a dû l'écrire à Votre Majesté.

Et la lettre ci-jointe est le duplicata de la sienne que j'envoyai de Rouen.

Que Dieu garde Votre Majesté.

D'Anvers, le 28 octobre.

Juan de Moreo.

Nota : La mention suivante existe à la suite de la lettre de Moreo; mais elle a été effacée :

« Il en est ainsien l'original demeuré entre les mains de nous, Conseiller et Maître des Requêtes ordinaire de l'Hôtel du Roy.

Signé : François Viète. »

NOTE II

INDISCRÉTIONS DE VIÈTE

Voici ce que dit M. Armand Baschet, au sujet de Viète :

« En 1595, un avis de l'ambassadeur Giovanni « Mocenigo, récemment revenu de la cour de « France, avait mis en émoi tout le Conseil, et « comme le document qui le rapporte touche aux « choses de cette cour, nous le traduisons ici, en « conservant autant que possible la forme presque « ingénue du récit :

1595, 5 Juin, en Conseil des Dix.

« Les illustrissimes seigneurs chefs, ayant fait « appeler le très illustre seigneur Zuane Mocenigo, « revenu de son ambassade en France, et l'ayant « invité à exposer ce qu'on avait appris qu'il lui « était arrivé relativement à la divulgation de nos « chiffres, il répondit :

« Je me trouvais à Tours, où m'entretenant un « jour avec M. de Viète, il en vint à me dire qu'on

« avait intercepté un très grand nombre de lettres « en chiffres, tant du roi d'Espagne que de l'Em- « pereur et autres princes, lesquelles avaient été « déchiffrées et interprétées par lui, en raison des « notions particulières qu'il avait des écritures « chiffrées. Et comme je lui montrais beaucoup « d'étonnement, il me dit : *J'en donnerai des « preuves effectives à Votre Seigneurie.* Il m'apporta « aussitôt un gros paquet de lettres desdits Princes « qu'il avait déchiffrées, et m'ajouta : « *Je veux que « vous sachiez que je comprends, et que je traduis « votre chiffre.* » *Je ne veux pas le croire, dis-je, à « moins que je ne le voie.* Et comme j'avais trois « sortes de chiffres, un ordinaire dont j'usais, un « autre différent dont je n'usais pas, et le troisième « appelé *dalle Caselle*, il me montra qu'il com- « prenait le premier. Pour mieux pénétrer alors ce « qui en était dans une affaire aussi grave, je lui « dis : *Vous comprenez sans doute aussi notre chiffre « dalle Caselle ?* Il répondit : « *Pour celui-là, il faut « en sauter beaucoup* », voulant dire qu'il ne com- « prenait que par morceaux.

« L'ayant prié de me faire voir quelques-unes de « nos lettres déchiffrées, il me promit de le faire; « mais, s'étant depuis en allé, il ne m'en parla plus, « et je ne l'ai plus vu. Toutefois, on peut tenir pour « certain, d'après ce qu'il m'a dit et montré des « chiffres des autres Princes, et pour ce qu'il m'a

« confidentiellement avoué dans le cours de la con-
« versation, que nos chiffres ne sont pas aussi dif-
« ficiles à traduire que nous le croyons. J'ai gardé
« tout cela bien en mémoire, étant chose d'une
« importance bien reconnue de Vos Seigneuries,
« et aussitôt arrivé, j'ai voulu, pour l'acquit de ma
« conscience, vous le faire savoir, afin que soient
« promptement prises les mesures qui paraîtront
« nécessaires à la prudence de vos Seigneuries.
« Ce qu'ayant dit, il se retira. »

* * *

Peu de jours après cette déclaration, le 12 juin suivant, le Conseil des Dix changea en effet tout le service du chiffre des ambassadeurs de la République, et leur envoya les inventions nouvelles du plus habile chiffreur qu'elle eût à cette époque, le sieur Pietro Partenio.

NOTE III

LE SERVICE DES CHIFFRES A VENISE

Les Archives de Venise — *Histoire de la Chancellerie secrète*, d'Armand Baschet — renferment plusieurs passages intéressants sur les chiffres de la République de Venise et sur les déchiffreurs.

Il nous a paru utile de les rapporter ici.

Page 111 : M. Luigi Pasini, employé aux Archives, aurait fait l'histoire des chiffres diplomatiques et l'étude de leur interprétation. Il a, de plus, reconstitué les clefs des chiffres de Giovanni Michieli, ambassadeur à la Cour d'Angleterre sous Marie Tudor et des ambassadeurs à la Cour de France pendant une période de douze années.

Page 191 : En récompense d'un avis aux inquisiteurs d'État, sur la possibilité de surprendre le secret des chiffres, on libéra d'une condamnation qu'il avait encourue l'auteur de cet avis.

Page 305 : Manière dont les ambassadeurs chiffraient. Certaines dépêches sont entièrement chiffrées; d'autres, sont partie en clair, partie en chiffres;

on chiffrait surtout les récits d'audience et on s'attachait à reproduire les propres termes dont s'était servi le souverain.

Lorsque les dépêches chiffrées arrivaient à Venise, elles étaient remises aux secrétaires aux chiffres, qui en faisaient une traduction à part, intercalée ensuite dans la dépêche originale.

Page 576 : Dans un des chapitres relatifs au Conseil des Dix, M. Armand Baschet entre dans de grands détails sur l'importance attachée à la sécurité du chiffre.

« Le Conseil s'occupait surtout du renouvelle-
« ment de ces inventions pour dérouter le mieux
« possible la curiosité des cabinets étrangers et
« mettre en défaut l'habileté de ceux qui s'exer-
« çaient à en découvrir le secret, dans l'intérêt des
« Ministres qu'ils servaient.

« Lorsque le Conseil des Dix avait conçu le
« moindre soupçon sur la pénétration d'un de ses
« alphabets en chiffres, il en déclarait aussitôt la
« nullité et prenait des mesures pour qu'il fût
« promptement remplacé.

« Il ordonnait à cet effet une sorte de concours et
« choisissait trois de ses membres pour être juges
« de la meilleure et plus sûre invention. Ces juges
« devaient présenter chacun un rapport aux chefs
« du conseil sur les qualités, les défauts ou les
« inconvénients des compositions que leur avaient

« présentées les *secrétaires députés aux chiffres*, « parmi lesquels il en était d'une extraordinaire « habileté. »

*
* *

Un traité des chiffres établi par Agostino Amadi existe aux Archives de Venise; il est intitulé : *Trattati varii sullo scrivere en cifrà.*

Les chapitres principaux de ce traité sont :

3e chapitre. — Polisteganografia.
4e chapitre. — Apogriptografia.
5e chapitre. — Chiffres invisibles.
6e chapitre. — Chiffres inventés par l'auteur.
7e et 8e chapitres. — Déchiffrements.

NOTE IV

CHIFFRE COMPLÉMENTAIRE

DÉCHIFFREMENT NUMÉRIQUE

1° *Chiffre complémentaire*

Le chiffre est dit complémentaire lorsque, en employant deux méthodes différentes, le résultat de l'une est le complément de l'autre.

On a vu, au chapitre 1er de la deuxième partie, que les cryptogrammes UARR et GAJJ représentaient tous les deux le mot **bien**, chiffré par la méthode de Beaufort; UARR a été obtenu en plaçant la clef **vive** en dessous; GAJJ s'obtient avec la même clef, mais placée en dessus.

En attribuant à chacune de ces lettres la valeur numérique que lui donne son rang d'après les tableaux ci-après.

1° Rang des lettres dans l'alphabet normal :

A	B	C	D	E	F	G	H	I	J	K	L	M	N	O
1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
P	Q	R	S	T	U	V	W	X	Y	Z	Ä			
16	17	18	19	20	21	22	23	24	25	26	27			

2° Rang des lettres dans l'alphabet retourné :

Z	Y	X	W	V	U	T	S	R	Q	P	O	N	M	L
1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
K	J	I	H	G	F	E	D	C	B	A				
16	17	18	19	20	21	22	23	24	25	26				

on obtient :

	U	A	R	R	G	A	J	J	UG	AA	RJ	RJ
									Totaux constants			
1er alphabet normal.	21	1 ou 27	18	18	7	27 ou 1	10	10	28	28	28	28
2e alphabet retourné. . . .	6	26	9	9	20	26	17	17	26	26	26	26
Autres totaux constants . .	27	27	27	27	27	27	27	27	54	54	54	54

GAJJ est dit complémentaire de UARR ; les lettres identiques dans les deux méthodes sont A et N.

2° *Déchiffrement numérique*

Une fois la clef trouvée, on peut, si on le désire, déchiffrer sans faire usage du tableau cryptographique.

Une simple addition et une simple soustraction donnent le même résultat que si on parcourait des yeux ledit tableau cryptographique.

On va opérer sur les trois différents chiffres WQZR UARR, GAJJ, qui ont été obtenus avec la clef **vive** en remplacement du mot **bien**[1].

Selon que l'on a employé l'une ou l'autre des méthodes, on chiffre la clef par l'alphabet **normal** ou **renversé**; on additionne la clef et le texte chiffré, puis on diminue 26 ou 27 (36 ou 37 si la valeur des lettres a été majorée de 10, comme c'était le cas pour les dépêches du duc d'Orléans), et on lit d'après l'alphabet **normal** ou **renversé**.

Voici la manière de s'y prendre en supposant que la transformation des lettres du cryptogramme en chiffres arabes ait été faite avec le tableau cryptographique du chapitre 1er (majoration de 10).

[1] Voir chapitre 1er de la deuxième partie.

1° Méthode de Vigenère :	W.	Q.	Z.	R.
Inscrire le texte chiffré	33	27	36	28
Inscrire la clef *vive* chiffrée d'après l'alphabet *retourné*	5	18	5	22
Faire l'addition.	38	45	41	50
Inscrire le nombre fixe à diminuer (36 ou 10)	36	36	36	36
Faire la soustraction. . . .	2	9	5	14
Transformer en lettres d'après l'alphabet *normal*	B	I	E	N

2° Méthode de Beaufort, clef en dessous	U.	A.	R.	R.
Texte chiffré	31	11	28	28
Clef chiffrée d'après l'alphabet *retourné*. .	5	18	5	22
Addition	36	29	33	50
Nombre fixe *à diminuer* (37 ou 11) . . .	11	11	11	37
Soustraction	25	18	22	13
Transformation en lettres d'après l'alphabet *retourné*.	B	I	E	N

3° Méthode de Beaufort, clef en dessus	G.	A.	J.	J.
Texte chiffré	17	11	20	20
Clef chiffrée d'après l'alphabet *normal*.	22	9	22	5
Addition	39	20	42	25
Nombre fixe à diminuer (37 ou 11). . .	37	11	37	11
Soustraction.	2	9	5	14
Transformation en lettres d'après l'alphabet *normal*	B	I	E	N

Nota. — Si le chiffrement n'avait pas été majoré de 10, le nombre fixe à diminuer aurait été :

Méthode de Vigenère, 26 ou 0;
Méthode de Beaufort, 27 ou 1.

NOTE V

TRIGRAMME ET TÉTRAGRAMME SEMBLABLES PRODUITS PAR LE HASARD

Deux des télégrammes du duc d'Orléans publiés par un journal, lors du procès devant la Haute-Cour, présentant comme particularités des répétitions qui ne sont pas dues à la périodicité de la clef, il a paru intéressant de les donner ici pour bien démontrer que le principe de Kasiski, quoique exact, n'est pas absolu, et qu'un déchiffreur qui aurait persisté à se baser sur cette indication de longueur de clef n'aurait jamais pu arriver à faire la traduction.

1° *Trigramme*

Le télégramme est du dimanche 19 février.

3021	1335	3316	1814	1115	2719	2025	1828
1115	2722	3336	2921	2034	3501		

En transformant les chiffres, pris 2 par 2 en lettres, selon la valeur donnée par le tableau servant à chiffrer et à déchiffrer, on obtient :

T K C Y W F H D A E Q I J O H R A E Q L W Z S K J X Y.

01, ne pouvant se transformer, ne peut être qu'un groupe nul terminant la dépêche, à moins qu'il n'indique le nom de l'expéditeur du télégramme, d'après un répertoire spécial en possession des correspondants.

L'intervalle entre les deux A E Q étant de 8, on est en droit de supposer, sachant surtout par des déchiffrements antérieurs que la clef était le jour, le quantième, le mois, que la clef de ce télégramme chiffré était **dimanche,** mot de 8 lettres. L'essai de déchiffrement n'a rien donné. Que peut-on bien avoir fait, se demande le déchiffreur?

Il essaie alors à l'envers. Pas de résultats. Il essaie les trois chiffres différents que peuvent donner les méthodes de Vigenère et de Beaufort. Pas davantage de résultat.

Il essaie le 2e chiffre de Vigenère complémentaire du 1er. Toujours pas de résultat.

* * *

Considérant comme certains la longueur de la clef : 8, et le mot clef **dimanche,** le déchiffreur est, amené à supposer qu'on s'est servi d'un autre tableau : un tableau à alphabets intervertis.

Il s'agit de reconstituer ce tableau, sinon en entier, du moins pour les lettres de la clef; ce n'est pas très facile; mais enfin on peut y arriver, surtout

en se pénétrant bien de la théorie sur la *symétrie de position* donnée par Kerchkoffs.

Le cryptogramme est ainsi arrangé :

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

Les lettres soulignées confirment le déchiffreur dans l'idée qu'il est sur la bonne piste, et finalement, ne pouvant rien trouver, puisque *dimanche* n'est pas la clef, il en est réduit à abandonner son travail et à déclarer son impuissance.

S'il veut ménager son amour-propre et ne pas s'avouer vaincu, il conclut à des erreurs qui l'empêchent d'aboutir.

*
* *

La clef étant : *Je lui demandai mon chemin*, 19e vers de la *Nuit de Décembre* d'Alfred de Musset, les lettres A E Q signifiaient *art* et *clu* et étaient obtenues par *a n d* et *c h e* de la clef.

T K C Y W F H D A E Q I J O H R A E Q etc
j e l u i d e m a n d a i m o n c h e
a r t c l u

2° *Tétragramme*

Le télégramme est du vendredi 17 février.

1724	2022	2428	1215	2528	2616	1322	2925	2135
2434	3024	1412	1922	2024	3615	2519	1729	2918
1216	3624	1530	2414	1220	2023	3627	2737	2726
3012	2522	3422	2321	3235	3727	1519		

La transformation des chiffres en lettres donne :

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

Les répétitions : E O sont à 22 d'intervalle.
T N D B — 21 —
A Q — 13 —

Le tétragramme étant à 21 d'intervalle, on en conclut que la clef doit être de 3, ou de 7, ou de 21. Les essais faits avec ces longueurs de clef ne donnèrent rien, puisque la clef : vendredi 17 février avait comme longueur 22 et non 21.

D'ailleurs le premier T N D B se traduit par *lesd* avec la clef *e r v e*, et le 2e donne en traduisant *prou* avec la clef *i e r v*. **Erve** et **ierv** appartiennent aux dernières lettres du mot *février* et aux premières du mot *vendredi*.

* * *

Ces deux exemples prouveront au lecteur combien, en cryptographie, aucune règle n'est absolue, et combien il ne faut jamais persister outre mesure dans des recherches même indiquées par le calcul, si les essais de déchiffrement sont infructueux. Il ne faut alors ni se buter, ni se rebuter, et faire comme en politique : changer son fusil d'épaule.

NOTE VI

DÉPÊCHE A LA CAMBRONNE DU DUC D'ORLÉANS

Le télégramme à la Cambronne du duc d'Orléans ayant fait un certain bruit dans la Presse, nous avons cru intéresser le lecteur en en donnant la traduction complète, précédée de la dépêche chiffrée, erronée, qui n'a pu être lue par le destinataire.

Paris, le 12 décembre 1898, 4 h. 30 soir.

1837	2636	3326	2621	3026	1619	1337
1231	2824	1430	2712	2331	3525	2318
1214	2319	3714	1229	2625	1623	1712
3119	1613	2719	2920	3312	2822	2611
2125	2928	3135	1626	1933	1725	1736
3633	2615	1716	2633	2525	2130	2634
2413	3513	2232	1113	1928	2522	1517
3416	26					

En se servant comme clef des mots : Lundi, douze décembre, le lecteur pourra transformer ces chiffres en langage clair, disant : succès d'estime environ deux mille hommes, mais police et municipaux *r a u i s e t* laissa pas passer, c'est à recommencer. Thuret.

*
* *

Voici le texte de la réponse, partie d'Evesham le 13 décembre 1898 à 9 h. 35 matin.

TÉLÉGRAMME

3733	3737	1514	1225	2020	2524

Déchiffrement [1]

Transformation des chiffres en lettres.	A W A A E D B O S J O N
Clef.....	m a r d i t r e i z e d
La traduction donne.....	M E R D E Q Q Q Q Q Q

Le mot est énergique.

Cambronne l'a jeté avec rage aux Anglais.

Victor Hugo l'a fait sublime.

Le duc d'Orléans l'agrémente d'une suite... fin de siècle !

[1] Voir le tableau du chapitre 1er de la deuxième partie.

NOTE VII

CRYPTOGRAPHE CYLINDRIQUE

Avant de donner la description de cet appareil, nous allons exposer sommairement la valeur scientifique du chiffre qu'il peut donner.

Le nombre d'alphabets interchangeables étant de 20, le nombre de combinaisons est donné par la formule des permutations qu'on peut faire subir à 20 objets différents, c'est-à-dire :

1 X 2 X 3 X 4 X 5 X 6 X 7 X 8 X 9 X 10 X 11 X 12 X 13 X 14 X 15 X 16 X 17 X 18 X 19 X 20 = DEUX QUINTILLIONS en chiffres ronds

soit 2 unités suivies de 18 zéros; c'est inimaginable, mais cela est.

Nous négligeons, intentionnellement, les 25 combinaisons de chaque alphabet, parce que ces combinaisons ne donneraient qu'une valeur illusoire; si mathématiquement le nombre de combinaisons est 2 quintillions puissance 25, nous nous en tenons à 2 quintillions tout court.

*
* *

Un coffre fort ayant 4 alphabets de 25 lettres donne comme nombre de combinaisons, 25 puissance 4 = 390.625.

En comparant la sécurité du coffre-fort à celle du cryptographe cylindrique, le lecteur pourra constater qu'il est 5 trillions de fois plus aisé d'ouvrir un coffre-fort dont on ne connait pas le mot que de déchiffrer un cryptogramme fait avec le cryptographe cylindrique si on n'en possède pas le mot clef.

*
* *

M. de Viaris, dont nous avons parlé au chapitre II de la deuxième partie de cette étude, a trouvé, *en théorie*, une formule mathématique de déchiffrement.

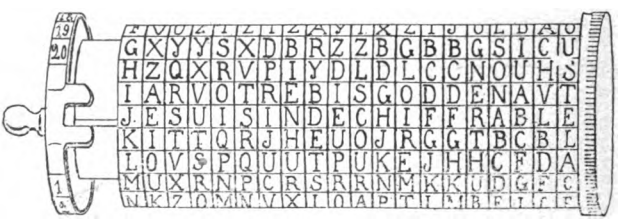
Cette formule *mathématique* n'a pu cependant aboutir à donner la traduction du cryptogramme de feu M. Edouard Lucas, qui termine l'exposé de l'appareil fait au Congrès de Marseille de 1891 pour l'avancement des sciences.

Le chiffre donné par le cryptographe cylindrique ne craint aucune espèce de recherche ni d'investigation; il est absolument indéchiffrable pour quiconque ne possède pas le mot secret. Il ne craint que la livraison du mot clef.

Description de l'appareil

L'appareil se compose de :

1° Un corps cylindrique, terminé à une extrémité par un disque invariablement fixé sur le



cylindre et présentant une fourche indicatrice, et à l'autre extrémité par un disque moleté de fermeture se vissant sur le cylindre ;

2° Des rondelles-alphabets au nombre de vingt, portant chacune vingt-cinq lettres [1] (caractères latins).

Les alphabets ainsi gravés sur les rondelles sont tous différents les uns des autres par l'ordre dans lequel les caractères sont placés.

Les rondelles-alphabets portent chacune, sur un des côtés, un numéro d'ordre ;

[1] Le W, qui n'existe pas dans les alphabets des appareils télégraphiques Hughes et Baudot, a été supprimé sur le cryptographe. Pour chiffrer W, on chiffre deux V successifs.

3° Une baguette-arrêtoir, dont la tête peut se visser dans le disque fixe du corps du cryptographe et dont la tige, en partie noyée dans un sillon longitudinal tracé sur le cylindre, pénètre dans des encoches pratiquées sur la face intérieure des rondelles et correspondant aux lettres gravées sur la face extérieure.

Trousse. — L'appareil au repos est enfermé dans une trousse en cuir, divisée par des anneaux de laiton en compartiments pouvant contenir: celui de gauche, le disque mobile; ceux du milieu, chacun cinq rondelles.

Le cylindre s'engage facilement dans les anneaux et dans les rondelles placées dans leurs compartiments.

La baguette-arrêtoir est enfilée dans deux brides cousues sur le revers de la trousse.

La disposition de la trousse obligeant à enlever les rondelles pour y placer le cylindre, on n'aura aucune raison pour ne pas les replacer dans l'ordre naturel de leurs numéros[1], ce qui permet de remonter l'appareil très rapidement et en rend la perte absolument sans danger.

[1] Le démontage de l'appareil et le rangement méthodique dans la trousse demandent, sans se presser, au plus trois minutes.

*
* *

Clef. — La clef consiste dans l'ordre de placement des rondelles sur le cylindre.

Cet ordre est donné par un mot répété autant de fois qu'il est nécessaire pour faire vingt lettres.

Pour transformer ce mot en chiffres, on inscrit 1 au-dessous de la première lettre de l'alphabet naturel employée la première fois ; le chiffre 2 au-dessous de la même lettre employée la deuxième fois, etc. ; le chiffre suivant au-dessous de la deuxième lettre de l'alphabet naturel employée la première fois, et ainsi de suite.

L'exemple suivant fera comprendre aisément le procédé à suivre.

Mot clef [1]. — B A T A I L L O N
II. I. VII. (I) III. IV. (IV). VI. V.

Nota.— Les chiffres romains placés au-dessous des lettres indiquent leur ordre dans l'alphabet naturel.

Transformation numérique { B A T A I L L O N B A T A I L L O N B A
6. 1. 19. 2. 9. 11. 12. 17. 15. 7. 3. 20. 4. 10. 13. 14. 18. 16. 8. 5

[1] Il est bien entendu que le mot clef dont on convient doit rester absolument secret. On peut d'ailleurs, par une entente préalable, changer ce mot plus ou moins complètement, toutes les fois qu'on le veut.

Le papier qui a servi à transformer le mot clef en chiffres est brûlé aussitôt que le cryptographe est monté.

* * *

Montage de l'appareil a la clef[1]. — Pour monter l'appareil à la clef : Sortir de la trousse le corps du cryptographe, disposer les rondelles sur une table, sur quatre rangées de cinq, par ordre numérique. (Il suffit de les prendre par cinq dans la trousse et de les étaler ; elles se trouvent ainsi tout naturellement disposées.)

Faire le mot numérique et enfiler les rondelles sur le cylindre, dans l'ordre des numéros placés au-dessous du mot clef. (Dans l'exemple qui précède, on placerait la rondelle n° 6 la première, n° 1 la deuxième, n° 19 la troisième, et ainsi de suite.)

Visser le disque mobile, et l'appareil se trouve monté à la clef.

Nota. — Il faut enfiler les rondelles le numéro d'ordre en dessus ; autrement les lettres seraient à l'envers.

* * *

Chiffrement. — Pour chiffrer, on amène la première lettre à chiffrer, prise sur la première rondelle, en regard de la fourche indicatrice ; la

[1] L'opération du montage, longue à énumérer, est extrêmement simple dans son exécution. Elle ne demande, sans se presser, que cinq minutes, montre en main, y compris le chiffrement du mot et son incinération.

deuxième lettre à chiffrer, prise sur la deuxième rondelle, à côté de la première, et ainsi de suite, en ayant soin de fixer de temps en temps les rondelles placées en poussant plus avant la baguette-arrêtoir et en la vissant d'un demi-tour lorsqu'on a fini la ligne.

Lorsque les vingt rondelles sont disposées, on lit dans la ligne de la fourche les mots formés par les vingt premières lettres du texte à chiffrer.

On relève ensuite le chiffre de ces vingt lettres.

Ce chiffre est donné par une ligne horizontale quelconque, choisie au gré et au caprice du chiffreur.

On continue l'opération pour les vingt lettres suivantes, et ainsi de suite jusqu'à ce que la dépêche entière soit chiffrée.

On chiffre toujours vingt lettres à la fois.

Le reliquat seul peut être inférieur à ce nombre.

Si ce reliquat ne comporte que cinq ou six lettres, il est avantageux pour le déchiffrement de prendre le chiffre sur la ligne horizontale située au-dessus ou au-dessous de la fourche indicatrice.

On a avantage à prendre également une de ces lignes, lorsque le texte qu'on veut chiffrer comporte des lettres conventionnelles de nombres, en assez grande quantité.

*
* *

Déchiffrement. — Le déchiffrement s'opère comme le chiffrement.

On amène les lettres du cryptogramme en regard de la fourche indicatrice. Lorsqu'on a placé les vingt premières lettres, on cherche autour du cryptographe la ligne horizontale qui donne la traduction en clair; *elle saute aux yeux immédiatement*, car une seule de ces lignes horizontales présente un assemblage de lettres formant des mots ayant un sens.

On répète l'opération pour les vingt lettres suivantes, et ainsi de suite jusqu'à ce que tout le cryptogramme soit déchiffré.

S'il ne reste que quelques lettres, on les trouvera au-dessus ou au-dessous de la fourche.

C'est parce que ces quelques lettres peuvent ne pas présenter à l'œil un sens immédiatement clair, qu'on prescrit ce qui est dit plus haut, pour le chiffrement du reliquat. Il en est de même d'une ligne contenant beaucoup de lettres représentant conventionnellement des nombres.

*
* *

Chiffrement de la ponctuation et des nombres. — Quoique l'appareil ne porte que des lettres, on peut, sans inscrire les nombres en toutes lettres,

ce qui allonge beaucoup le chiffrement et les transmissions télégraphiques, adopter des lettres conventionnelles faciles à reconnaître, en les encadrant entre des K, et faciles à traduire.

La lettre K est avantageuse parce qu'elle est très peu usitée dans la langue française, et peut, sans inconvénient, être l'indicatrice de la ponctuation et des nombres.

Pour indiquer un signe de ponctuation, on encadre ce signe représenté par sa lettre conventionnelle entre deux K ; pour indiquer un nombre, on encadre ce nombre représenté par une ou plusieurs lettres conventionnelles entre deux doubles K[1].

Lettres conventionnelles de ponctuation

A	B	C	D	E	F	G	H	I	J
.	,	;	:	'	!	?	-	·/·	( )
point	virgule	point et virgule	deux points	apostrophe	point d'exclamation	point d'interrogation	trait d'union	alinéa et point final	parenthèse

Lettres conventionnelles des nombres

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

Lettres conventionnelles des accessoires des nombres

L	M	N	O	P	Q
barre de fraction	terminaison « ième »	« er ou o »	virgule entre deux chiffres	mot « numéro »	mot « et » entre deux chiffres

[1] Ou bien, encadrer les nombres entre deux K et les signes de ponctuation entre deux doubles K. C'est une affaire de convention.

Exemples de chiffrement

Pour chiffrer	2500	placer dans la ligne de la fourche		K K C F A A K K
—	15/100	—	—	K K B F L B A A K K
—	1er ou 1e	—	—	K K B N K K
—	7e	—	—	K K H M K K
—	5, 6, 7, et 8	—	—	K K F O G O H Q I K K
—	n° 4	—	—	K K P E K K
—	point	—	—	K A K
—	point à la ligne	—	—	K A I K

Dans la pratique, en fait de ponctuation, on ne chiffre guère que le point. Les apostrophes, traits d'union, virgules, etc., n'ont pas besoin d'être chiffrés pour la clarté du texte; mais on peut le faire, si c'est utile ou nécessaire.

Quant aux nombres, on chiffre soit en toutes lettres, soit au moyen de la convention ci-dessus. On choisit celui des deux systèmes qui est le plus rapide, c'est-à-dire celui qui exige le moins de caractères.

* * *

DÉCHIFFREMENT DE LA PONCTUATION ET DES NOMBRES. — Lorsque le déchiffrement d'une dépêche donne une lettre encadrée entre deux K qui n'ont pas de sens précis, il est facile de reconnaître que la lettre placée entre les deux K est une lettre conventionnelle de ponctuation facile à lire avec la convention adoptée.

Si le déchiffrement donne une ou plusieurs lettres encadrées entre quatre K qui n'ont pas de sens,

il est facile de voir que les lettres placées entre les doubles K représentent des nombres faciles à traduire avec la convention adoptée et la numération ordinaire.

Nota. — Pour ne pas se charger la mémoire des détails relatifs au chiffrement de la ponctuation et des nombres, un tableau des lettres conventionnelles est placé dans le tube du cryptographe pour pouvoir le consulter, si c'est nécessaire. La connaissance de ce document par l'ennemi n'a d'ailleurs aucun inconvénient.

*
* *

Cryptogramme chiffré avec un mot tenu secret et donné comme défiant toutes recherches

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

RÉSUMÉ

Le cryptographe cylindrique donne un chiffre basé sur le principe ci-après :

Emploi simultané de plusieurs alphabets différents pour le chiffrement d'une même dépêche

Son emploi n'exige aucune connaissance spéciale ; il suffit de savoir transformer le mot-clef en mot numérique.

Les opérations du chiffrement ou du déchiffrement se font pour ainsi dire machinalement, sans aucun travail d'esprit, et, par conséquent, sans fatigue intellectuelle.

En cinq minutes on peut apprendre à se servir du cryptographe. Après l'avoir manœuvré une ou deux fois, on devient très habile, pour le placement des lettres. On peut arriver à chiffrer vingt lettres par minute.

Les erreurs de transmission télégraphique n'empêchent point la lecture, car elles se détruisent facilement par le sens général de la dépêche.

Ni l'appareil ni la méthode n'ont besoin d'être tenus secrets.

NOTE VIII

SYSTÈME N'EXIGEANT QU'UN CRAYON ET DU PAPIER

Quoique nous ne soyons pas chauds partisans de ce système, nous allons publier la proposition qui en a été faite au Ministre de la Guerre, fin août 1898 et l'exposé de cette méthode.

Dédaignée à la Guerre, elle pourra peut-être rendre des services à quelques-uns de nos lecteurs.

CRYPTOGRAPHIE MILITAIRE

COMMANDANT BAZERIES

PROPOSITION d'un système cryptographique militaire, n'exigeant qu'un crayon et du papier, facile à retenir de mémoire.

(Copie)

En 1891, j'ai présenté à la Guerre un appareil cryptographique de mon invention, donnant un chiffre facile à établir, facile à traduire, n'exigeant aucun secret de l'appareil, ni aucune étude préalable.

Tous les officiers supérieurs et généraux qui ont eu entre les mains mon cryptographe ont été surpris de sa facilité d'emploi et m'en ont fait des éloges.

Ce cryptographe n'a pas été adopté.

* * *

Il résulte de plusieurs conversations que j'ai eues avec des officiers généraux au sujet de la cryptographie et de la cryptographie militaire en particulier, que l'idée bien arrêtée de l'État-Major général est de trouver un système n'exigeant qu'un crayon et du papier, et pouvant se retenir facilement de mémoire sans le secours d'aucune note écrite.

J'ai fait des recherches et des essais dans cet ordre d'idées. Je n'ose me flatter d'avoir trouvé

un système indéchiffrable. Cependant, si les trois cryptogrammes que je donne plus loin résistent aux essais des déchiffreurs auxquels ils seront soumis, j'aurai peut-être trouvé la solution du problème, cherchée en vain jusqu'ici.

*
* *

Tout système cryptographique trahit sa méthode par l'analyse et la décomposition du cryptogramme. Une fois la méthode trouvée, le reste du déchiffrement n'est qu'un jeu pour un spécialiste un peu habile.

Le système auquel je me suis arrêté a l'avantage de laisser le doute sur la méthode employée ; je dirai plus, il trompe le déchiffreur. Les recherches, portant à faux, ne peuvent aboutir.

Les combinaisons compliquées ne valent rien. Je me suis attaché, comme toujours, à la plus grande simplicité possible. J'ai employé quelques ruses cryptographiques pour déguiser le système. Ces ruses triompheront-elles des déchiffreurs ? Je le pense. Il me semble que, personnellement, j'y aurais été trompé et, par conséquent, dépisté et impuissant.

Reste à savoir si de plus habiles s'y tromperont aussi. Si oui, le système est bon.

Je ne puis, pour le moment, indiquer la méthode

employée; elle est tellement simple que le secret de cette méthode me paraît s'imposer absolument. Cependant je n'ai pas dit mon dernier mot; car, en modifiant un peu cette méthode, tout en lui conservant sa conception originale, on pourrait peut-être arriver à ne pas craindre sa divulgation.

*
* *

J'ai toujours considéré comme un danger réel de baser la sécurité d'un système cryptographique sur le secret de la méthode employée. Trop de négligences peuvent être commises pour que ce secret, objet des convoitises de l'ennemi et forcément en la possession d'un très grand nombre de personnes, reste longtemps *secret*. A mon avis, la sécurité doit résider dans l'excellence du système et dans le seul secret de la clef.

Tout ce que je puis dire, pour l'instant, c'est que, comme rapidité du chiffrement et du déchiffrement, le système ne laisse rien à désirer. Il est aussi rapide, sinon plus, que les systèmes connus ou employés. En plus, chaque cryptogramme est fait avec une clef différente, clef choisie à volonté par le chiffreur sans qu'il soit tenu de l'indiquer au préalable au destinataire. En un mot, le cryptogramme indique et porte sa clef.

*
* *

On remarquera que je ne suis pas aussi affirmatif pour l'indéchiffrabilité que je l'ai été lorsque j'ai présenté mon cryptographe cylindrique, n'étant pas aussi sûr de ce système que je l'étais et le suis toujours de mon cryptographe.

Je donnerai la méthode dès qu'elle me sera demandée.

Cryptogrammes chiffrés d'après la méthode Bazeries et n'exigeant pour leur traduction qu'un crayon et du papier.

N° 1. — 85 Groupes

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

N° 2. — 40 Groupes

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

N° 3. — 48 Groupes

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

Signé : Com[t] Bazeries.

Le 14 septembre 1898, on nous avisait que notre mémoire était soumis à l'examen de la Commission de cryptographie militaire.

Quelque temps après, nous avons été invité par M. le général Niox à faire connaître notre méthode, tenue secrète jusqu'alors.

Voici copie de cette méthode.

CRYPTOGRAPHIE MILITAIRE

COMMANDANT BAZERIES

MÉTHODE n'exigeant qu'un crayon et du papier

(Copie)

POUR CHIFFRER. — Écrire le texte clair de préférence sur du papier quadrillé, une lettre dans chaque case en écriture courante et en laissant une ligne en blanc entre chaque ligne du texte clair. Cette ligne en blanc est destinée à recevoir le chiffrement.

Soit à chiffrer : Envoyez un bataillon d'infanterie au Creuzot, ce soir, par voie ferrée.

Exemple :

e n v o y e z u n b a t a i l l o n d i n f a n t e r i e
a u c r e u z o t c e s o i r p a r v o i e f e r r é e

*
* *

CLEF. — Choisir une clef de substitution. Cette clef consiste en deux lettres quelconques. En attribuant à chacune d'elles leur numéro d'ordre dans l'alphabet normal, on transforme ces deux lettres en un nombre entier.

Exemple :

A B = 1 2
D Z = 4 2 5
B A = 2 1
Z F = 2 5 6
etc. etc.

Une fois la clef choisie, ZF, par exemple; soit : « *Deux cent cinquante-six* », établir un alphabet conventionnel où toutes les lettres existant dans la clef sont en tête, soit : DEUXCNTIQAS et celles non existant dans la clef prennent place à leur suite dans leur ordre d'alphabet, soit : BFGHTKLMOPRVYZ.

Écrire horizontalement cet alphabet conventionnel, du commencement à la fin, dans les cases d'un carré de 5.

Exemple :

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

Écrire à côté dans un carré semblable, mais verticalement, l'alphabet normal du commencement à la fin.

Exemple :

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

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

Nota. — Ne pas se préoccuper des lettres qui se trouveraient être les mêmes dans les cases correspondantes des deux carrés de cinq. C'est un effet du hasard.

*
* *

Chiffrement par substitution. — Une fois la clef établie, substituer à chaque lettre du texte clair, sur la ligne laissée en blanc, la lettre donnée par la clef de substitution et écrire cette lettre en majuscule.

Nota. — Pour ne pas perdre de temps, transformer en suivant, toutes les mêmes lettres, avant de passer à la lettre suivante. En opérant ainsi; l'opération du chiffrement est vite faite.

Exemple :

e	n	v	o	y	e	z	u	n	b	a	t	a	i	l	l	o	n	d	i	n	f	a	n	t	e	r	i	e
P	L	A	V	O	P	Z	C	L	N	D	Y	D	K	I	I	V	L	J	K	L	E	D	L	Y	P	G	K	P

a	u	c	r	e	u	z	o	t	c	e	s	o	i	r	p	a	r	v	o	i	e	f	e	r	r	é	e
D	C	S	G	P	C	Z	V	Y	S	P	M	V	K	G	X	D	G	A	V	K	P	E	P	G	G	P	P

Une fois la substitution opérée, partager le chiffrement en tranches de trois lettres par une ligne noire, rouge ou au crayon.

Exemple :

e	n	v	o	y	e	z	u	n	b	a	t	a	i	l	l	o	n	d	i	n	f	a	n	t	e	r	i	e
P	L	A	V	O	P	Z	C	L	N	D	Y	D	K	I	I	V	L	J	K	L	E	D	L	Y	P	G	K	P

a	u	c	r	e	u	z	o	t	c	e	s	o	i	r	p	a	r	v	o	i	e	f	e	r	r	é	e
D	C	S	G	P	C	Z	V	Y	S	P	M	V	K	G	X	D	G	A	V	K	P	E	P	G	G	P	P

*
* *

CRYPTOGRAMME PAR TRANSPOSITION. — Former le cryptogramme en renversant les tranches de trois lettres.

*
* *

CONVENTIONS. — Il est convenu que les deux premières lettres du cryptogramme indiquent la clef de substitution et que, chaque fois que la première lettre d'un groupe de trois est une voyelle : A.E.I.O.U.Y., cette voyelle est nulle. On fait ainsi des nulles quand on le veut, et autant qu'on le veut. Forcément une nulle doit être employée lorsque la première lettre de la tranche renversée est une voyelle. Lorsque cette première lettre est une consonne, la nulle est facultative.

*
* *

OBSERVATIONS. — On s'arrange pour terminer le cryptogramme en un dernier groupe de 5 lettres, sans fractions, clef comprise, ce qui est facile par la liberté que l'on a de faire des nulles à volonté.

Il est bon d'indiquer le nombre de groupes de 5 lettres en tête de la dépêche, de manière que, si le télégraphe en omet un, on puisse essayer de déchiffrer quand même, sans être obligé de redemander la transmission de la dépêche.

*
* *

Exemple de cryptogramme pour la dépêche chiffrée plus haut :

Général Commandant 8e Corps à
Général Commandant d'Armes à Dijon.

13 groupes. Z F I A L P P O V L C Z A Y D N E I K D
L V I A L K J L D E G P Y D P K G S C A Z C P S Y
V V M P X G K A A G D P K V G P E P P G

*
* *

Pour déchiffrer. — Commencer par éliminer les lettres nulles en faisant les tranches de trois lettres.

Exemple :

13 groupes. (Z) (F) (I) A L P | P O V | L C Z | (A) Y D N | (E) I K D
L V I | (A) L K J | L D E | G P Y | D P K | G S C | (A) Z C P | S Y
V | V M P | X G K | (A) A G D | P K V | G P E | P P G

Cette opération faite, copier en interligne en retournant les tranches.

Exemple :

P L A V O P Z C L N D Y D K I I V L J K L E D L
Y P G K P D C S G P C Z V Y S P M V K G X D G A
V K P E P G G P P.

Il ne reste plus qu'à substituer à chaque lettre du cryptogramme la lettre vraie, d'après la clef indi-

quée et que l'on a eu, au préalable, le soin d'établir, et on lit : Envoyez un bataillon, etc... etc...

Comme on le voit, c'est assez vite fait.

* * *

Les cryptogrammes soumis au déchiffrement, dans mon étude cryptographique du 28 août dernier, sont établis comme il vient d'être exposé dans cette méthode.

Il deviendra aisé de les traduire.

C'est la méthode dans sa plus grande simplicité.

* * *

Comme je l'ai dit dans mon étude précitée et comme on peut maintenant s'en rendre compte, le secret de cette méthode s'impose absolument. Il est déjà imprudent de l'avoir écrite. C'est de vive voix qu'elle aurait dû être communiquée.

Cependant, avec une petite modification, j'espère arriver à ne pas craindre la divulgation du procédé.

Cette modification, je la ferai connaître de vive voix. Avant, il serait utile que des déchiffreurs, connaissant ma méthode, essayent de faire la traduction du nouveau cryptogramme ci-après.

S'il résiste au déchiffrement, c'est que le système est réellement indéchiffrable pour quiconque n'en possède pas la clef.

CRYPTOGRAMME

Fait divers pris, dans un journal, aux nouvelles judiciaires

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

Ce cryptogramme, comme ceux précédemment établis, porte sa clef.

Signé :

Com[t] BAZERIES.

Le lecteur connaît la réponse; elle est du 19 avril 1899, et elle figure au chapitre III de la troisième partie.

Reproduisons-la, quand même :

« Il a été reconnu que la méthode ne présentait « pas les garanties de sécurité suffisantes pour être « adoptée. »

*
* *

Comment concilier cette réponse, bien affirmative, avec le non-déchiffrement du cryptogramme de 43 groupes qui termine l'exposé de notre méthode ?

Mystère !

NOTE IX

TABLE DÉCHIFFRANTE POUR LE PETIT CHIFFRE DE LA GRANDE ARMÉE

Nota. — Ce chiffre n'a pas été changé de toute la campagne et était lu par les Russes.

1	cinq	25	ar.tillerie
2	neu.f	26	trois
3	bu.t.e.e.r.s	27	
4	ca.l.s	28	
5		29	bi
6	c	30	
7		31	
8		32	ca.val.erie.ier
9	ba.l.s	33	
10	d	34	at
11		35	bo.r.d
12	Danzig	36	ai.t
13	*bataill*.s.on.s	37	b
14		38	
15	a.u	39	al.lemagne.and.s.es
16	da	40	co.lonie.s.ale.s
17	fo	41	
18	ab.s	42	
19	a	43	
20	ce	44	deux
21	ac	45	*cav.gaison.s*
22	ar.me.e.s.m$^{t\cdot s}$	46	un.e s
23	d	47	
24	ad	48	in.fanterie

49
50 et
51 ga.r
52 de.fense
53 e
54 gu
55 em
56 do.m.age.s
57
58 fe.u
59 eg
60 ge.neral
61 he
62 er
63 el.s
64
65 go
66 ho
67 di.vision.s
68 en.nemi.s.e.s
69 fa
70 ei
71 fo.r.ce.s.t.te.s.m'
72 ha.i
73 f
74 effet.s.ectif.ve.s.m'
75 di.rection
76 du
77 hi
78 ga.rnison
79 gi.r.s.t
80
81 g
82 es
83 fi
84
85 h
86 es
87 i.j
88
89 i.j
90 o
91 na
92 it
93 li
94 ne
95 mi
96 l
97 im.mense
98
99 me
100
101
102
103 lu
104 nu
105 mu
106 la
107 ma.gasin.s
108 il.s
109 la
110 lo
111 mo.uvement.s
112
113 ig
114 m
115 n
116 ni
117 le
118 in.cendie
119 i.j
120
121 no
122 is
123 j'ai
124 vu
125
126 re
127 pi
128 of
129
130
131 te
132 ve.s
133 om
134 si

135		159	ro
136	que.l.s.le.s	160	pu
137	p	161	vi.s
138	u.v	162	pu
139	oi	163	
140	ru	164	u.v
141	m	165	pe.rte.s
142	y	166	z
143		167	s
144		168	so.ldat
145	ti.on.s	169	r
146	ra	170	va
147	o	171	sa
148	ri	172	
149	on	173	q
150	tu	174	su.r
151	x	175	vo
152	po.se.er.s.sition.s	176	t
153	ot	177	se.s
154	qui	178	
155	ze	179	
156	pa.r	180	
157	to	181	
158	ta	182	es

Nota. — Les mots en italique ne sont pas absolument certains ; ils ne sont que probables. Le contrôle n'a pu en être fait en raison de la rareté d'emploi du groupe dans les dépêches déchiffrées.

TABLE DES MATIÈRES

CHAPITRE III.

CHAPITRE IV

DEUXIÈME PARTIE

Étude sur le chiffre carré. — Dictionnaires chiffrés

CHAPITRE PREMIER

CHAPITRE II

CHAPITRE III

CHAPITRE IV

CHAPITRE V

CHAPITRE VI

CHAPITRE VII

TROISIÈME PARTIE

Étude sur les chiffres militaires français

CHAPITRE PREMIER

CHAPITRE II

CHAPITRE III

APPENDICE

Tours, imprimerie Deslis Frères, rue Gambetta, 6.

Extrait du Catalogue de la **BIBLIOTHÈQUE-CHARPENTIER**
à 3 fr. 50 le volume
EUGÈNE FASQUELLE, ÉDITEUR, 11, RUE DE GRENELLE

OUVRAGES HISTORIQUES ET MILITAIRES

GÉNÉRAL F. CANONGE

Histoire militaire contemporaine..... 2 vol.

ALFRED DUQUET

La Guerre d'Italie (1859) (2e mille)..... 1 vol.
Frœschwiller, Châlons, Sedan (4e mille)..... 1 vol.

METZ

Les Grandes Batailles (3e mille)..... 1 vol.
Les Derniers Jours de l'Armée du Rhin (3e mille)..... 1 vol.

PARIS

OUVRAGES COURONNÉS PAR L'ACADÉMIE FRANÇAISE (PRIX BERGER)

Le Quatre Septembre et Châtillon (3e mille)... 1 vol.
Chevilly et Bagneux (2e mille)..... 1 vol.
La Malmaison, Le Bourget et le Trente et un Octobre (2e mille)..... 1 vol
Thiers, le Plan Trochu et L'Haÿ (2e mille). 1 vol.
Les Batailles de la Marne (2e mille)..... 1 vol.
Second Échec du Bourget et Perte d'Avron, 9-31 décembre (2e mille)..... 1 vol.
Le Bombardement et Buzenval (2e mille)..... 1 vol.
La Capitulation et l'Entrée des Allemands. 1 vol.

GALLI

L'Armée française en Égypte (1798-1801). 1 vol.

AMIRAL JURIEN DE LA GRAVIÈRE

Guerres maritimes contemporaines..... 2 vol.

COMMANDANT ÉMILE MANCEAU

Armées Étrangères (2e mille)..... 1 vol.

4273. — L.-Imprimeries réunies, rue Saint-Benoît, 7, Paris.

F