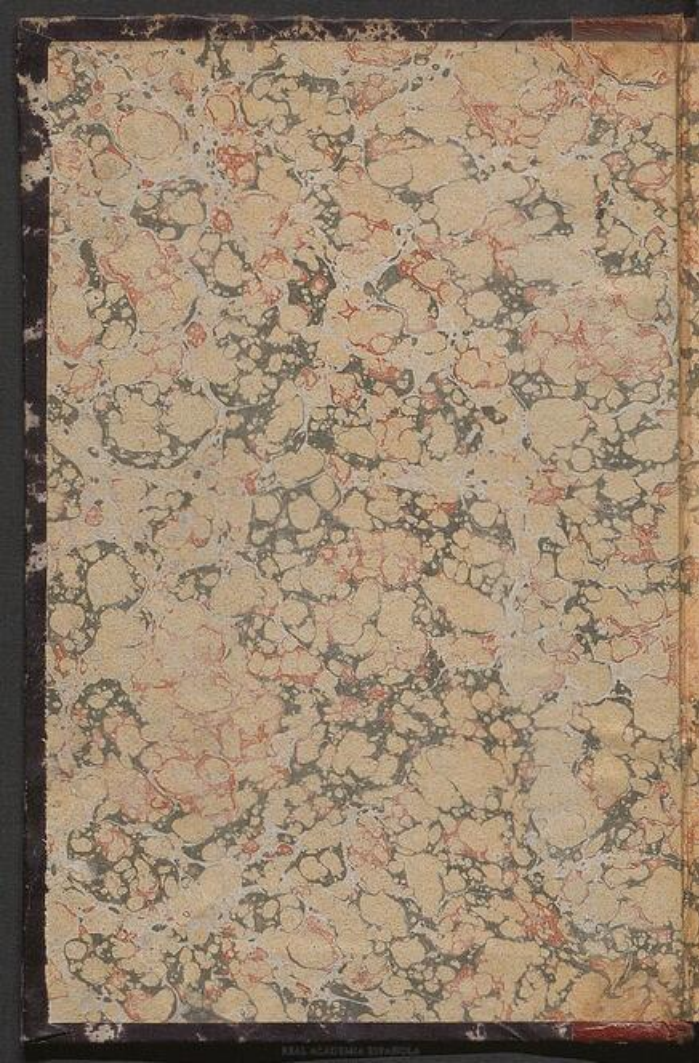


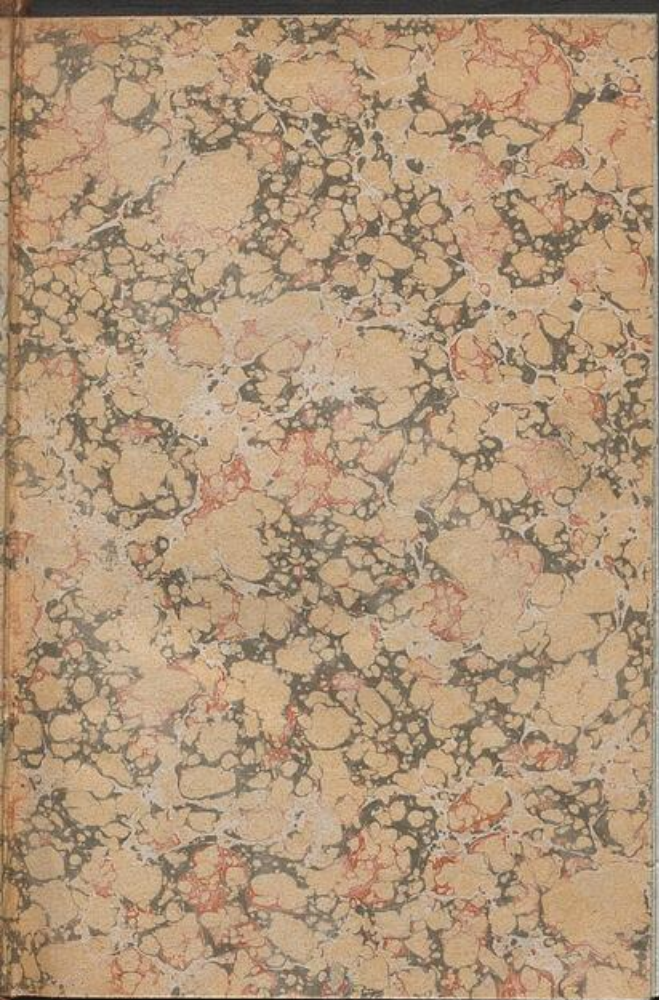


10

X

92





10-X-92

CRYPTOGRAPHIE

UNIVERSELLE.



P. 50

LIBRARY
OF THE
MUSEUM OF
COMPARATIVE ZOOLOGY



CRYPTOGRAPHIE
UNIVERSELLE,
O U
E S S A I
S U R
LA CRYPTOGRAPHIE;

Par N. D. L. P. D. V.



A A M S T E R D A M ;
Et se trouve à P A R I S ,
Chez M O N O R Y , Libraire de S. A. S. Mgr. le
Prince de Condé , rue de la Comédie Française.

M. DCC. LXXXV.





ESSAI

SUR

LA CRYPTOGRAPHIE.

CRYPTOGRAPHIE (ou STÉNOGRAPHIE) signifie écriture en chiffres, ou caractères déguisés (*cæcas litteras, lettres occultes*); ainsi que s'exprime Jules-César dans Suétone, selon D. de Vaines, Dictionn. de Diplôm., tom. 1, pag. 499 : car, qu'on ne s'y trompe pas, un chiffre, dans ce sens, n'est pas plus un caractère Arabe, soit numérique ou autre, qu'un caractère Romain, Grec, &c. ou un de nos caractères de Finances. Un chiffre peut donc être indistinctement l'un ou l'autre de ces

différens caractères; ainsi, 1, 2, &c. I, II, &c. i, ij, &c. sont des chiffres, ou caractères numériques, qui représentent les mêmes idées qu'un, deux, &c.; mais par figures différentes les unes des autres. Or, un chiffre est donc, à proprement parler, un caractère, ou un assemblage de caractères numériques, ou autres, représentatifs, non-seulement d'une ou de plusieurs idées, pour la représentation desquelles nous avons déjà des caractères généralement convenus, mais encore de ces mêmes caractères généralement convenus, qu'on appellera ici, pour se rendre autant sensible qu'il est possible de l'être, vrais caractères, ou caractères naturels.

L'origine de la *Cryptographie* remonte assez haut dans l'antiquité (1), & voici ce qu'en

(1) Voyez le Dictionnaire Mithohermétique: il fait remonter encore plus haut l'origine de la *Cryptographie*; puisqu'il prouve, ainsi que plusieurs autres Auteurs, que les caractères Chymiques viennent des Philosophes Hermétiques, dont Hermès, Trismégiste ou Mercure, étoit le premier. Nous renvoyons notre Lecteur curieux à ce Dic-

dit *Guillet de la Guilletière*, dans un Livre intitulé : *Lacédémone ancienne & nouvelle*. Il prétend que les Lacédémoniens ont été les Inventeurs de l'Art d'écrire en chiffres.

Leurs scytales furent, selon lui, comme l'ébauche de cet Art mystérieux ; c'étoit deux rouleaux de bois, d'une longueur & d'une épaisseur égales : les Ephores en gardoient un, & l'autre étoit pour le Général d'Armée, qui marchoit contre l'Ennemi. Lorsque ces Magistrats lui vouloient envoyer des ordres secrets, ils prenoient une bande de parchemin étroite & longue, qu'ils rouloient exactement autour de la scytale, qu'ils s'étoient réservée : ils écrivoient alors dessus leurs intentions, & ce qu'ils avoient écrit formoit un sens parfait & suivi, tant que la bande de parchemin étoit

tionnaire, singulier dans son genre, puisque la découverte du grand Œuvre y est très-fortement soutenue.

Cet article Cryptographie, du Dictionnaire *Mithohermétique*, est tiré du *Traité des Chiffres de Vigenère, Bourbonnois*, imprimé à Paris en M. D. LXXXVII, chez Abel l'Angelier, avec Privilège du Roi.

appliquée sur le rouleau ; mais dès qu'on la dé-
 veloppoit, l'écriture étoit tronquée & sans liai-
 son : il n'y avoit que leur Général qui pût en
 trouver la suite & le sens, en ajoutant la bande
 sur la scytale, ou rouleau semblable qu'il avoit.

Jules-César écrivoit en chiffre, ainsi qu'Au-
 guste ; nous avons un Livre intitulé :

J O H A N N I S

T R I T H E M I I,

PRIMO SPANHEIMENSIS DEINDE

DIVI JACOBI PÆAROPOLITANI ABBATIS ;

STEGANOGRAPHIA &c.

✠

M O G U N T I Æ,

Sumptibus Joannis-Petri ZUBRODT.

Anno M. DC. LXXVI.

On voit dans l'Ouvrage de cet Abbé, *Livre premier*, une manière d'écrire en chiffre, qui est trop singulière pour ne pas trouver place ici, quoique Latine.

Humanæ salutis Amator universonum Creator maximus Nobis indicit Obedientiam mandatorum, Cui omnes Tenemur obedire, Ex amore; Præmium verò, Obedientibus promisit Sempiternæ felicitatis Tabernaculum possidere; Xti obedientiam inspiciamus, quam Imitari curemus, Ut ad æternam felicitatem nobis promissam ingredi mereamur, Angelorumque consociari Mansionibus sempiternis; agamus pœnitentiam, dum possumus, tempus pretiosum Expendentes fructuosè; Caveamus ne Imperatos mors Rapiat quæ concedere moram alicui recusat. Ideoque, fratres, agere pœnitentiam non tardetis, Velociter enim ad vos mors veniet, Quam nemo, vestrum diu Evadere potest. Dies ergo vestros transeuntes conspiciate pœnitentiam inchoantes, quando tempus habetis; appropinquat hora descendendi hinc: O mors rerum terribilium terribilissima, quam Velociter nos miseros consumis incolatumque nostrum brevissimum, multis injuriis plenum miseris facis esse crudelem! Evigilemus

miseri , Xto Jesu Salvatore nostro piissimo nos exhortante & Contestante ut turpes negligentias Arguamus & bonis operibus Justitiæ vias sollicitè custodiamus. Alme redemptor generis humani exaudi nos , Veniamque nobis tribue peccatorum. O Pater misericordiæ , sis nobis propitius in omnibus adversitatibus nostris ; Sana , Domine , infirmas animas nostras quoniam tui sumus ; Præsta nobis efflicis Vermiculis Requiem sempiternæ Amœnitatis quatenus , te semper aspiciendo laudemus. Amen.

Pour donner une idée de ce chiffre singulier , nous en présentons ici un exemple en François.

Battons à outrance tous nos Ennemis , suivons nos opérations ; après , jouissons d'un repos durable.

Pour savoir ce que signifie cette phrase , prenez les lettres initiales des mots impairs , en commençant par le premier , & vous en aurez le sens : il en est de même du chiffre de l'Abbé Trithème.

D'après ces deux exemples d'écritures en chiffre , l'on doit sentir quelle peine il y a

d'écrire ainsi. Quant à la manière des Lacédémoniens, au premier examen elle paroît *indéchiffable* : mais avec de la patience & un Tourneur adroit, l'on peut rajuster le parchemin sur la fausse scytale : ce nom de fausse que je donne lui convient, puisqu'elle n'est faite que pour surprendre le secret.

Revenons à notre sujet, & examinons quelles sont les qualités d'une *Cryptographie*.

Une *Cryptographie* doit réunir en elle les qualités suivantes, sans lesquelles elle ne pourroit être qu'imparfaite : son principe doit être simple & immuable ; sa marche toujours conséquente & invariable ; son opération facile, & elle doit fournir des combinaisons non pas innombrables (car tout peut se nombrer), mais au moins dont la somme soit telle, que la vie la plus longue de plusieurs hommes, doués de la patience la plus rare, & qui travailleroient consécutivement à déchiffrer une *Cryptographie*, ne pût suffire à rétablir l'ordre naturel ; c'est-à-dire, celui d'où les transpositions Mathématiquement combinées les auroient tirées ; mais le point de perfection d'une *Cryptogra-*



phie, dépend essentiellement de son *indéchiffrabilité* (1).

D'après l'idée qu'on vient de tâcher de déterminer & de fixer sur la définition du mot Chiffre, il est aisé de sentir que tous les caractères numériques ou autres, figures, emblèmes, hiéroglyphes, étant également indifférens pour un chiffre, on doit, pour la facilité de l'opération, tant en écrivant *cryptographiquement*, si l'on peut s'exprimer ainsi, qu'en traduisant un chiffre, préférer, ainsi qu'on l'a fait pour celui dont il est question, les caractères les plus simples & les plus connus; c'est-à-dire, ceux mêmes de l'Idiôme dans lequel on doit être lu. L'Inventeur (2) a fait choix des caractères employés dans l'Alphabet François: or, on peut également,

(1) Peut-être ce mot nouveau paroîtra-t-il hasardé; au reste, l'Auteur n'a pas cherché à le créer: ce mot s'est présenté tout naturellement, & comme de soi-même, à son esprit; il a senti qu'il donnoit une idée juste & précise.

(2) Nous parlons de la *Cryptographie* qui suit cet Essai.

d'après ce qu'on vient de dire, y substituer les caractères *Arabes*, *Grecs*, &c. si c'est en *Arabe*, en *Grec*, &c. qu'on doit être lu; car le caractère ne fait rien à la bonté d'un chiffre; s'il n'a pour lui que son caractère, il n'est *indéchiffrable* que pour celui qui ignore les caractères de l'Idiôme qu'on a feint d'employer.

Le style *allusoire*, l'allégorique, le *figuré*, les signes hiéroglyphiques, les emblèmes, quoique très-connus, peuvent encore embarrasser considérablement les indiscrets; mais nécessairement, ils ont une complication; ils exigent un travail, & leur marche est d'une lenteur, qui ne permet que très-rarement d'en faire usage; ils sont même toujours tellement bornés, que chacun d'eux ne peut avoir qu'une seule signification; parce que ce ne sont que des conventions *pures & simples*, qui ne sont susceptibles de fournir aucune espèce de combinaison.

Prendre dans l'Alphabet même de l'Idiôme dans lequel on veut être lu (1), des lettres

(1) Plusieurs *Cryptographes* substituent des caractères

une fois convenues : voilà encore la convention *pure & simple* dont on vient de parler, & rien de plus : telle étoit la manière d'écrire en chiffres de Jules-César (1) & de César-Auguste. En effet, ces Empereurs écrivoient, l'un *D*, pour *A*, &c. & l'autre *B*, pour *A*, &c. Il résulte de là, que l'un & l'autre n'avoient également que vingt-quatre clefs, ou vingt-quatre manières *de rechange*. Ainsi, *D* représentoit toujours *A*, & *B* représentoit toujours *A*, &c.

Le Cardinal de Richelieu avoit aussi son chiffre ; mais ce chiffre est embarrassant, compliqué, & toujours également lent, quoiqu'il soit plus proche qu'aucun autre du point de perfection d'une *Cryptographie*. — Ce chiffre est trop connu pour en donner un exemple.

Après avoir défini le mot *Cryptographie*,

tères étrangers aux caractères de l'idiôme dans lequel ils écrivent ; il ne faut alors, pour déchiffrer, qu'un peu plus d'étude.

(1) Voyez *Suétone*, à la Vie de chacun de ces Empereurs.

& avoir cité les chiffres les plus abstraits, voyons si la *Cryptographie*, dont nous allons parler, a toutes les qualités qu'il faut pour être parfaite : examinons si son principe est simple & immuable, sa marche conséquente & invariable, son opération facile & rapide, & sur-tout *indéchiffrable*.

Cette nouvelle *Cryptographie* a cela d'avantageux ; c'est qu'après en avoir communiqué notre méthode à deux personnes, nous ne pouvons rien déchiffrer de ce qu'elles se feront confiées l'une à l'autre, d'après cette même méthode.

Après cette méthode, & les deux exemples *Cryptographiques* que nous donnons ici, nous démontrerons les combinaisons qui en résultent, & qui en prouvent l'*indéchiffrabilité* ; quant à la marche de ce nouveau chiffre, il demande de l'habitude & la connoissance de la clef dont on se sert ; quant à la quantité de clefs qu'elle fournit, il nous suffit de dire qu'elle passe de beaucoup 999,999 millions (1).

(1) L'on peut avancer que le nombre surpasse 1, suivi de 24 zéros.

Ces clefs ne tiennent pas grande place (1); celles que deux Correspondans se donnent diffèrent encore entr'elles, en ce que chacun des deux Correspondans n'a que l'inverse de l'Alphabet de l'autre, comme on peut le voir ci-après.

Il n'y a que les numéros de l'Alphabet & les numéros dits puissance inconnue, qui ne peuvent varier entre les deux Correspondans. Cependant, avant de donner la méthode, l'on nous permettra d'insister sur ce que nous avons dit plus haut sur l'*indéchiffabilité*, & d'avancer que lorsqu'un Ministre croit pouvoir soupçonner un Correspondant d'infidélité, dès l'instant il en envoie un autre, chargé d'une nouvelle clef; alors, le Ministre n'a pas à craindre que l'ancien Correspondant puisse traduire une lettre chiffre, qu'il auroit pu surprendre à ce nouveau Correspondant.

Passons à la *Méthode Cryptographique*.

(1) Les Tableaux qui suivent prouvent notre assertion.





M É T H O D E

CRYPTOGRAPHIQUE.

L'OPÉRATION dont il est question ici, est détaillée dans la Méthode, & il ne faut savoir compter que jusqu'à quarante-neuf.

La *Cryptographie* dont on va parler, est aussi simple dans sa marche que dans son principe, & n'a pas besoin d'un grand calcul (comme nous l'avons dit plus haut) pour être mise en œuvre; quoique réellement elle fournisse des combinaisons presque innombrables, puisque chaque lettre seule peut être représentée par les vingt-quatre autres, qui, chacune en particulier, peut être représentée par celle-là seule; car *A* peut être représenté par *B*, ou *C* ou *D*, &c. de même que *B*, ou *C* ou *D*, peuvent être représentées par *A*; comme il est aisé de le voir dans les morceaux *Crypto-*

graphiques ci-joints (1). Venons à la méthode : Mon Correspondant d'Amsterdam devant partir pour cette Ville, je lui donne l'Alphabet François non point tel qu'il est dans les Dictionnaires, mais tel que le hasard l'a fourni, ou à la volonté des deux Correspondans. Je suppose que mon Correspondant ait l'Alphabet numéroté 2 ci-joint, moi je me réserve l'Alphabet numéroté 1, qui n'est différent du n^o 2, que par l'inversion des lettres; cependant, les deux Alphabets se déchiffrent réciproquement, à l'aide d'un certain nombre de chiffres rangés au hasard ou à notre volonté; ces nombres, je les ai nommés puissance inconnue, & c'est sur cette puissance inconnue qu'est fondée l'*indéchiffrabilité* du chiffre : or, comme les vingt-quatre nombres peuvent se

(1) L'on peut examiner, à la fin de cet Essai, la forme ou figure que doit avoir une clef de cette *Cryptographie*, ainsi que les chiffres ou correspondances de deux personnes qui s'écrivent la même lettre, sans pouvoir se servir réciproquement des mêmes signes, quoique l'un & l'autre puissent se déchiffrer.

combiner d'une infinité de manières différentes, celui qui pourroit surprendre un chiffre écrit d'après cette méthode, a-t il les moyens de découvrir cet agent ou puissance inconnue à lui ; puissance qui détermine la valeur de chaque lettre-chiffre ; puisque, comme il est dit plus haut, que *A* peut être un *B* ou un *C*, & même représenter *B* & *C* dans le même mot. Le Tableau numéroté 1, a composé le chiffre (1) numéroté 1, & l'Alphabet numéroté 2 doit le déchiffrer, comme le chiffre numéroté 2, & composé d'après le Tableau numéroté 2, est décomposé par le Tableau numéroté 1. Or, mon chiffre étant arrivé à sa destination, le Correspondant arme ce chiffre de sa puissance, qui commence par 24 & finit par 11, & ensuite recommence par 24, comme on peut le voir ; d'après ces détails, on peut consulter le morceau *Cryptographique*, numéroté 1, que mon Correspondant d'Amsterdam doit déchiffrer. Suivons-le dans sa marche : le chiffre qu'il reçoit commence par

(1) Voyez les dixième & onzième pages de cette Méthode.

h, d, o, f, e, p, k, m, f, f, e, b,
 24, 7, 5, 21, 10, 2, 14, 9, 3, 13, 18, 6,
g, i, v, v, i, i, f, f, p, q, y,
 4, 22, 12, 19, 1, 16, 15, 23, 17, 20, 8,
h, a, q, z. Dès-lors, mon Correspondant
 11, 24, 7, 5.

appliquant sous chaque lettre-chiffre, ces nombres, dits puissance inconnue, & qui n'est connue que de nous deux seuls, puisqu'elle peut être variée à chaque Correspondant nouveau que je veux employer; variation qui peut monter à plus de 999,999, comme on peut le voir par les numéros ci-dessus. Mon Correspondant ayant ainsi numéroté ses lettres-chiffres, prend le Tableau numéroté 2, & qui est celui que je lui ai donné à son départ. Mon Correspondant connoissant l'arrangement de son Alphabet, n'a pas besoin de grande peine ni de grands calculs pour retrouver dans cet Alphabet les vrais caractères des phrases que je lui ai envoyées en caractères-chiffres; & voici la manière dont mon Correspondant fait son opération. Il dit en prenant son Tableau: La lettre *H*, dans mon Tableau, est numérotée 20, & par sa puissance elle dit 24, qui, plus,

20 de son Tableau vaut 44; mais à 44 dans le Tableau, c'est un *C* qu'il trouve : donc c'est un *C* qui devient vrai caractère; passant à la seconde lettre-chiffre *D*, qui a pour puissance 7; & dans le Tableau *D* est numéroté 17 : or, 7, plus 17, égalent 24, & 24 me donne un *R*, & toujours en continuant, mon Correspondant dit *O*, ou 5 de puissance; plus, 8 de l'Alphabet égalent 13, ou *Y*, *S*, ou 21 de puissance; plus, 10 de l'Alphabet égalent 31, ou *P*, *E*, ou 10 de puissance; plus, 2 de l'Alphabet égalent 12, ou *T*, *P*, ou 2 de puissance; plus, 6 de l'Alphabet égalent 8, ou *O*, ou 14 de puissance; plus, 9 de l'Alphabet égalent 23, ou *G*. *M*, ou 9 de puissance, plus, 15 de l'Alphabet égalent 24, ou *R*. *F*, ou 3 de puissance; plus, 18 de l'Alphabet égalent 21, ou *A*. *F*, ou 13 de puissance; plus, 18 de l'Alphabet égalent 31, ou *P*. *E*, ou 18 de puissance; plus, 2 de l'Alphabet égalent 20, ou *H*. *B*, ou 6 de puissance; plus, 5 de l'Alphabet égalent 11, ou *J*. *G*, ou 4 de puissance; plus, 23 de l'Alphabet égalent 27, ou *E*. Voilà donc mon Correspondant parvenu à déchiffrer ce que je lui ai écrit en chif-

fres : mais supposé qu'il doive m'écrire le même mot François *Cryptographie*, il ne peut, avec son Alphabet numéroté 2, me chiffrer ce mot comme je le lui ai chiffré : or, il arme le mot François *C r y p t o g r a p h i e*,
 24; 7; 5; 21; 10; 2; 14; 9; 3; 13; 18; 6; 4;
 comme il a fait du mot-chiffre, dont il a voulu connoître le François; & il dit, comme on a pu le remarquer à la page numérotée 20 de cette Méthode, *C* ou 24 de sa puissance; plus, 19 de l'Alphabet égalent 43, ou *F. R*, ou 7 de sa puissance; plus, 24 de l'Alphabet égalent 31, ou *P. Y*, ou 5 de sa puissance; plus, 13 de l'Alphabet égalent 18, ou *F. P*, ou 21 de sa puissance; plus, 6 de l'Alphabet égalent 27, ou *E. T*, ou 10 de sa puissance; plus, 12 de l'Alphabet égalent 22, ou *Z. O*, ou 2 de sa puissance; plus, 8 de l'Alphabet égalent 10, ou *S. G*, ou 14 de sa puissance; plus, 23 de l'Alphabet égalent 37, ou *T. R*, ou 9 de sa puissance; plus, 24 de l'Alphabet égalent 33, ou *O. A*, ou 3 de sa puissance; plus, 21 de l'Alphabet égalent 24, ou *R. P*, ou 13 de sa puissance; plus, 6 de l'Alphabet égalent 19, ou *C. H*, ou 18 de sa puissance;

plus, 20 de l'Alphabet égalent 38, ou *Y. S*,
ou 6 de sa puissance; plus, 11 de l'Alphabet
égalent 17, ou *D. E*, ou 4 de sa puissance;
plus, 2 de l'Alphabet égalent 6, ou *P*.



Ces exemples suffisent pour le reste de la
Cryptographie.

ALPHABET numéroté I.

26,	27,	28,	29,	30,
<i>n</i>	<i>r</i>	<i>g</i>	<i>z</i>	<i>a</i>
<u>1,</u>	<u>2,</u>	<u>3,</u>	<u>4,</u>	<u>5,</u>
31,	32,	33,	34,	35,
<i>h</i>	<i>c</i>	<i>f</i>	<i>d</i>	<i>v</i>
<u>6,</u>	<u>7,</u>	<u>8,</u>	<u>9,</u>	<u>10,</u>
36,	37,	38,	39,	40,
<i>m</i>	<i>x</i>	<i>y</i>	<i>t</i>	<i>i</i>
<u>11,</u>	<u>12,</u>	<u>13,</u>	<u>14,</u>	<u>15,</u>
41,	42,	43,	44,	45,
<i>f</i>	<i>k</i>	<i>o</i>	<i>l</i>	<i>p</i>
<u>16,</u>	<u>17,</u>	<u>18,</u>	<u>19,</u>	<u>20,</u>
46,	47,	48,	49,	
<i>b</i>	<i>q</i>	<i>u</i>	<i>e</i>	<i>j</i>
<u>21,</u>	<u>22,</u>	<u>23,</u>	<u>24,</u>	<u>25.</u>

Puissance inconnue, n^o. I.

24, 7, 5, 21, 10, 2, 14, 9, 3, 13, 18, 6,
4, 22, 12, 19, 1, 16, 15, 23, 17, 20, 8, 11.

ALPHABET

ALPHABET numéroté II.

26,	27,	28,	29,	30,
<i>j</i>	<i>e</i>	<i>u</i>	<i>q</i>	<i>b</i>
<u>1,</u>	<u>2,</u>	<u>3,</u>	<u>4,</u>	<u>5,</u>
31,	32,	33,	34,	35,
<i>p</i>	<i>l</i>	<i>o</i>	<i>k</i>	<i>f</i>
<u>6,</u>	<u>7,</u>	<u>8,</u>	<u>9,</u>	<u>10,</u>
36,	37,	38,	39,	40,
<i>i</i>	<i>t</i>	<i>y</i>	<i>x</i>	<i>m</i>
<u>11,</u>	<u>12,</u>	<u>13,</u>	<u>14,</u>	<u>15,</u>
41,	42,	43,	44,	45,
<i>v</i>	<i>d</i>	<i>f</i>	<i>c</i>	<i>h</i>
<u>16,</u>	<u>17,</u>	<u>18,</u>	<u>19,</u>	<u>20,</u>
46,	47,	48,	49,	
<i>a</i>	<i>z</i>	<i>g</i>	<i>r</i>	<i>n</i>
<u>21,</u>	<u>22,</u>	<u>23,</u>	<u>24,</u>	<u>25.</u>

Puissance inconnue, n°. II.

24, 7, 5, 21, 10, 2, 14, 9, 3, 13, 18, 6,
4, 22, 12, 19, 1, 16, 15, 23, 17, 20, 8, 11,

B

Démontrons maintenant les résultats que donne cette manière de poser l'Alphabet, & l'impossibilité de pouvoir déchiffrer une écriture composée d'après notre Méthode; nous nous contenterons de donner au Lecteur curieux, les moyens de trouver ce que cette Méthode fournit de clefs, & nous allons mettre ensuite le Tableau de progression jusqu'au nombre 6.

Pour savoir, Lecteur, combien de clefs cette Méthode fournit, multipliez d'abord

2 par 1, & vous aurez deux.

3 par 2, & vous aurez six.

4 par 6, qui donne vingt-quatre.

5 par 24, qui donne cent vingt.

6 par 120, qui donne sept cents vingt, ainsi de suite, jusqu'au nombre 25.



PROGRESSION de la quantité de manières dont chaque mot d'une lettre, de deux lettres, de trois lettres, de quatre lettres, de cinq lettres, de six lettres, &c. peuvent être rendus.

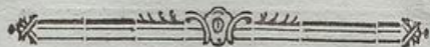
Une lettre seule par les autres	24.
Un mot de 2, par	552.
Un de 3, par	12,144.
— de 4, par	255,024.
— de 5, par	5,100,480.
— de 6, par	96,909,120.

Ces nombres suffisent pour prouver l'abondance de cette *Cryptographie*.



B 2





EXPLICATION

DÉMONSTRATIVE

DE

CETTE PROGRESSION.

C E Tableau progressif va jusqu'à presque l'innombrabilité (1); mais pour nous mieux faire entendre, nous nommerons *Extraits*, la quantité de manières dont une lettre peut être rendue, & disons qu'il y en a vingt-quatre, puisqu'il ne peut s'en trouver vingt-cinq; parce que la vraie lettre est toujours absente dans le chiffre; puisque sans cela, il arriveroit

(1) Nous rajoutons ici la quantité de manières dont un mot de sept lettres peut être représenté,
 1, 744, 364, 160,

qu'un caractère naturel étant représenté par sa propre figure, c'est-à-dire par lui-même; dès-lors, il cesseroit d'être *Cryptographique*. *Les Ambes*, ce sont des mots de deux lettres; *les Ternes*, ceux de trois : or, voici le détail de cette opération numérique.

On sent qu'ici les Extraits sont toujours déterminés, puisqu'ils ne peuvent ne pas l'être; ainsi, une lettre de l'Alphabet François, qui en contient vingt-cinq, peut toujours avoir vingt-quatre figures représentatives d'elle-même, de même qu'à son tour, elle peut toujours aussi représenter chacune de ces vingt-quatre figures : donc vingt-quatre Extraits, c'est-à-dire vingt-quatre manières de représenter une seule lettre.

Les Ambes, *les Ternes*, &c. sont également ici toujours déterminés; ce qui fournit d'autant plus de combinaisons, par rapport aux *Ambes* : il est très-clair que (1 & 2) (2 & 1), ne forment qu'un *Ambe simple*, mais bien deux *Ambes déterminés*; mais comme il s'agit ici de lettres qu'il n'y a pas de transposition qui n'en détermine nécessairement l'assemblage, & que cet assemblage est lui-même déterminé,

dans les lettres naturelles qui forment le mot ; ces lettres, soit *naturelles* soit *représentatives*, sont donc toujours nécessairement déterminées. En effet, supposons, quant aux *lettres naturelles*, cette syllabe, *ab*, elle est absolument déterminée ; puisqu'en transposant les deux lettres qui la composent, on n'auroit plus *ab*, mais *ba* : voilà donc pour ces deux lettres *a* & *b*, ou *b* & *a*, bien évidemment deux *Ambes déterminés* ; puisque *ab*, n'est *ba*.

Il faut dire la même chose des *Ternes*, avec cette différence, qu'un *Terne simple*, ou ici mot de trois lettres, fournit six *Ambes déterminés*, ainsi qu'il suit.

Supposons, par exemple, ce *Terne simple*,

a, b, c.

1^{er} *Terne déterminé*, *A, B, C.*

2^{me} ————— *B, C, A.*

3^{me} ————— *C, A, B.*

4^{me} ————— *C, B, A.*

5^{me} ————— *B, A, C.*

6^{me} ————— *A, C, B.*

Voilà bien évidemment six *Ternes déterminés* pour un *Terne simple* ; c'est-à-dire, ici, un composé de trois lettres.

Il en est ainsi des *Quaternes*, *Quines*, &c. en suivant la progression, qui mène à des nombres considérables ; c'est-à-dire, qui égalent la quantité des transpositions dont le composé de lettres est susceptible.

Nous mettrons ici les deux chiffres réciproques que peuvent s'envoyer les Correspondans, tant celui de Paris que celui d'Amsterdam ; ils s'écriront les mêmes phrases, & cependant ces chiffres n'auront aucune ressemblance, comme on peut le voir ci-après.

C H I F F R E , N^o. I.

Hdofepkmffebg iv vüfspqyhaqz xjaiemgk
 zyerfekt qo rnciepm px fz pufdznogih,
 Cfuñnihb gghbt Cfpobtek Ktxlzfsys fgljl lvo
 Kirolvly, eaepn dyjfi rmay gkjafes mcakf
 Ttm my tfglcny Berc hfo Zuoyquqmezms
 qñfuineihxbs.

C H I F F R E , N^o. II.

Epfezftorcydp bm Qyfmpmcqdeff Panxharh
ogagppqmd nd xuqdnzgh fd in lxbnvransn
mefizkkm mfgoby hqfvrimi gdsqefa lfrdxvc
Rrfvm jma Kdtgecjj nftgh avcrt fegl zjuugge
bsfn Zqz cv nrrfppl qmjj npd Tebifyafgnob
Bqtibemyecje.

Nec plus ultra.

F I N.



