La Revue de la BNU

13 | 2016
Varia 13

Strasbourg, témoin de l'évolution de la cryptologie du 16e au 17e siècle

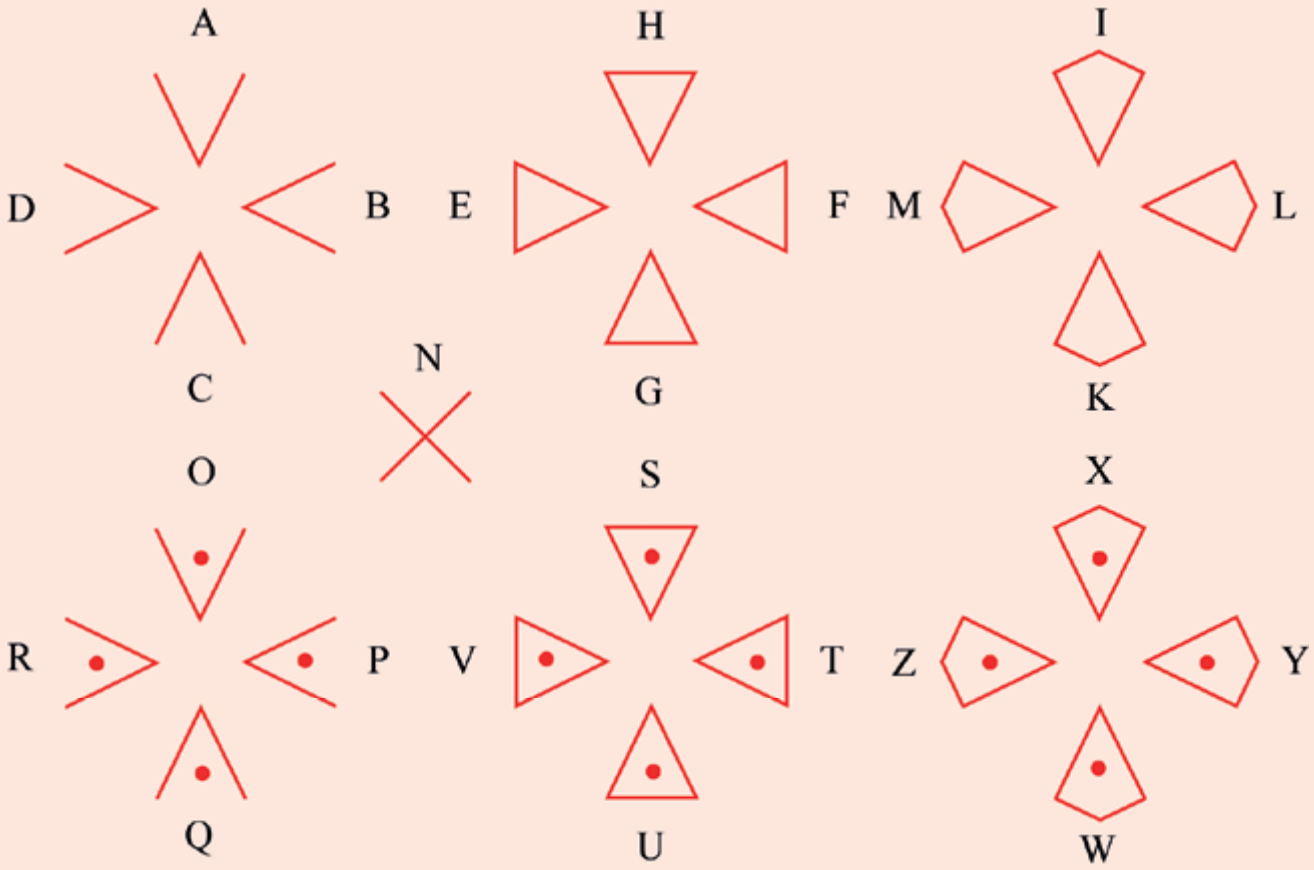
Hervé Lehning

Édition électronique
URL : http://journals.openedition.org/rbnu/1501
DOI : 10.4000/rbnu.1501
ISSN : 2679-6104

Éditeur
Bibliothèque nationale et universitaire de Strasbourg

Édition imprimée
Date de publication : 1 mai 2016
Pagination : 46-57
ISBN : 9782859230623
ISSN : 2109-2761

Référence électronique
Hervé Lehning, « Strasbourg, témoin de l'évolution de la cryptologie du 16e au 17e siècle », *La Revue de la BNU* [En ligne], 13 | 2016, mis en ligne le 01 mars 2020, consulté le 11 décembre 2020. URL : http://journals.openedition.org/rbnu/1501 ; DOI : https://doi.org/10.4000/rbnu.1501



Le chiffre des Templiers avait l'avantage d'être facile à retenir car fondé sur leur croix.
Ici, les symboles en rouge doivent être substitués aux lettres en noir.

STRASBOURG, TÉMOIN DE L'ÉVOLUTION DE LA CRYPTOLOGIE DU 16E AU 17E SIÈCLE

Les Archives municipales de Strasbourg contiennent une belle collection de lettres chiffrées et de tables de chiffrement, de la Renaissance au règne de Louis XIV. Pour la plupart, ces documents correspondent à des relations diplomatiques, ce qui est naturel puisque la diplomatie est l'un des champs d'application traditionnels de la cryptographie. Pour l'historien de cette discipline, le grand intérêt de cette collection est qu'elle couvre une époque charnière, où les méthodes de chiffrements héritées de l'Antiquité et du Moyen Âge, affaiblies par les découvertes des cryptanalystes, ont été remplacées par de nouvelles qui ont duré ensuite jusqu'à la guerre de 1870 – voire jusqu'à la Première Guerre mondiale pour les relations diplomatiques. Dans cet article, nous nous proposons de situer ces chiffres dans l'histoire de la cryptologie avant de les analyser[1]. Comme tous ceux de l'époque, ils appartiennent à la famille des chiffres par substitution. Nous nous y limiterons donc, en écartant autant les méthodes stéganographiques, qui consistent à cacher le message et non son sens, que les méthodes par transposition, comme la scytale de Sparte qui consiste à changer l'ordre des lettres d'un texte, à les mélanger en quelque sorte, c'est-à-dire à fabriquer des anagrammes. Nous ne parlerons pas non plus des méthodes conçues à l'époque étudiée mais dont il n'existe aucune preuve de l'utilisation effective, comme les méthodes de substitution poly-alphabétique (cadran d'Alberti, chiffre de Vigenère[2], boîte à chiffrer d'Henri II[3]).

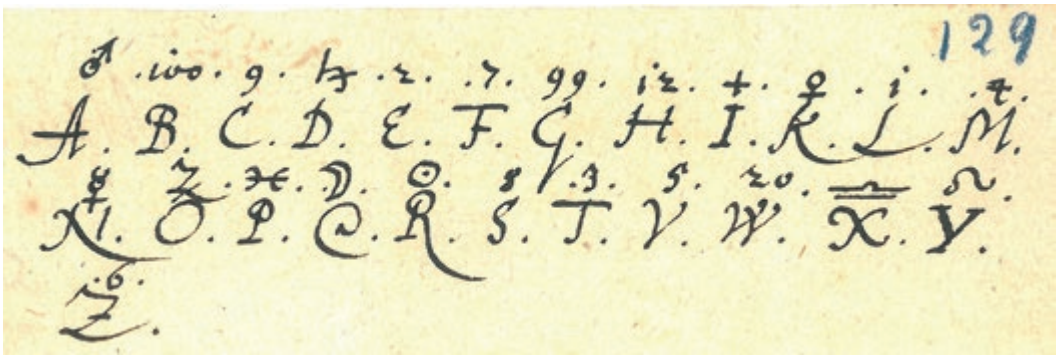
Quelques rappels sur la cryptologie, de l'Antiquité à l'âge classique

L'histoire de la cryptologie est celle d'une lutte entre chiffreurs, qui cherchent à cacher des messages, et décrypteurs qui, sans savoir a priori comment ils ont été chiffrés, cherchent à en découvrir le sens. Le premier chiffre par substitution connu est attribué à Jules César et décrit par Suétone[4] :

« César [...] employait, pour les choses tout à fait secrètes, une espèce de chiffre qui en rendait le sens inintelligible (les lettres étant disposées de manière à ne pouvoir jamais former un mot) et qui consistait, je le dis pour ceux qui voudront les déchiffrer, à changer le rang des lettres dans l'alphabet, en écrivant la quatrième pour la première, c'est-à-dire le D pour l'A, et ainsi de suite ».

Ainsi, « la revue de la BNU » se chiffre en « od uhyxh gh od eqx ». Bien sûr, on peut changer l'amplitude du décalage mais le nombre de chiffrements possibles reste limité à 25, ce qui rend le décryptement facile dès lors qu'on connaît la méthode. Les Templiers, et bien d'autres avant eux, eurent l'idée de substituer un symbole différent à chaque lettre de l'alphabet (voir ill. ci-contre). De cette façon, « la revue de la BNU » se chiffre en : « ◁V ≻▷▷◬▷ ≻▷ ◁V <X◬ ». Bien avant que les Templiers n'inventent ce chiffre, un savant arabe, Abu Yusuf al-Kindi (801–873), avait trouvé une méthode pour décrypter les chiffres par substitution alphabétique, ce qu'il expose très clairement[5] :

« Une façon d'élucider un message chiffré, si nous savons dans quelle langue il est écrit, est de nous procurer un autre texte clair dans la même langue, de la longueur d'un feuillet environ, et de compter alors les apparitions de chaque lettre. Nous appellerons la lettre apparaissant le plus souvent la « première », la suivante la « deuxième », et ainsi de suite pour chaque lettre figurant dans le texte. Ensuite, nous nous reportons au texte chiffré que nous voulons éclaircir et nous relevons de même les symboles. Nous remplaçons le symbole le plus fréquent par la lettre « première » du texte clair, le suivant par la lettre « deuxième », le suivant par la



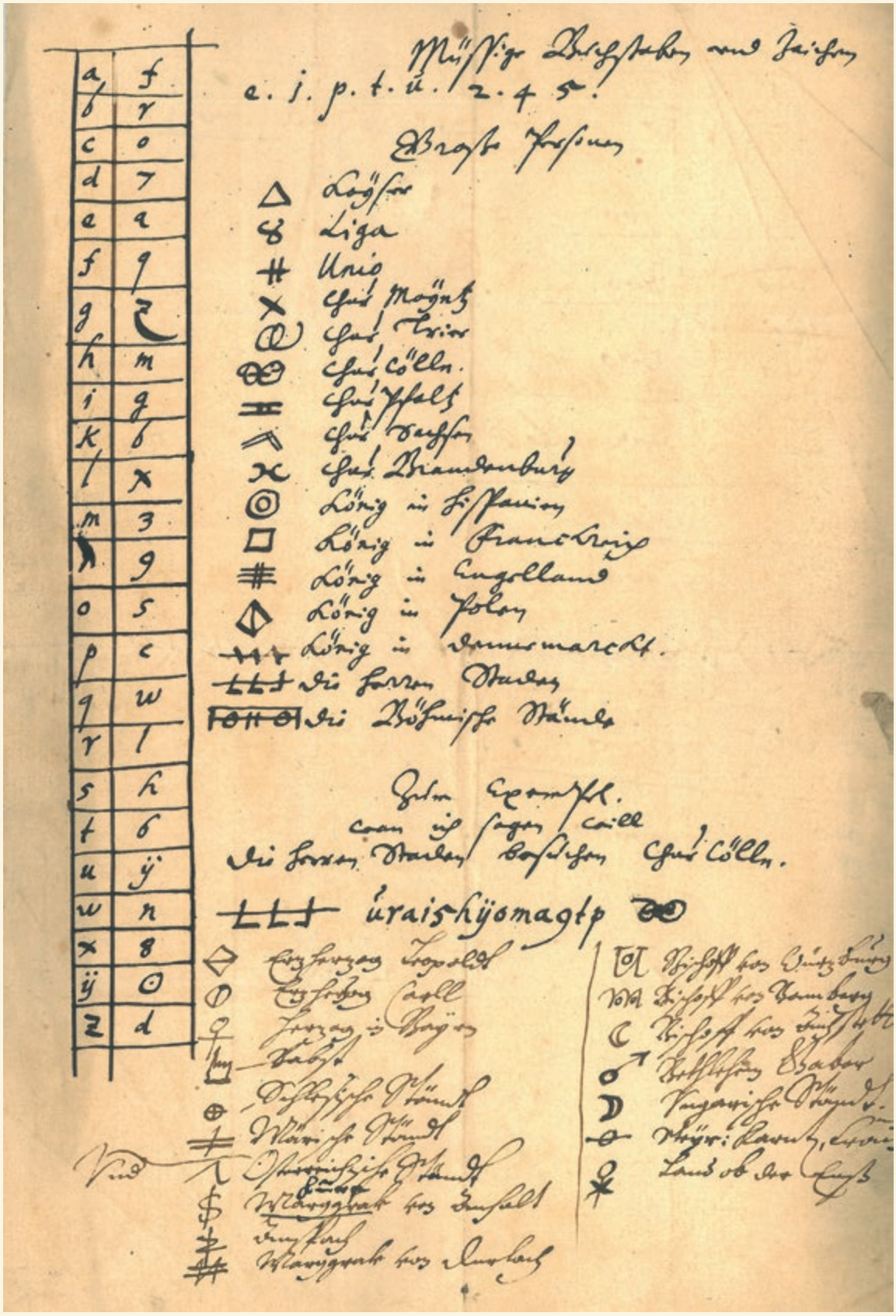
Alphabet chiffré utilisé en 1627 par un délégué de Strasbourg. De façon classique, I et J d'une part, U et V de l'autre sont confondus. Le fait que V et W soient distincts laisse penser que cet alphabet servait plutôt à chiffrer des textes écrits en allemand (coll. Archives municipales de Strasbourg).

« troisième », et ainsi de suite jusqu'à ce que nous soyons venus à bout de tous les symboles du cryptogramme à résoudre ».

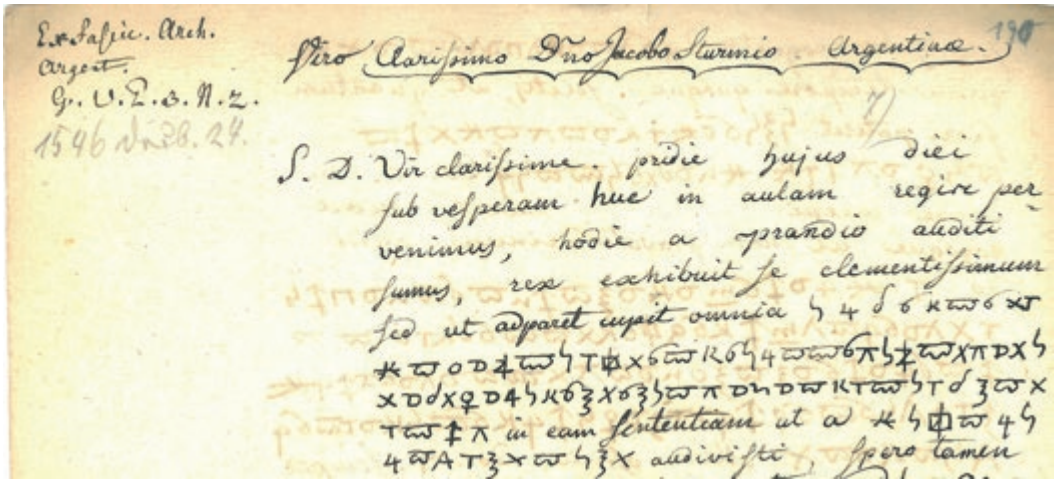
La méthode d'al-Kindi, dite méthode des fréquences, donnait l'avantage aux décrypteurs, même si elle ne fonctionnait que sur des messages très longs. Les chiffreurs trouvèrent alors une parade : multiplier les substitutions possibles pour chaque lettre et ajouter des nulles, c'est-à-dire des symboles ne signifiant rien afin de brouiller les fréquences.

Un scientifique italien de la Renaissance, Giambattista della Porta (1535–1615), le père de la cryptographie selon certains, inventa une méthode générale qui cassait ces nouveaux chiffres, dits à substitution homophonique. Elle consiste à chercher un mot dont la présence dans le message est probable. Il en existe presque toujours, par exemple les noms propres qui doivent être épelés. Prenons l'exemple d'un message chiffré par une substitution alphabétique simple, où nous pensons qu'il doit être question du prince électeur de Cologne, pour rester dans le contexte des messages de Strasbourg. La méthode des fréquences d'al-Kindi permet de trouver le représentant de la lettre la plus fréquente, qui est « e » en français. Admettons qu'ici nous trouvions le symbole « 1 ». Nous examinons le message jusqu'à trouver une occurrence possible, comme par exemple « ε1 β3δ9α1 1ε1α21μ3 γ1 απεπ891 ». En effet, ce texte chiffré a les mêmes répétitions que le texte clair « le prince électeur de Cologne » et les mêmes occurrences pour le symbole « 1 » d'un côté et la lettre « e » de l'autre. Bien sûr, rien de certain dans cette hypothèse. Elle doit être confrontée à la réalité en reportant les équivalences trouvées dans le texte (ε signifie l, 1, e, β, p, etc.). Si l'on voit apparaître alors des mots ou des phrases ayant un sens, elle est probablement juste. C'est ainsi que les décrypteurs de l'époque opéraient. Pour contrer cette méthode, les chiffreurs se mirent à ne plus respecter le découpage des mots et à traiter certains noms propres ou même certains mots de façon particulière. La première méthode consiste à dresser une liste de mots à traduire par des symboles uniques (on parle alors de nomenclateurs). La seconde consiste à camoufler les noms propres en les remplaçant par d'autres. Par exemple, on peut convenir de remplacer « le prince électeur de Cologne » par « Gustave ». Nous obtenons ainsi les chiffres classiques de la Renaissance qui furent utilisés par des rois de France comme Henri II (1519–1559) ou par Marie Stuart (1542–1587), qui fut élevée à sa cour et dont les messages chiffrés (au moyen d'un chiffre pourtant digne de ceux des rois de l'époque) furent décryptés par les services d'Elisabeth I[ère], ce qui conduisit à sa condamnation et à sa mort.

Les chiffres employés étaient de ce type, voire plus faibles quand, en 1626, Henri II de Bourbon, prince de Condé, mit le siège devant Réalmont, une place forte protestante. Ses troupes interceptèrent un homme muni d'un message chiffré sortant de la ville. On fit venir Antoine Rossignol (1600–1682), un jeune mathématicien, connu dans la région pour son talent de décrypteur. Le message ne lui résista pas. Il expliquait que la ville était à court de munitions et en réclamait. Condé renvoya le message décrypté à Réalmont[6], qui se rendit. Rossignol réitéra son exploit au siège de La Rochelle l'année suivante, si bien que le cardinal de Richelieu le prit à son service. Cet excellent cryptanalyste modifia ensuite profondément la cryptographie de son époque en transformant les vieilles tables de chiffrement en dictionnaires chiffrés, c'est-à-dire en dictionnaires bilingues dont l'une des langues est le français et la seconde, des nombres. Ainsi, on chiffre non seulement des lettres (et de plusieurs manières), comme auparavant, mais aussi des syllabes et des mots. La méthode des fréquences n'a alors plus aucun sens



Cette table de chiffrement, datée de 1619–1620, contient un alphabet chiffré (à gauche), des nulles (en haut), un nomenclateur (à droite) et un exemple (au milieu). Le tout est écrit en allemand (coll. Archives municipales de Strasbourg).



Le début de la partie chiffrée se décrypte en « secreto magister opter cesarem », en tenant compte du tableau et des nulles trouvées. Des camouflages de noms propres peuvent rendre le texte inintelligible malgré tout (coll. Archives municipales de Strasbourg).

et celle du mot probable devient difficile à utiliser, surtout si les chiffres ne correspondent pas à l'ordre alphabétique. Rossignol et ses descendants (fils et petit-fils) mirent au point le Grand Chiffre de Louis XIV, dont le décryptement attendit Étienne Bazeries (1846–1931). Pour le casser, Bazeries utilisa la méthode du mot probable en remarquant la série 124 22 125 46 345 et en émettant l'hypothèse qu'elle signifiait les–en–ne–mi–s, « les ennemis ». En la supposant juste, le code s'écroula progressivement et Bazeries le décrypta pratiquement entièrement. Un chiffrement du type du Grand Chiffre de Louis XIV était encore en usage dans l'armée française lors de la guerre de 1870, et dans la diplomatie allemande pendant la Première Guerre mondiale. En particulier, le fameux télégramme Zimmermann dont le décryptement par les Britanniques en 1917 provoqua l'entrée en guerre des États-Unis, en révélant les intentions allemandes, était chiffré avec un code de ce type.

Les chiffres par substitution alphabétique simple dans les Archives municipales de Strasbourg

Ce petit tour d'horizon des chiffres utilisés à l'époque nous permet de revenir sur ceux contenus dans les archives de Strasbourg. On y trouve plusieurs chiffres par substitution alphabétique simple, où chaque lettre est chiffrée par un seul et même symbole. Étrangement, ce ne sont pas les plus anciens car le plus parfait exemple est contemporain de la prise de Réalmont. Il servait au délégué de Strasbourg à l'assemblée des électeurs de Mülhausen en Thuringe en 1627 (voir ill. p. 48). On retrouve le même type de chiffre dans une lettre de la correspondance du secrétaire de Strasbourg avec les agents de la ville à Paris, lettre dont les parties chiffrées sont déchiffrées[7], ce qui permet de reconstituer la table de chiffrement. L'originalité de ce chiffre est de ne pas utiliser de symboles étranges, mais des digrammes. La lettre est datée de 1642 et prouve qu'à l'époque, certains concepteurs de chiffres s'étaient rendu compte que l'utilisation de symboles ésotériques ne servait à rien, ce qui préfigurait le passage au chiffrement à l'aide de nombres. Le chiffre qui nous occupe est d'ailleurs accompagné d'un nomenclateur fonctionnant également avec des couples de chiffres. On trouve ainsi 25 et 39 désignant des personnages de la Cour, semble-t-il, dont Noyers (pour 25). Le tableau qui suit montre la reconstitution de la table de chiffrement d'une correspondance déchiffrée ; chaque lettre doit se chiffrer par le digramme situé en dessous.

Clair	*a*	*b*	*c*	*d*	*e*	*f*	*g*	*i*	*l*
Chiffré	*bo*	*ao*	*rp*	*gq*	*fs*	*es*	*lg*	*tx*	*mz*
Clair	*m*	*n*	*o*	*p*	*r*	*s*	*t*	*u*	
Chiffré	*lz*	*hw*	*ab*	*rc*	*cp*	*ef*	*ix*	*Ky*	

Avec ce chiffre, « la revue de la BNU » s'écrit « mz bo cp fs Ky Ky fs gq fs mz bo ao hw Ky ». Même si elle témoigne toujours d'un chiffre par substitution alphabétique simple, une table de chiffrement datant de 1619–1620 est particulièrement intéressante car elle introduit des nulles (e, j, p, t, u, 2, 4, 5), en plus d'un nomenclateur

Le chiffre de l'affaire Hénot, daté de 1627 : substitution alphabétique simple avec chiffrement de digrammes et nomenclateur (coll. Archives municipales de Strasbourg).

pour des personnes importantes comme des princes électeurs, des évêques et des rois. Enfin, cette table contient un exemple, « urai5hyomagtp » qui, une fois les nulles supprimées, devient « rahyomag » qui se déchiffre en « besuchen » (voir ill. p. 49).

Un exemple de décryptement d'une lettre chiffrée par substitution alphabétique simple

Les documents décrits dans les Archives municipales de Strasbourg comme : « relations avec la France, lettres de Jean Sturm, Jacques Sturm, Jean Sleidan (1544 – 1547) » ne contiennent pas de table de chiffrement, mais sont partiellement déchiffrés, ce qui permet de reconstituer la table. Nous remarquons quelques nulles comme ל, E et Γ ainsi que les correspondances contenues dans le tableau qui suit ; il reconstitue la table de chiffrement de la correspondance de 1544–1547[8].

Clair	*a*	*b*	*c*	*d*	*e*	*f*	*g*	*h*	*i*	*k*	*l*	*m*
Chiffré	ϖ	♀	K	λ	6	A	o	m	ʊ	ɬ	n	ϰ
Clair	*n*	*o*	*p*	*q*	*r*	*s*	*t*	*u*	*w*	*x*	*y*	*z*
Chiffré	ʒ	T	⊕	∏	ϖ	4	X	↟	↑	Q		⊡

La lettre « y » n'a jamais été utilisée, les lettres « p » et « z » sont chiffrées différemment, quoique de façon très semblable, dans les deux lettres déchiffrées. D'autre part, les textes commencent par quatre symboles qui doivent sans doute être considérés comme nuls car ils ne sont pas déchiffrés. Dans l'une des lettres, après les symboles EΓ, le texte n'a plus de sens et cesse très vite d'être déchiffré. Sauf erreur improbable de chiffrement, il pourrait s'agir d'une méthode pour rendre le calcul des fréquences inopérant. Le chiffreur aurait inséré une partie sans sens véritable, ce qui est d'autant plus vraisemblable que nous verrons plus loin des exemples de ce procédé. À partir de notre table, nous pouvons décrypter une partie des documents figurant dans le même dossier (voir ill. p. 50).

Les Archives municipales de Strasbourg contiennent d'autres chiffres du même type, avec substitution alphabétique simple et nomenclateur. L'un d'entre eux[9] prévoit de chiffrer certains digrammes courants, comme ff, ll, mm, etc., avec un seul symbole. De même, un document daté de 1627 concernant le procès en sorcellerie de Séraphin Hénot, secrétaire intime du duc Léopold d'Autriche, évêque de Strasbourg, contient un chiffre du même type (voir ill. ci-dessus), avec une graphie évoquant le chiffre des Templiers ou celui des francs-maçons (le fameux « parc à cochons » qu'ils utilisèrent jusqu'au 19e siècle)[10].

Les chiffres par substitutions alphabétiques multiples dans les Archives municipales de Strasbourg

Nous retrouvons vraisemblablement Jean Sturm dans un document figurant dans une chemise contenant par ailleurs le cycle des dates de la fête de Pâques[11], car l'entête de la première page porte la mention : *cifra, quam habet Sturmius in Gallia* (voir ill. p. 53). Ce chiffre est plus élaboré que le précédent concernant Jean Sturm puisqu'il contient un nomenclateur, des nulles mais

aussi des substitutions multiples pour chaque lettre. Il est typique de la Renaissance, et du niveau de ceux des rois de l'époque. Il serait logique qu'il soit postérieur au précédent.

Un chaînon intermédiaire

Les tables de chiffrement rencontrées jusqu'ici dans les Archives municipales de Strasbourg correspondent à des substitutions alphabétiques, éventuellement pourvues de nomenclateurs. La première table ressemblant à un dictionnaire chiffré est datée de 1636. Elle servait à la correspondance de l'électeur de Bavière avec le feld-maréchal von Goetz et le commissaire général des guerres. Il s'agit d'une sorte d'intermédiaire entre les chiffres homophones et les dictionnaires chiffrés désordonnés comme le Grand Chiffre de Louis XIV. Les chiffres n'y sont d'ailleurs pas des nombres, comme c'est le cas dans les dictionnaires chiffrés, mais des symboles suivis de nombres. C'est pourquoi nous mettons ce chiffre à part. L'avantage de cette méthode est de permettre un déchiffrement facile à l'aide de la seule table de chiffrement. L'inconvénient majeur est qu'elle garde une faiblesse importante puisque les chiffres des mots commençant par la même lettre sont ordonnés entre eux. Ainsi, si on découvre que 910 signifie *ab* et 920, *alb*, les chiffres entre 911 et 919 représentent des mots entre *ab* et *alb* dans l'ordre alphabétique. Antoine Rossignol a évité ce genre de faiblesse pour créer le Grand Chiffre de Louis XIV.

Cette faiblesse ne se retrouve pas dans le chiffre daté de la même année et qui le suit dans les archives (voir ill. p. 54 en haut)[12], où les chiffres sont désordonnés, mais elle se retrouve partiellement ou complètement dans un certain nombre de chiffres datés du règne de Louis XIV où tous les mots commençant par *a* ou *b* se trouvent chiffrés dans l'ordre par des nombres finissant par 1, de même pour les mots commençant par *da*, avec un nombre finissant par 2, etc. Ceci affaiblit l'ensemble, faiblesse que nous retrouvons dans le chiffre suivant (voir ill. p. 54 en bas)[13]. Ces chiffres sont accompagnés de listes de camouflages pour des noms propres ou communs (personnalités, lieux et matériels) ; ainsi, les *oranges* sont des *bombes* et les *citrons*, des *grenades*, *la Forêt-Noire*, *zurzach*, etc. De façon générale, les noms des villes sont échangés.

Les dictionnaires chiffrés désordonnés

Pour être véritablement solides, ces dictionnaires chiffrés doivent être désordonnés, ce qui est le cas dans la plupart des chiffres datant des années 1680 environ et qui se trouvent dans les Archives de Strasbourg, comme celui servant à la correspondance entre le marquis d'Huxelles et le marquis de Villard (voir ill. p. 55)[14].

Pour déchiffrer, on ne peut plus se contenter de lire les tables de chiffrement à l'envers – ce qui reviendrait à utiliser un dictionnaire français-allemand pour traduire un texte allemand en français : la recherche des mots serait extrêmement fastidieuse ! Pour faciliter le travail de traduction chiffres / mots, il apparaît alors des tables de déchiffrement ordonnées selon les chiffres (voir ill. p. 56-57, où par exemple on trouve rapidement que « 158 » signifie « la France »).

Conclusion

Ainsi, les chiffres détenus par les Archives municipales de Strasbourg décrivent bien l'évolution du système tel qu'il était utilisé de l'Antiquité jusqu'à la fin du 19e siècle. Au début de cette période, la substitution alphabétique simple est la seule qui soit utilisée, bien qu'elle soit attaquable par la méthode des fréquences. Elle se munit très vite de symboles nuls pour pouvoir y résister, puis d'un nomenclateur ou de méthodes de camouflage pour résister à la méthode du mot probable. Tout ceci ne suffisant pas, des substitutions alphabétiques multiples apparaissent. Comme elles restent attaquables par la méthode du mot probable, les tables de chiffrement deviennent des dictionnaires chiffrés semblables au Grand Chiffre de Louis XIV, méthode de chiffrement qui restera la principale jusqu'au milieu du 19e siècle.

Hervé Lehning

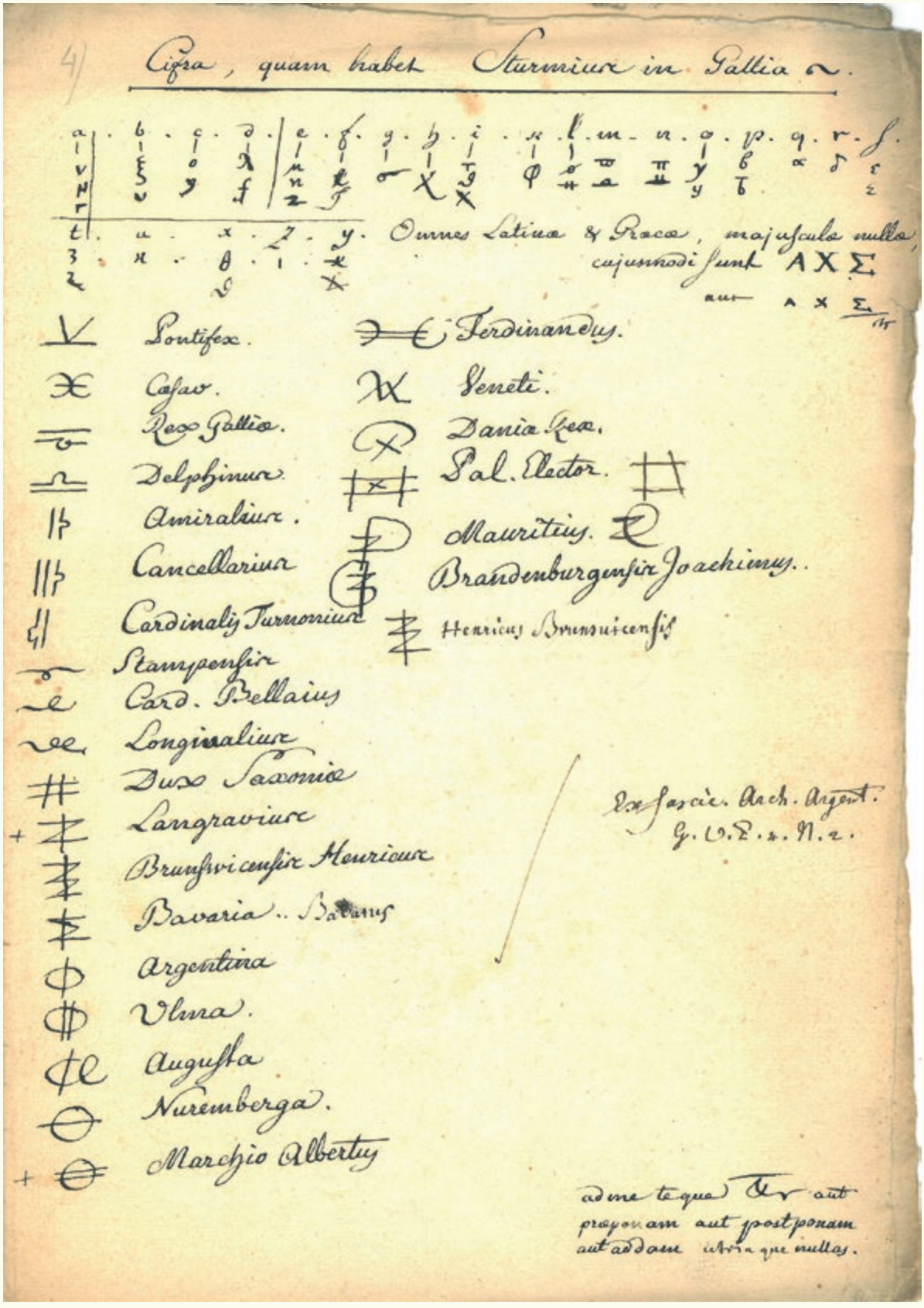
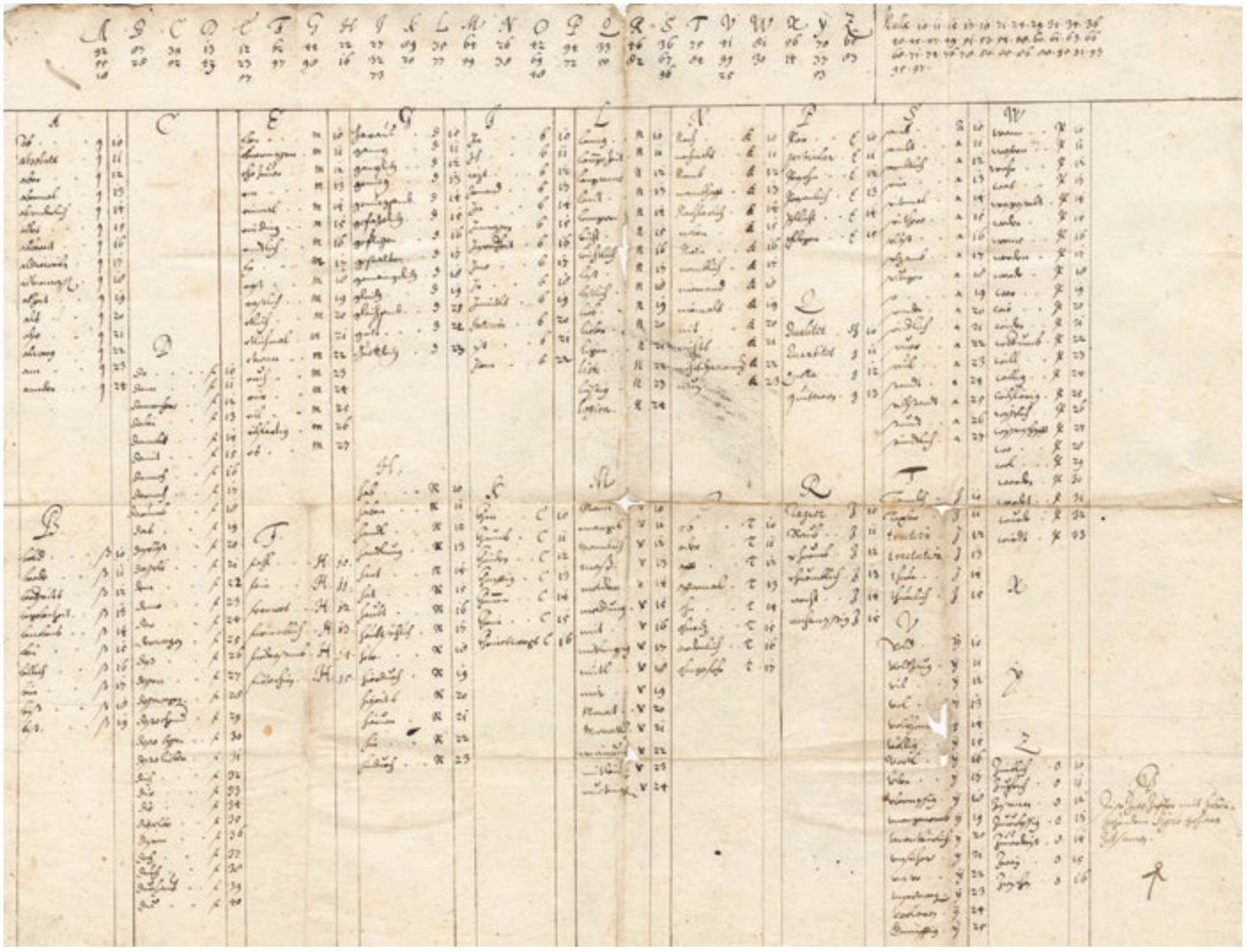
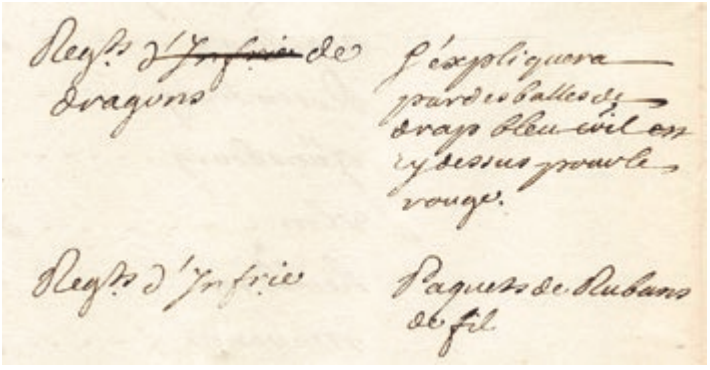


Table de chiffrement multiple avec nulles et nomenclateur, plus un symbole en bas à droite destiné à annuler une partie du texte. L'existence de ce type d'instructions explique la difficulté qu'on peut avoir à déchiffrer, même en connaissant la table (coll. Archives municipales de Strasbourg).



Proto-dictionnaire chiffré des Archives municipales de Strasbourg, daté de 1636
(coll. Archives municipales de Strasbourg).



Instruction pour donner le nombre
de régiments de dragons et d'infanterie
(coll. Archives municipales de Strasbourg).

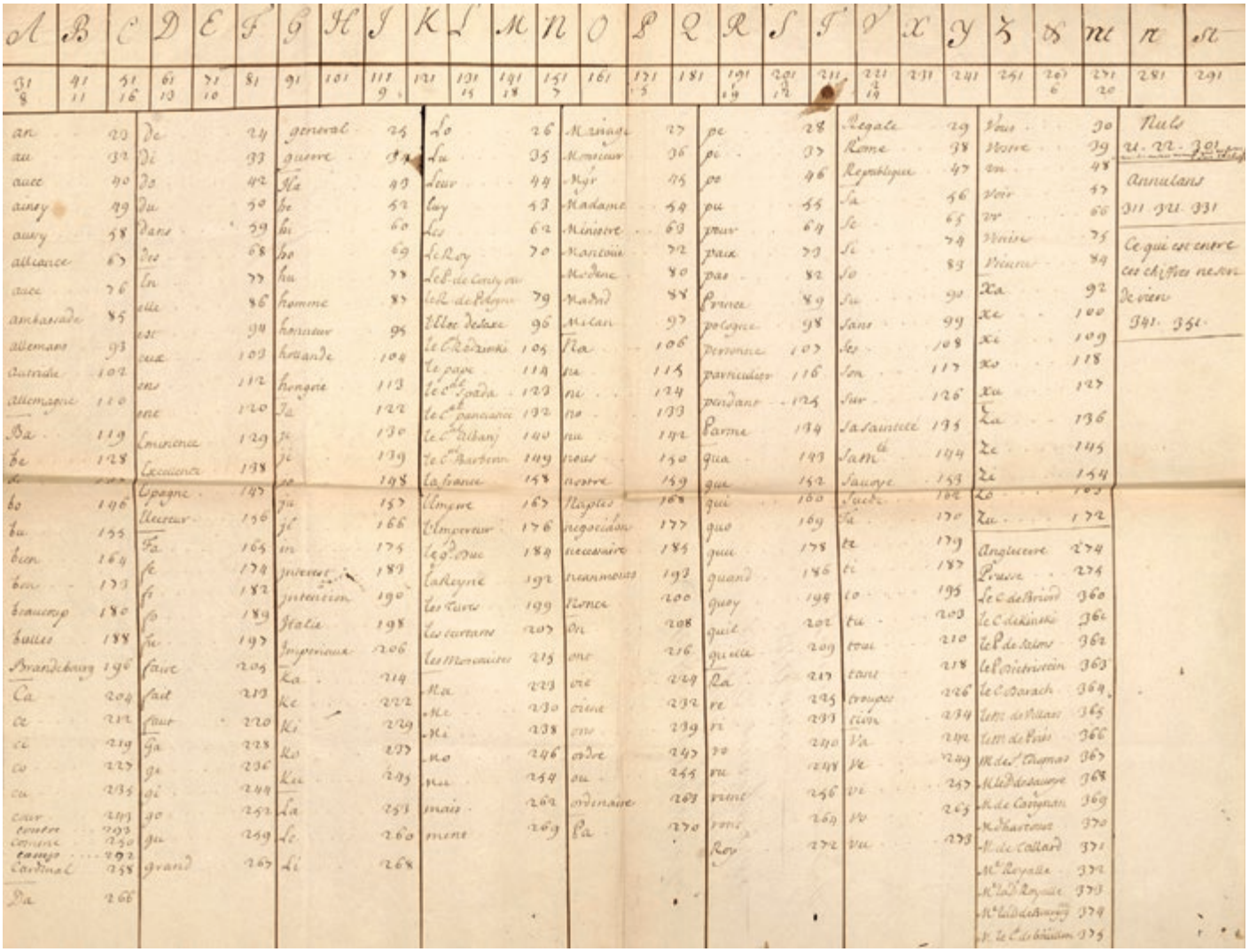
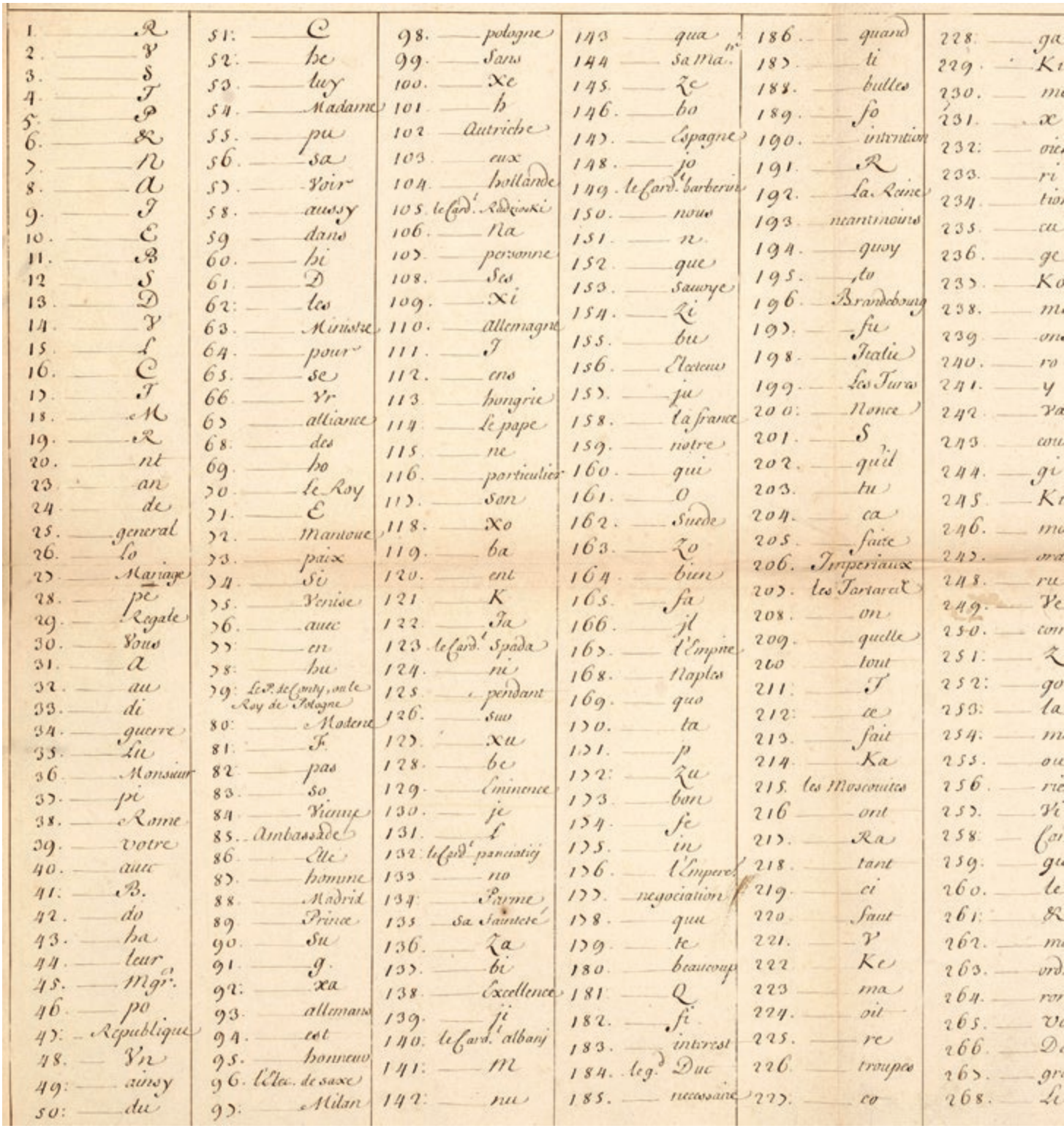


Table de chiffrement pour la correspondance entre le marquis d'Huxelles et le marquis de Villard. Les chiffres y sont désordonnés et des instructions de nullité sont là pour compliquer la tâche des décrypteurs. Ainsi, on voit dans l'avant-dernière colonne qu'en plus des nuls et des annulants (le chiffre suivant), deux symboles servent à entourer des parties entièrement nulles (coll. Archives municipales de Strasbourg).


1 R
2 V
3 S
4 T
5 P
6 K
7 N
8 A
9 J
10 E
11 B
12 S
13 D
14 V
15 L
16 C
17 T
18 M
19 R
20 nt
23 an
24 de
25 general
26 lo
27 Mariage
28 pe
29 Regale
30 Vous
31 A
32 au
33 di
34 guerre
35 Lu
36 Monsieur
37 pi
38 Rome
39 votre
40 auec
41 B.
42 do
43 ha
44 leur
45 Mgr.
46 po
47 Republique
48 Vn
49 ainsy
50 du
51 C
52 he
53 luy
54 Madame
55 pu
56 sa
57 Voir
58 aussy
59 dans
60 hi
61 D
62 les
63 Ministre
64 pour
65 se
66 Vr
67 alliance
68 des
69 ho
70 le Roy
71 E
72 Mantoue
73 paix
74 Si
75 Venise
76 auec
77 en
78 hu
79 Le R. de Comty, ou le Roy de Pologne
80 Modene
81 F.
82 pas
83 so
84 Vienne
85 Ambassade
86 Ile
87 homme
88 Madrid
89 Prince
90 Su
91 g.
92 xa
93 allemans
94 tot
95 honneur
96 l'Elec. de saxe
97 Milan
98 pologne
99 Sans
100 Xe
101 h
102 Autriche
103 eux
104 hollande
105 le Card.l Radzioski
106 Na
107 personne
108 Ses
109 Xi
110 allemagne
111 J
112 ens
113 hongrie
114 Le pape
115 ne
116 particulier
117 Son
118 Xo
119 ba
120 ent
121 K
122 Ja
123 le Card.l Spada
124 ni
125 pendant
126 sur
127 xu
128 he
129 Eminence
130 je
131 L
132 le Card.l panciatic
133 no
134 Parme
135 Sa Saintete
136 Za
137 bi
138 Excellence
139 ji
140 le Card.l albani
141 M
142 nu
143 qua
144 Sa Mta
145 Ze
146 ho
147 Espagne
148 jo
149 le Card.l barberin
150 nous
151 n
152 que
153 sauoye
154 Zi
155 bu
156 Electeur
157 ju
158 la france
159 notre
160 qui
161 O
162 Suede
163 Zo
164 bien
165 Sa
166 jl
167 l'Empire
168 Naples
169 quo
170 ta
171 p
172 Zu
173 bon
174 Se
175 in
176 l'Empereur
177 negociation
178 qui
179 te
180 beaucoup
181 Q
182 Si
183 interest
184 leg.d Duc
185 necessaire
186 quand
187 li
188 bulles
189 So
190 intention
191 R
192 la Reine
193 neantmoins
194 quoy
195 to
196 Brandebourg
197 Su
198 Italie
199 les Turcs
200 Nonce
201 S
202 quil
203 tu
204 ca
205 faite
206 Imperiaux
207 les Tartares
208 on
209 quelle
210 tout
211 T
212 se
213 fait
214 Ka
215 les Moscouites
216 ont
217 Ra
218 tant
219 ci
220 Saint
221 V
222 Ke
223 ma
224 oit
225 re
226 troupes
227 co
228 ga
229 Ki
230 m
231 x
232 vie
233 ri
234 tio
235 cu
236 ge
237 Ko
238 m
239 on
240 ro
241 y
242 Va
243 cou
244 gi
245 Ki
246 m
247 ora
248 ru
249 Ve
250 con
251 Z
252 go
253 la
254 m
255 ou
256 re
257 Vi
258 Car
259 gu
260 le
261 K
262 m
263 ord
264 ro
265 Va
266 D
267 gr
268 Le

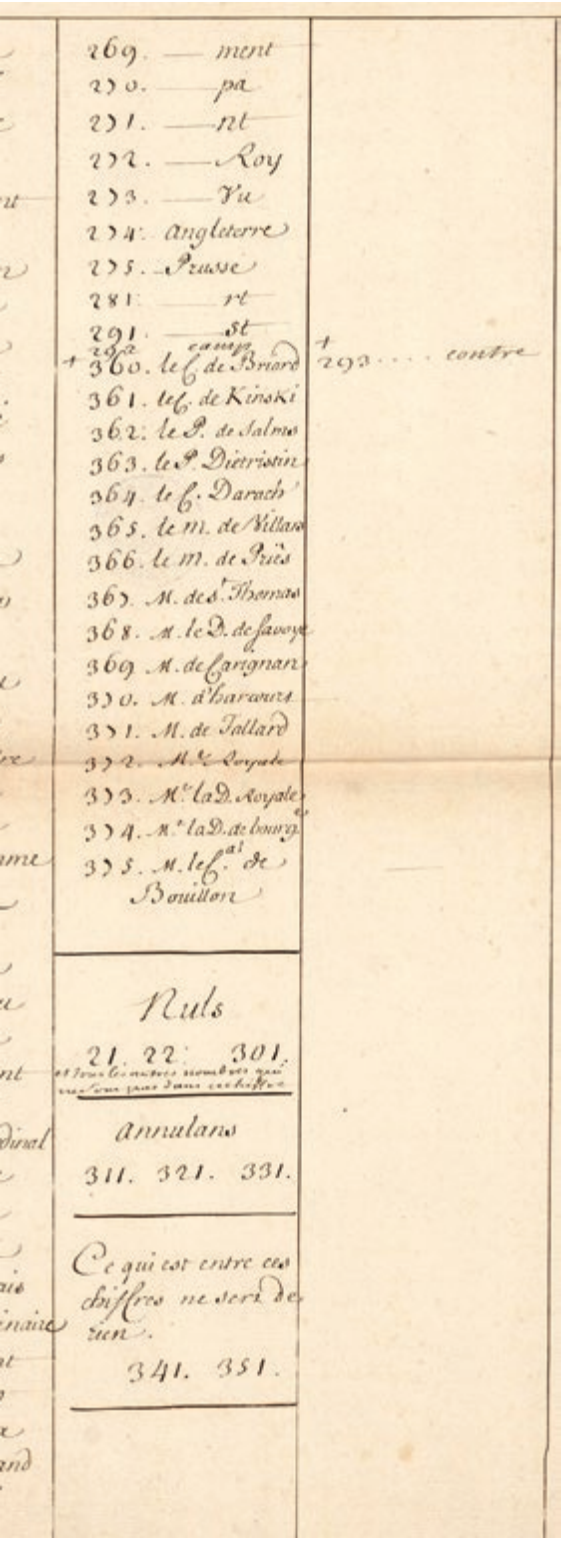

269. — ment
270. — pa
271. — nt
272. — Roy
273. — Vu
274. angleterre
275. Prusse
281. — rt
291. — st
292. camp
360. le C. de Briaré
361. le C. de Kinski
362. le P. de Salms
363. le P. Dietrichstin
364. le C. Darach
365. le M. de Villars
366. le M. de Prés
367. M. des Thomas
368. M. le D. de savoye
369. M. de Langnan
370. M. d'harcourt
371. M. de Tallard
372. M. Royale
373. M. la D. Royale
374. M. la D. de bourg
375. M. le al de Bouillon
293. . . . contre
Nuls
21. 22. 301.
et tous les autres nombres qui ne sont pas dans cet chiffre
annulans
311. 321. 331.
Ce qui est entre ces chiffres ne sert de rien.
341. 351.

Table de déchiffrement pour la correspondance entre le marquis d'Huxelles et le marquis de Villard (coll. Archives municipales de Strasbourg).

Notes

1 — Voir aussi, pour une introduction générale à la cryptologie, l'article de Valérie Caniart p. 25.

2 — Hervé Lehning, *L'univers des codes secrets de l'Antiquité à Internet*, Ixelles, 2012

3 — Hervé Lehning, « La boîte à chiffrer d'Henri II », in *Bulletin de l'Association des réservistes du chiffre et de la sécurité de l'information*, n° 41, p. 89-100

4 — Suétone, *Vies des douze Césars*, livre I, paragraphe 56

5 — al-Kindi, *Manuscrit sur le déchiffrement des messages cryptographiques*, Archives ottomanes d'Istanbul

6 — Vu la rapidité du décryptement d'Antoine Rossignol sur un texte probablement court, il est probable que le message venant de Réalmont était chiffré par une substitution alphabétique simple.

7 — Ces documents datés de 1642 sont classés sous la cote AA 1901. Les lettres déchiffrées l'ont été très probablement par leurs destinataires, qui connaissaient la table de chiffrement.

8 — Ces documents datés de 1644 – 1647 sont classés sous la cote AST 327. Les documents partiellement déchiffrés sont classés sous les cotes AST 327 90 et 92. La partie que nous déchiffrons p. 50 est classée sous la cote AST 327 88-1. Les autres se déchiffrent de même.

9 — Ce document est classé sous la cote AST 100-3.

10 — Le « parc à cochons » est l'autre nom donné au chiffre des francs-maçons, qui s'était inspiré de celui des Templiers.

11 — Ce document est coté AST 100 57-2 et porte la mention : Clefs pour correspondance secrète, cycle pascal, 1501 – 1530, Fondation Saint-Thomas.

12 — Le chiffre du feld-maréchal von Goetz figure sous la cote AA 1084-1. Le chiffre suivant est coté AA 1084-2.

13 — Tous ces chiffres sont classés sous la cote AMC 67482 VI. Le premier que nous citons est le 316-3, le suivant, le 316-4. Les listes de camouflage se trouvent sous les cotes 316-5 à 14.

14 — La table de chiffrement pour la correspondance entre le marquis d'Huxelles et le marquis de Villard se trouve sous la cote AMC 67482 VI 316-41, et la table de déchiffrement sous la cote AMC 67482 VI 316-40.