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

La Revue de la BNU est mise à disposition selon les termes de la Licence Creative Commons Attribution - Pas d'Utilisation Commerciale - Partage dans les Mêmes Conditions 4.0 International.

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 16^E AU 17^E 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 analyser¹. 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 Vigenère², boîte à chiffrer d'Henri II³).

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 dé-

crypteurs 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 Suétone⁴ :

« 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 >D>D>D> >D <V <XΔ ». 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 clairement⁵ :

« 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 Réalmont⁶, 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

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 Bazeris (1846-1931). Pour le casser, Bazeris 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 Bazeris 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 déchiffrées⁷, 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 Hénnot, 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 7, E et Γ ainsi que les correspondances contenues dans le tableau qui suit ; il reconstitue la table de chiffrement de la correspondance de 1544–1547⁸.

Clair	a	b	c	d	e	f	g	h	i	k	l	m
Chiffré	⊞	♀	K	λ	6	A	o	⊞	⊞	⊞	n	⊞
Clair	n	o	p	q	r	s	t	u	w	x	y	z
Chiffré	3	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 chiffréur 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 eux⁹ 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 Hénnot, 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 19^e 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 Pâques¹¹, 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 19^e 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 suffisait 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 19^e siècle.

Hervé Lehning

4) Cifra, quam habet Sturmium in Gallia.

a	b	c	d	e	f	g	h	i	k	l	m	n	o	p	q	r	s
v	u	y	f	n	z	o	x	g	φ	π	α	β	γ	δ	ε	ζ	η
t	u	x	z	y													
3	x	θ	i	x													
2		2		x													

Omnes Latina & Graeco, majuscula nullo,
cujusmodi sunt $\Lambda X \Sigma$

aut $\Lambda X \Sigma$

V	Sontifex.	€	Ferdinandus.
X	Cesar.	X	Seneti.
o	Rex Gallie.	Q	Dania Rex.
u	Delphinus.	†	Sal. Elector.
h	Amiralus.	D	Mauritius.
h	Cancellarius	€	Brandenburgensis Joachimus.
h	Cardinalis Turmonius	€	Henricus Brunsuicensis
e	Stampensius		
e	Card. Bellaius		
ee	Longinialis		
#	Dux Saxonie		
+ #	Langravius		
#	Brunsvicensis Henricus		
#	Bavaria. Batavi		
φ	Argentina		
φ	Ulna.		
φe	Augusta		
φ	Nuremberga.		
+ φ	Marchio Albertus		

Ex fascic. Arch. Argent.
G. V. S. 2. N. 2.

ad me te qua. Er aut
proponam aut postponam
aut addam ultra que nullas.

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																										16 17 18 19 20 21 22 23 24 25									
26	27	28	29	30	31	32	33	34	35	36	37	38	39	40	41	42	43	44	45	46	47	48	49	50	51	52	53	54	55	56	57	58	59	60	
61	62	63	64	65	66	67	68	69	70	71	72	73	74	75	76	77	78	79	80	81	82	83	84	85	86	87	88	89	90	91	92	93	94	95	
96	97	98	99	100	101	102	103	104	105	106	107	108	109	110	111	112	113	114	115	116	117	118	119	120	121	122	123	124	125	126	127	128	129	130	
131	132	133	134	135	136	137	138	139	140	141	142	143	144	145	146	147	148	149	150	151	152	153	154	155	156	157	158	159	160	161	162	163	164	165	
166	167	168	169	170	171	172	173	174	175	176	177	178	179	180	181	182	183	184	185	186	187	188	189	190	191	192	193	194	195	196	197	198	199	200	
201	202	203	204	205	206	207	208	209	210	211	212	213	214	215	216	217	218	219	220	221	222	223	224	225	226	227	228	229	230	231	232	233	234	235	
236	237	238	239	240	241	242	243	244	245	246	247	248	249	250	251	252	253	254	255	256	257	258	259	260	261	262	263	264	265	266	267	268	269	270	
271	272	273	274	275	276	277	278	279	280	281	282	283	284	285	286	287	288	289	290	291	292	293	294	295	296	297	298	299	300	301	302	303	304	305	
306	307	308	309	310	311	312	313	314	315	316	317	318	319	320	321	322	323	324	325	326	327	328	329	330	331	332	333	334	335	336	337	338	339	340	
341	342	343	344	345	346	347	348	349	350	351	352	353	354	355	356	357	358	359	360	361	362	363	364	365	366	367	368	369	370	371	372	373	374	375	
376	377	378	379	380	381	382	383	384	385	386	387	388	389	390	391	392	393	394	395	396	397	398	399	400	401	402	403	404	405	406	407	408	409	410	
411	412	413	414	415	416	417	418	419	420	421	422	423	424	425	426	427	428	429	430	431	432	433	434	435	436	437	438	439	440	441	442	443	444	445	
446	447	448	449	450	451	452	453	454	455	456	457	458	459	460	461	462	463	464	465	466	467	468	469	470	471	472	473	474	475	476	477	478	479	480	
481	482	483	484	485	486	487	488	489	490	491	492	493	494	495	496	497	498	499	500	501	502	503	504	505	506	507	508	509	510	511	512	513	514	515	
516	517	518	519	520	521	522	523	524	525	526	527	528	529	530	531	532	533	534	535	536	537	538	539	540	541	542	543	544	545	546	547	548	549	550	
551	552	553	554	555	556	557	558	559	560	561	562	563	564	565	566	567	568	569	570	571	572	573	574	575	576	577	578	579	580	581	582	583	584	585	
586	587	588	589	590	591	592	593	594	595	596	597	598	599	600	601	602	603	604	605	606	607	608	609	610	611	612	613	614	615	616	617	618	619	620	
621	622	623	624	625	626	627	628	629	630	631	632	633	634	635	636	637	638	639	640	641	642	643	644	645	646	647	648	649	650	651	652	653	654	655	
656	657	658	659	660	661	662	663	664	665	666	667	668	669	670	671	672	673	674	675	676	677	678	679	680	681	682	683	684	685	686	687	688	689	690	
691	692	693	694	695	696	697	698	699	700	701	702	703	704	705	706	707	708	709	710	711	712	713	714	715	716	717	718	719	720	721	722	723	724	725	
726	727	728	729	730	731	732	733	734	735	736	737	738	739	740	741	742	743	744	745	746	747	748	749	750	751	752	753	754	755	756	757	758	759	760	
761	762	763	764	765	766	767	768	769	770	771	772	773	774	775	776	777	778	779	780	781	782	783	784	785	786	787	788	789	790	791	792	793	794	795	
796	797	798	799	800	801	802	803	804	805	806	807	808	809	810	811	812	813	814	815	816	817	818	819	820	821	822	823	824	825	826	827	828	829	830	
831	832	833	834	835	836	837	838	839	840	841	842	843	844	845	846	847	848	849	850	851	852	853	854	855	856	857	858	859	860	861	862	863	864	865	
866	867	868	869	870	871	872	873	874	875	876	877	878	879	880	881	882	883	884	885	886	887	888	889	890	891	892	893	894	895	896	897	898	899	900	
901	902	903	904	905	906	907	908	909	910	911	912	913	914	915	916	917	918	919	920	921	922	923	924	925	926	927	928	929	930	931	932	933	934	935	
936	937	938	939	940	941	942	943	944	945	946	947	948	949	950	951	952	953	954	955	956	957	958	959	960	961	962	963	964	965	966	967	968	969	970	
971	972	973	974	975	976	977	978	979	980	981	982	983	984	985	986	987	988	989	990	991	992	993	994	995	996	997	998	999	1000	1001	1002	1003	1004	1005	
1006	1007	1008	1009	1010	1011	1012	1013	1014	1015	1016	1017	1018	1019	1020	1021	1022	1023	1024	1025	1026	1027	1028	1029	1030	1031	1032	1033	1034	1035	1036	1037	1038	1039	1040	
1041	1042	1043	1044	1045	1046	1047	1048	1049	1050	1051	1052	1053	1054	1055	1056	1057	1058	1059	1060	1061	1062	1063	1064	1065	1066	1067	1068	1069	1070	1071	1072	1073	1074	1075	
1076	1077	1078	1079	1080	1081	1082	1083	1084	1085	1086	1087	1088	1089	1090	1091	1092	1093	1094	1095	1096	1097	1098	1099	1100	1101	1102	1103	1104	1105	1106	1107	1108	1109	1110	
1111	1112	1113	1114	1115	1116	1117	1118	1119	1120	1121	1122	1123	1124	1125	1126	1127	1128	1129	1130	1131	1132	1133	1134	1135	1136	1137	1138	1139	1140	1141	1142	1143	1144	1145	
1146	1147	1148	1149	1150	1151	1152	1153	1154	1155	1156	1157	1158	1159	1160	1161	1162	1163	1164	1165	1166	1167	1168	1169	1170	1171	1172	1173	1174	1175	1176	1177	1178	1179	1180	
1181	1182	1183	1184	1185	1186	1187	1188	1189	1190	1191	1192	1193	1194	1195	1196	1197	1198	1199	1200	1201	1202	1203	1204	1205	1206	1207	1208	1209	1210	1211	1212	1213	1214	1215	
1216	1217	1218	1219	1220	1221	1222	1223	1224	1225	1226	1227	1228	1229	1230	1231	1232	1233	1234	1235	1236	1237	1238	1239	1240	1241	1242	1243	1244	1245	1246	1247	1248	1249	1250	
1251	1252	1253	1254	1255	1256	1257	1258	1259	1260	1261	1262	1263	1264	1265	1266	1267	1268	1269	1270	1271	1272	1273	1274	1275	1276	1277	1278	1279	1280	1281	1282	1283	1284	1285	
1286	1287	1288	1289	1290	1291	1292	1293	1294	1295	1296	1297	1298	1299	1300	1301	1302	1303	1304	1305	1306	1307	1308	1309	1310	1311	1312	1313	1314	1315	1316	1317	1318	1319	1320	
1321	1322	1323	1324	1325	1326	1327	1328	1329	1330	1331	1332	1333																							

A	B	C	D	E	F	G	H	I	K	L	M	N	O	P	Q	R	S	T	V	X	Y	Z	ne	π	π	
31 8	41 11	51 16	61 13	71 10	81	91	101	111 9	121	131 15	141 18	151 7	161	171 5	181	191 19	201 12	211 13	221 19	231	241	251	261 6	271 20	281	291
an	23	de		24	general	25	Lo	26	Marriage	27	pe	28	Regale	29	vous	30	Nuls									
au	32	di		33	guerre	34	lu	35	Monsieur	36	pe	37	Rome	38	Morre	39	u. 22. 301									
avec	40	do		42	Ha	43	leur	44	Ny	45	po	46	Republique	47	en	48	Annulans									
ainsy	49	du		50	be	52	luy	53	Madame	54	pu	55	Ja	56	voir	57	311 321 331									
auwy	58	dans		59	bi	60	Les	62	Ministre	63	pour	64	Je	65	27	66	311 321 331									
alliance	67	du		68	bo	69	le Roy	70	Monsieur	72	paix	73	Je	74	Minis	75	ce qui est entre									
avec	76	En		77	hu	78	le d. de Courcy		Madame	80	pas	82	Je	83	Prin	84	ce qui est entre									
ambassade	85	elle		86	homme	87	le d. de Courcy	79	Madame	88	Prin	89	Ja	90	Ja	92	ce qui est entre									
allemand	93	est		94	honneur	95	elle de Courcy	96	Monsieur	97	police	98	Jans	99	Ja	100	ce qui est entre									
Autriche	102	cuz		103	horande	104	le d. de Courcy	105	Ja	106	Personne	107	Je	108	Ja	109	ce qui est entre									
Allemagne	110	ens		112	hongrie	113	le d. de Courcy	114	Ja	115	particulier	116	Je	117	Ja	118	ce qui est entre									
		enc		120	Ja	122	le d. de Courcy	123	Ja	124	pendant	125	Je	126	Ja	127	ce qui est entre									
Da	119	Emence		129	Je	130	le d. de Courcy	132	Ja	133	Parne	134	Ja	135	Ja	136	ce qui est entre									
de	128	Excellence		138	Je	139	le d. de Courcy	140	Ja	142	qua	143	Ja	144	Ja	145	ce qui est entre									
de	141	Epagne		145	Ja	148	Ja	149	Ja	150	qua	152	Ja	153	Ja	154	ce qui est entre									
bo	146	Heur		147	Ja	157	Ja	167	Ja	168	qui	169	Ja	170	Ja	172	ce qui est entre									
bu	155	Heur		156	Ja	166	Ja	176	Ja	177	quo	178	Ja	179	Ja	180	ce qui est entre									
ben	164	Ja		165	Ja	175	Ja	185	Ja	186	qui	187	Ja	188	Ja	189	ce qui est entre									
ben	173	Ja		174	Ja	184	Ja	194	Ja	195	Ja	196	Ja	197	Ja	198	ce qui est entre									
braucy	180	Ja		182	Ja	192	Ja	202	Ja	203	Ja	204	Ja	205	Ja	206	ce qui est entre									
bulle	188	Ja		189	Ja	199	Ja	209	Ja	210	Ja	211	Ja	212	Ja	213	ce qui est entre									
Brandebour	196	Ja		197	Ja	207	Ja	217	Ja	218	Ja	219	Ja	220	Ja	221	ce qui est entre									
Ca	204	Ja		205	Ja	215	Ja	225	Ja	226	Ja	227	Ja	228	Ja	229	ce qui est entre									
ce	212	Ja		213	Ja	223	Ja	233	Ja	234	Ja	235	Ja	236	Ja	237	ce qui est entre									
ce	219	Ja		220	Ja	230	Ja	240	Ja	241	Ja	242	Ja	243	Ja	244	ce qui est entre									
co	225	Ja		226	Ja	236	Ja	246	Ja	247	Ja	248	Ja	249	Ja	250	ce qui est entre									
cu	235	Ja		236	Ja	246	Ja	256	Ja	257	Ja	258	Ja	259	Ja	260	ce qui est entre									
cour	241	Ja		242	Ja	252	Ja	262	Ja	263	Ja	264	Ja	265	Ja	266	ce qui est entre									
cour	249	Ja		250	Ja	260	Ja	270	Ja	271	Ja	272	Ja	273	Ja	274	ce qui est entre									
cour	250	Ja		251	Ja	261	Ja	271	Ja	272	Ja	273	Ja	274	Ja	275	ce qui est entre									
Cardinal	258	Ja		259	Ja	269	Ja	279	Ja	280	Ja	281	Ja	282	Ja	283	ce qui est entre									
Da	268	Ja		269	Ja	279	Ja	289	Ja	290	Ja	291	Ja	292	Ja	293	ce qui est entre									

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	51.	C	98.	pologne	143.	qua	186.	quand	228.	ga
2.	V	52.	be	99.	Sans	144.	sa ma.	187.	li	229.	K
3.	S	53.	luy	100.	Xe	145.	ze	188.	bulles	230.	me
4.	T	54.	Madame	101.	h	146.	bo	189.	fo	231.	x
5.	P	55.	pu	102.	Autriche	147.	Espagne	190.	intention	232.	on
6.	R	56.	sa	103.	eux	148.	jo	191.	R	233.	ri
7.	N	57.	voir	104.	hollande	149.	le fard. barberin	192.	la. Raine	234.	tion
8.	A	58.	aussy	105.	le fard. Adrien	150.	nous	193.	neantmoins	235.	ca
9.	I	59.	dans	106.	Na	151.	n.	194.	quoy	236.	ge
10.	E	60.	hi	107.	personne	152.	que	195.	to	237.	Ko
11.	B	61.	D	108.	Ses	153.	sauoye	196.	Brandebourg	238.	m
12.	S	62.	les	109.	Xi	154.	Li	197.	fu	239.	on
13.	D	63.	Ministre	110.	Allemagne	155.	bu	198.	Italie	240.	ra
14.	V	64.	pour	111.	I	156.	Nacteu	199.	Les Turcs	241.	y
15.	L	65.	se	112.	ens	157.	ju	200.	Nonce	242.	va
16.	C	66.	vr	113.	hongrie	158.	la France	201.	S	243.	con
17.	T	67.	alliance	114.	le pape	159.	notre	202.	qu'il	244.	gi
18.	M	68.	des	115.	ne	160.	qui	203.	tu	245.	K
19.	R	69.	ho	116.	particulier	161.	O	204.	ca	246.	me
20.	nt	70.	le Roy	117.	son	162.	Suede	205.	faite	247.	ma
21.	de	71.	E	118.	Xo	163.	zo	206.	Imperiaux	248.	ru
22.	general	72.	Mantoue	119.	ba	164.	bien	207.	les Tartares	249.	Ve
23.	lo	73.	paix	120.	ent	165.	fa	208.	on	250.	con
24.	Mariage	74.	Su	121.	K	166.	il	209.	quelle	251.	L
25.	pe	75.	Venise	122.	Ja	167.	l'Empire	210.	tout	252.	go
26.	Regale	76.	auc	123.	le fard. Spada	168.	Naples	211.	T	253.	la
27.	Sous	77.	en	124.	ni	169.	quo	212.	ce	254.	m
28.	A	78.	hu	125.	pendant	170.	ta	213.	fait	255.	ou
29.	au	79.	Le P. de Conty, ou le Roy de Pologne	126.	suu	171.	p	214.	Ka	256.	rie
30.	di	80.	Modene	127.	Xu	172.	zu	215.	les Moscovites	257.	Vi
31.	guerre	81.	F.	128.	be	173.	bon	216.	ont	258.	fan
32.	Lu	82.	pas	129.	eminence	174.	je	217.	Ra	259.	gu
33.	Monsieur	83.	so	130.	je	175.	in	218.	tant	260.	le
34.	pi	84.	Vianus	131.	L	176.	l'Empereur	219.	ci	261.	R
35.	Rome	85.	Ambassade	132.	le fard. panclatig	177.	negociation	220.	saut	262.	ma
36.	votre	86.	Alc	133.	no	178.	qui	221.	V	263.	ord
37.	auc	87.	homme	134.	Prime	179.	te	222.	Ke	264.	ron
38.	B.	88.	Madrid	135.	sa. Sainete	180.	beaucoup	223.	ma	265.	Ve
39.	do	89.	Prince	136.	za	181.	Q	224.	oit	266.	D
40.	ha	90.	Su	137.	bi	182.	fi	225.	re	267.	gre
41.	leur	91.	J.	138.	excellence	183.	interest	226.	troupes	268.	L
42.	Mgr.	92.	xa	139.	ji	184.	leg. Duc	227.	co		
43.	po	93.	alleman	140.	le fard. albanj	185.	necessaire				
44.	Republique	94.	est	141.	M						
45.	Vn	95.	honneu	142.	nu						
46.	aussy	96.	l'Ele. de saxe								
47.	du	97.	Milan								

269.	— ment
270.	— pa
271.	— nt
272.	— Roy
273.	— Vu
274.	— Angleterre
275.	— Prusse
281.	— rt
291.	— st
292.	— ^{causé} le f. de Briard
293.	— contre
361.	le f. de Kinski
362.	le P. de Salmo
363.	le P. Dietrich
364.	le f. Darach
365.	le m. de Villard
366.	le m. de Riès
367.	M. des Thomas
368.	M. le D. de Savoye
369.	M. de Langnau
370.	M. d'Harancourt
371.	M. de Tallard
372.	M. le Royale
373.	M. le D. Royale
374.	M. le D. de Bourg
375.	M. le f. de Bouillon

Ruls		
21.	22.	301.
et pour les autres symboles qui sont dans ce chiffre		
annulans		
311.	321.	331.
Ce qui est entre ces chiffres ne sera 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 déchiffrèrent 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.