Paulo Sarpi, le chiffrement de la correspondance

Marie Viallon

BREVE PRESENTATION DE PAOLO SARPI

Paolo Sarpi est né à Venise le 14 août 1552 et mort, dans sa ville natale, le 15 janvier 1623. Une carrière brillante mais discrète le conduit jusqu'à la charge de procureur général de l'Ordre des Serviteurs de Marie —ou servites— et jusqu'à Rome où il doit régler les affaires de son Ordre. Pendant ses deux séjours dans la cité pontificale, en 1579 et de 1585 à 1589, il se lie d'estime et d'amitié avec des personnalités attachées à l'idéal de réforme de l'Eglise romaine, en particulier avec le cardinal Giambattista Castagna qui est, peu après, élevé au trône de Saint-Pierre, sous le nom d'Urbain VII. La mort du pape, le 27 septembre 1590, au terme de quelques jours de règne et l'élection de Grégoire XIV, qui s'est surtout illustré par son excommunication d'Henri IV, mettent

un terme aux espoirs sarpiens de voir le renouvellement des structures ecclésiales. Après trois tentatives infructueuses pour obtenir un petit évêché tranquille (Milopotamos en 1593, Caorle en 1600, Nona en 1601), Sarpi semble se destiner à une existence studieuse et retirée au couvent Santa Fosca de Venise où parviennent —tout de même— les *stimuli* de l'université de Padoue et des recherches de Galilée. L'érudition scientifique de Sarpi le porte essentiellement vers les mathématiques et les sciences naturelles, alors que sa réflexion philosophique s'inscrit dans ses *Pensieri* dont la recherche souligne toujours plus les affinités avec la pensée de Montaigne, Charron ou Bodin.

Cependant, la crise de l'Interdit de 1606, fulminé par le pape Paul V contre la République de Venise, tire Paolo Sarpi de sa retraite et il observe justement dans une lettre à Christoph von Dohna :

> Un homme ne peut rien sans l'occasion. Si l'occasion de l'Interdit ne s'était pas présentée, je n'aurais jamais rien écrit.

Sarpi a accepté de s'engager de toutes ses forces dans la lutte contre l'Interdit pour des motifs politiques évidents, liés à l'indépendance et aux libertés menacées de la République de Venise, et pour des motifs religieux tout aussi évidents, liés à son désaccord profond avec l'Eglise quant à la conception des dogmes et de la discipline ecclésiastique.

Tout tourne autour de l'Interdit de Venise et il convient d'en rappeler très brièvement les éléments. Même si le différend entre Venise et Rome remonte au début du XIIIe siècle ; en effet, la République lagunaire s'est souvent montrée récalcitrante face au pouvoir pontifical ce qui lui a valu les foudres de l'Interdit romain sous les règnes d'Innocent III, de Martin IV, puis de Clément V (1309), de Calixte III, de Sixte IV (1483) et de Jules II (1509). A la fin du XVIe siècle, les dossiers embarrassants entre les deux capitales sont déjà nombreux et on se bornera à citer : l'attitude de Venise à l'égard de la France d'Henri de Navarre que, selon Rome, elle s'est trop vite empressée de reconnaître ; la succession du duché de Ferrare dont les deux Etats revendiquent le territoire ; les pirates uscoques qui ruinent la navigation en Adriatique ; l'affaire de Ceneda où le pape Clément VIII tente de s'ingérer entre l'autorité de l'évêque et celle du pouvoir civil. En outre, en 1603 puis en 1605, les autorités vénitiennes ont promulgué ou renforcé des lois qui cherchent à contrôler les implantations de nouvelles congrégations religieuses dans la ville et à contingenter les legs aux institutions religieuses ; ces dispositions veulent limiter l'emprise de l'Eglise sur le territoire réduit de la cité lagunaire (dans certaines paroisses, la propriété ecclésiastique s'élève à plus de 20% du

bâti[1]) et elles veulent réduire l'évasion de trop de revenus fonciers hors de la République alors qu'ils seraient beaucoup plus utiles dans des investissements dans l'économie de la République. Le 16 mai 1605, l'élection du pape Paul V, un expert en droit canon qui veut renforcer l'autorité pontificale et le prestige de l'Eglise, ne contribue pas à l'apaisement. Le feu est mis aux poudres par deux événements d'apparence mineure qui prennent soudain une dimension exagérée : à l'occasion du décès du patriarche de Venise, Matteo Zane, le Sénat procède selon le vieil usage de la *proba* et nomme son successeur, Francesco Vendramin, attendant du pape qu'il entérine ce choix … mais Paul V refuse et exige un examen que Venise, par principe, ne veut ni ne peut accepter. D'autre part, deux ecclésiastiques sont arrêtés (Scipione Saraceni en août et Marcantonio Brandolino en septembre 1605) pour des délits de droit commun que le Conseil des Dix entend juger suivant la loi civile vénitienne alors que le pape exige de les faire comparaître devant un tribunal ecclésiastique.

Tous ces dossiers puisent à la même source : la défense de l'autorité d'un Etat indépendant face au pouvoir temporel *super partes* du souverain pontife. En fait, les deux Etats partagent —sans se l'avouer— la même conscience de leur inéluctable affaiblissement face aux monarchies européennes modernes et de leur fatal besoin d'exister. Sommée, par bref pontifical du 10 décembre 1606, de se soumettre sous peine d'excommunication, la République de Venise refuse de venir à résipiscence et l'Interdit est fulminé sur la ville. Il faut attendre le 21 avril 1607, pour que la médiation française conduise à la levée de l'Interdit ; entre ces deux dates, a sévi une guerre généralisée des écrits où *toutes les provinces du monde chrétien ont été troublées* (Jacques de Thou cité par Filippo de Vivo).

C'est dans ce contexte que, le 14 janvier 1606, le Sénat vénitien nomme Sarpi *consultore in iure, perito della Theologia et cognitione canonica*, au service de la Sérénissime République ; pour reprendre les termes de son biographe[2], Sarpi est entré dans *un autre monde* face à cette Eglise qui se veut *théâtre du monde*. Une armée d'écrivains en campagne s'engage dans une « guerre des écrits » qui, à grand renfort de traités, oppose Sarpi aux plus grands cardinaux et théologiens de la Curie romaine, en particulier le vieil et intraitable Cesare Baronio, le jésuite Roberto Bellarmino et l'aristocratique Ascanio Colonna. Sarpi s'illustre par la publication de son *Apologia sopra la validità della scomunica ingiusta e giusta*[3]*,* puis ses *Considerazioni sopra le censure della Santità di papa Paolo V contra la Serenissima Republica di Venetia*[4]. Dans ses traités comme dans ses

[1] Anna Pizzati, *Commende e politica ecclesiastica nella repubblica di Venezia tra '500 e '600*, Venezia, Istituto veneto di scienze, lettere ed arti, 1997.
[2] Fulgenzio Micanzio, « Vita del padre Paolo », in Corrado Vivanti (éd.), *Paolo Sarpi. Istoria del concilio di Trento*, Torino, Einaudi, 1974, p. 1329.
[3] Venetia, Roberto Meietti, 1606. Traduction française, [s.l.], [s.n.], 1606.
[4] Venetia, Roberto Meietti, 1606. Cet ouvrage paraît en traduction française sous le titre de *Droits des souverains défendus contre les Excommunications*, La Haye, H. Scheurleer, 1721.

consulti[5] et dans sa vaste correspondance, Sarpi incite la République de Venise à résister à l'autorité pontificale quand elle s'ingère, sur le plan civil et judiciaire, dans sa souveraineté temporelle, violant ainsi la liberté politique et l'indépendance de la Sérénissime. Il exhorte la République à défendre contre le pouvoir universaliste et monarchique du souverain pontife, les libertés religieuses de son Eglise (en appelant *ad futurum concilium*) et, contre les abus du clergé et de l'inquisition, la liberté de conscience des Vénitiens, citoyens et fidèles (en invoquant la réforme intérieure de l'Eglise). Enfin, il invite la République à lutter contre les *superstitieux* (c'est-à-dire les catholiques de la Contre-réforme triomphante) et les *vicieux* qui *préfèrent servir dans l'oisiveté que lutter dans la liberté*[6]. Dans « l'un et l'autre droit », Sarpi tire autorité de nombreux auteurs condamnés par l'Eglise, à commencer par Jean Gerson et l'école gallicane, et, dès le 30 septembre 1606, ses écrits sont inscrits à l'*Index* et son excommunication *latæ sententiæ* est placardée sur les portes de la basilique Saint-Pierre, sur le Campo de' Fiori à Rome et sur les portes des églises de Venise[7]. Le Sénat vénitien réplique en marquant son soutien à son *consultore* par une augmentation substantielle de son salaire.

Cette sanction de l'Interdit est une réponse religieuse —donc spirituelle— à une difficulté politique —donc temporelle— entre Rome et Venise ; elle a des conséquences géopolitiques européennes car chacun se positionne selon ses intérêts, d'où une sévère dégradation des relations internationales. Finalement, alors que les préparatifs pour une guerre guerroyante vont bon train dans tous les Etats européens, la médiation du cardinal de Joyeuse, au nom du bon roi Henri, débouche sur la levée de l'Interdit, le 21 avril 1607. Ces quelques mois de différend vénéto-pontifical ont attiré le regard de nombreux européens sur le père Paul qui est apparu comme le théoricien clair et intelligent d'une doctrine qui préconise :

> • … que Dieu a créé deux gouvernements dans le monde, l'un spirituel et l'autre temporel. Chacun est suprême et indépendant de l'autre. Le premier est le ministère ecclésiastique, l'autre est le gouvernement politique. Il a donné le gouvernement spirituel aux Apôtres et à leurs successeurs et le temporel aux Princes de sorte que les uns ne peuvent s'ingérer dans ce qui appartient aux autres. Que le pape n'a pas pouvoir d'annuler les lois des princes sur des choses temporelles, ni de les priver de leurs Etats, ni de libérer leurs peuples de leur sujétion[8].

La levée de l'Interdit met un terme à la crise dans les relations vénéto-pontificales mais elle n'éteint pas le différend : Rome cherche alors à s'en prendre à celui qu'elle juge comme le

[5] Corrado Pin (éd.), *Paolo Sarpi. Consulti*, Pisa-Roma, Ist. Ed. e poligrafici internazionali, 2001.
[6] M. D. Busnelli (éd.), *Paolo Sarpi. Lettere ai protestanti*, Bari, Laterza, 1931, p. 282. Lettre à Groslot de L'Isle du 11 avril 1617 : i superstiziosi e i viziosi che amano meglio servir in ozio che faticar in libertà.
[7] Un exemplaire de ce placard d'excommunication de Paolo Sarpi, 5 janvier 1607, [Romæ, ex typ. Rev. Cam. Apostol., 1607] est conservée à la bibliothèque nationale Marciana, ms. it. VII,1952 (=8479).
[8] Paolo Sarpi, *Trattato dell'interdetto della santità di papa Paolo V, nel quale si dimostra che egli non è legitimamente publicato et che per molte ragioni non sono obligati gli ecclesiastici all'essecutione di esso né possono senza peccato osservarlo*, Venetia, Roberto Meietti, 1606, Lib. IV, p. 145. Nous traduisons.

« maillon faible » de la résistance vénitienne : Sarpi, en personne. Le cardinal de camerino, Mariano Perbenedetti, résume la situation dans une lettre au cardinal-neveu, Scipione Borghese :

> • … aussi lontemps que cette peste restera, il ne pourra y avoir de bonne entente entre Sa Sainteté et la république
> • … mentre vi starà questa peste, non potrà mai passare buona intelligenza tra Sua Beatitudine et la Republica[9]

Le 5 octobre 1607, un attentat est perpétré contre lui, au pont de Santa Fosca, tout près de son couvent, comme l'a raconté le président Jacques-Auguste De Thou :

> • Le poignard d'une main et le pistolet de l'autre, les assassins se saisissent du frère Marino pour l'empêcher de secourir son compagnon, blessent de trois coups Fra-Paolo au visage et à la gorge, lui laissent un poignard dans le corps; et, après avoir écarté à coups de pistolet le peuple qui couroit sur eux, se jettent dans un esquif à dix rames et se sauvent [10].

Avec esprit, Sarpi a déclaré y avoir reconnu le *stile romano* : en italien, le mot *stile* signifie le style, la manière comme le stylet, le poignard. Cet attentat manqué est suivi d'une tentative d'empoisonnement, quelques mois plus tard, à l'intérieur même du couvent des servites.

Parallèlement, Rome essaye deux voies pour se débarasser de Sarpi : une voie diplomatique pour que la France cesse de le soutenir et, d'une certaine manière, de le protéger ; et une voie plus judiciaire en essayant de monter contre lui un procès en inquisition ; le pape écrit au nonce à Venise, Berlingerio Gessi :

> • … s'hanno tanti inditii delle heresie di fra Paolo
> • … on a tant d'indices des hérésies du frère Paul.

Mais ce n'est pas suffisant, il faut des preuves matérielles indiscutables : des lettres compromettantes. Les nonces à Venise et à Paris sont instamment priés de se saisir des correspondances de Sarpi avec les réformés de France, d'Angleterre ou de Hollande qui voyagent par la valise diplomatique. Finalement, le noce parision finira par s'emparer de lettres qui sont encore conservées aux archives vaticanes.

Tirant les conséquences de ces événements, Paolo Sarpi introduit dès lors un chiffrement de sa correspondance.

LES TECHNIQUES DE CHIFFREMENT

Le chiffrement d'un texte —correspondance, dépêche, message, etc— est une technique qui doit permettre la transmission d'une information en garantissant qu'elle ne soit connue que de

[9] Archivio Vaticano, *Fondo Borghese*, II, 300, f. 291.
[10] Jacques de Thou (1553-1617), *Jac. Augusti Thuani Historiarum sui temporis libri CXXV*, Lutetiae, apud A. et H. Drouart, 1609-1614.
Comprend : Pars 1a. I. [Lib. I-VIII, 1543-1551.] ; II. [Lib. IX-XVI, 1551-1555.] ; III. [Lib. XVII-XXII, 1555-1559.] ; Pars 2a. IV. [Lib. XXIII-XXVI, 1559-1560.] ; Pars 3a. V. [LIb. XXVII-XXXIV, 1560-1563.] ; VI. [Lib. XXXV-XLII, 1563-1568.] ; VII. [Lib. XLIII-L, 1568-1571.] ; VIII. [Lib. LI-LVII, 1571-1574.] ; Pars 4a. IX. [Lib. LVIII-LXV, 1574-1578.] ; X. [Lib. LXVI-LXXIII, 1578-1580.] ; XI. [Lib. LXXIV-LXXX, 1581-1584.].

l'expéditeur et du destinataire qui ont convenu, auparavant, d'une méthode de cryptage. Il s'agit donc de faire voyager un document dont le texte doit rester illisible ou non-significatif pour tout autre lecteur.

Dans un premier temps, il convient de distinguer les méthodes de cryptographie des techniques de stéganographie [στεγανός / steganos « je couvre » + γραφή / graphein, « écriture »]. En effet, ces dernières ne sont que des obstacles à la lecture qui ne modifient pas le message. Ainsi peut-on considérer les *grilles de Cardan* : Jérôme Cardan (1501-1576) a imaginé une feuille dans laquelle il a découpé des fenêtres de lecture ; le chiffreur pose sa grille sur le papier puis écrit le message dans les cases et, enfin, complète ses lignes d'écriture avec des lettres inutiles. Au moment du décryptage, il suffira d'appliquer de nouveau la grille pour qu'elle ne laisse apparaître que le message en clair. On peut utiliser un livre déjà imprimé à cette fin en ne transmettant que la grille. Cette technique sera reprise par Richelieu (1585-1642) mais elle présente l'inconvénient que le message caché est beaucoup plus long que le message en clair.

A l'époque où Sarpi convient avec ses correspondants d'un système d'écriture codée, la cryptographie connaît une grande vogue et un nombre important de traités savants ont été publiés pour en vanter les avantages ou pour en fournir les règles d'usage : le théologien catalan Ramon Llull a publié *Ars inventiva veritatis* (1300) où il fournit la technique des disques chiffrés, Leon Battista Alberti compose son *De componendis cyfris* (1466) qui utilise un disque de chiffrement poly-alphabétique directement inspiré de ses travaux en architecture c'est-à-dire que les lettres du message sont remplacées par les lettres d'un autre alphabet et l'opération est répérée plusieurs fois. Au début du XVIe siècle, un abbé bénédictin de Würzsbourg, Johannes Heidenberg *dit* Trithemius (1462-1516), rédige une véritable somme intitulée *Libri polygraphiæ* qui connaitra un grand succès tout au long su siècle et sera traduite en français en 1561 par Gabriel de Collange sous le titre de *Polygraphie et universelle escriture cabalistique* : il propose de remplacer chaque mot du message par un groupe de mots[11]. Cette méthode a été notoirement utilisée par les Vénitiens aux XVe-XVIe

[11] Voici l'un de ces alphabets dits de l'*Ave Maria*:

A	dans les cieux	N	en paradis
B	à tout jamais	O	toujours
C	un monde sans fin	P	dans la divinité
D	en une infinité	Q	dans la déité
E	à perpétuité	R	dans la félicité
F	sempiternel	S	dans son règne
G	durable	T	dans son royaume
H	sans cesse	U, V, W	dans la béatitude
I, J	irrévocablement	X	dans la magnificence
K	éternellement	Y	au trône
L	dans la gloire	Z	en toute éternité
M	dans la lumière		

siècles et on peut citer les lettres *sub enigma* d'Andrea Gritti, ambassadeur vénitien à Istanbul, qui espionne au bénéfice du sénat vénitien et informe

> *chi in prigione per debiti sarà rilasciato in giugno* / celui qui sortira de prison pour dettes en juin = la flotte turque qui prendra la mer en juin.

De même, le chiffre mercantile de 1529 établi par la chancellerie secrète où

- *x brazza di fustagno* / x bras de futaine = x navires
- *le ballotte di saon de barba* / des caisses de savon à barbe = les cardinaux
- *i guanti di vitello belli* / de beaux gants de veau = les Français
- *bambasin con pello de far una veste a mia moier* / une pièce de coton pour faire une robe à ma femme = les galères de Doria qui rentrent sans escorte.

A la même époque, plusieurs auteurs italiens publient leurs traités : Giovanni Battista Bellaso publie *La cifra* (1553)*, Novi e singoli modi di cifrare* (1555), *Il vero modo di scrivere in cifra con facilità* (1564) ; Giovani Battista della Porta fait paraître *De furtivis litterarum notis, vulgo de ziferis* (1563) où il propose une méthode par substitution diagrammatique, c'est-à-dire qu'il remplace chaque couple de lettres du message par un symbole. On notera que Della Porta a connu Paolo sarpi à l'occasion d'un séjour à Padoue et Venise, en 1592.

En France, l'ouvrage le plus célèbre est celui de Blaise de Vigenère : *Traicté des chiffres et secrètes manières d'escrire* (1596) qui présente une méthode de substitution poly-alphabétique qui ne sera décryptée qu'en 1854, par le major prussien Friedrich Kasiski. Ces ouvrages présentent d'amples considérations techniques sur la manière de construire un système d'écriture cachée, dans un jargon complexe qui les rend presque inaccessible ; c'est le paradoxe de ces discours qui veulent donner des moyens de communication qui ne doivent pas être communiqués. Trithemius reconnaît :

> Tout ce qui, par communication et publique divulgation, peut nuyre, doit estre raisonnablement caché et couvert par mystique et obscure parole, ou par secrette et incogneue escriture[12].

Les méthodes de cryptographie peuvent être rangées en trois grandes familles, si l'on suit les classifications de Jérôme Cardan dans son *De subtilitate* (1550)[13] :

— le chiffrement par transposition,
— le chiffrement par translation,
— le chiffrement par substitution.

Le chiffrement par transposition

L'inconvénient de ce chiffre est qu'il exige beaucoup de temps pour le cryptage et que le message crypté est excessivement long.

[12] Trithemius (1462-1516), *Clavicule ou interprétation sur le contenu és cinq livres de Polygraphie ou universelle escriture cabalistique, traduicte et augmentée par Gabriel de Collange*, Paris, J. Kerver, 1561, p. 194.

[13] Jérôme Cardan (1501-1576), *De subtilitate libri XXI*, Norimbergiæ, apud J. Petreium, 15550 ; Lugduni, apud P. Rolletium, 1554

C'est une technique fondée sur la perturbation de l'offre des lettres dans le mot crypté sans modifier ces lettres. A l'image du verlan (= l'envers) qui modifie l'ordre des syllabes par métathèse, la transposition est utilisée dans le jargon des milieux populaires depuis le Moyen-Age ou le verlan : on place la consonne initiale à la fin, puis on ajoute un L et enfin on ajoute le suffixe *-ébem* ou *–oque*. Si l'on part du mot FOU, les diverses étapes de chiffrement sont :

OUF ▷ LOUF ▷ LOUFOQUE.

Le chiffrement par translation

Il s'agit de déplacer l'ordre des lettres sans les modifier, ainsi on peut prendre un texte : RENDEZ-VOUS DEMAIN A L'UNIVERSITE et l'inscrire en 4 colonnes :

R	E	N	D
E	Z	V	O
U	S	D	E
M	A	I	N
A	L	U	N
I	V	E	R
S	I	T	E

puis on brouille les colonnes suivant un code pré-établi 3142, et on obtient :

N	R	D	E
V	E	O	Z
D	U	E	S
I	M	N	A
U	A	N	L
E	I	R	V
T	S	E	I

Ainsi, le message codé est : NRDEVEOZDUESIMNAUANLEIRVTSEI .

Le chiffrement par substitution

C'est —et de loin— la méthode la plus utilisée, même par la fameuse machine *Enigma* des Allemands, au début de la Seconde guerre mondiale ; une même lettre est toujours substituée par le même signe d'où la facilité du décryptage ou cryptanalyse, par l'analyse fréquentielle des lettres.

Le carré de Polybe

Dans cette catégorie, on peut classer le « carré » de l'hisorien Polybe qui consiste à substituer des nombres aux lettres. Il s'agit de tracer un carré 5X5 (on peut augmenter le nombre de cases pour un alphabet plus important) :

	1	2	3	4	5
1					
2					
3					
4					
5					

dans lequel on place les lettres, quel que soit l'alphabet ou la langue mais avec des adaptations :

	1	2	3	4	5
1	A	B	C	D	E
2	F	G	H	I/J	L
3	M	N	O	P	Q
4	R	S	T	U	V
5	W	X	Y	Z	

Dès lors, chaque lettre est définie par le chiffre de sa ligne, suivi du chiffre de sa colonne.

A = 11 ; B = 12 ; C = 13 ; D = 14 ; E = 15
F = 21 ; G = 22 ; H = 23 ; …
M = 31 ; N = 32 ; …
R = 41 ; …
W = 51 ; … .

On peut compliquer ce carré en lui appliquant un mot de passe. Exemple, si on donne le code « PAOLO SARPI », on en inscrit les lettres dans le carré en évitant les doubles :

	1	2	3	4	5
1	P	A	O	L	S
2	R	P	I		
3					
4					
5					

puis on complète avec les lettres inutilisées, dans l'ordre usuel de l'alphabet :

	1	2	3	4	5
1	P	A	O	L	S
2	R	P	I	B	C
3	D	E	F	G	H
4	M	N	Q	R	T
5	U	V	W	X	Z

Dans ce cas, A = 12 ; B = 24 ; C = 25 ; D = 31
E = 32 ; F = 33 ; G = 34 ; …

Le code de César

Il y a aussi un système dont la paternité est attribuée à Jules César, d'après les informations données par Suétone dans *La vie des 12 Césars*, livre I, § LVI. Ce *code de César* utilisé dans sa correspondance avec Cicéron consiste en une substitution mono-alphabétique (c'est-à-dire qu'une lettre remplace une lettre) définie par un décalage —ou rotation— de 4 ; A = D

A	B	C	D	E	F	G	H	I	J	…
D	E	F	G	H	I	J	K	L	M	…

En conséquence, le message « Veni vidi vici » = YHOL YLGL YLFL

Ce chiffrement présente l'inconvénient de n'offrir que 25 possibilités de cryptage, donc c'est un code très peu sûr. Mais comme il est d'une très grande simplicité, il a été encore utilisé par les sudistes américains pendant la guerre de Sécession et par l'armée russe en 1915. Ce code a été utilisé plus récemment sur Internet sous le nom de ROT13 car la rotation est de 13 (A = N). Du fait de la facilité de son décryptage, l'idée de ROT13 est de diffuser des textes qui ne peuvent pas être lus par mégarde ou bien de crypter son numéro de CB.

La table de Blaise de Vigenère (1523-1596)

C'est une méthode de chiffrement qui utilise le principe du code de César avec une seule table (qui n'a même pas besoin d'être si secrète que cela !) et un mot de passe ou clé littérale qui indique le décalage alphabétique à appliquer pour chaque lettre. Avant Vigenère, Giovanni Battista Bellaso et Govanni Battista della Porta avaient proposé une semblable grille qui donne des suites de permutations ; Della Porta (qui a eu l'occasion de rencontrer Paolo Sarpi à Venise et/ou Padoue en 1592) a appelé sa clé le *verme littérale / le ver littéral*. Cet algorithme de cryptage présente l'avantage d'être d'une mise en place très simple (comme le décryptage) ; en outre, il rend inopérante la méthode de décryptage par analyse fréquentielle et, enfin, il peut avoir une infinité de clés.

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

Si on prend pour clé « Paolo Sarpi », pour encoder le texte « correspondance chiffrée », on prend la colonne de la première lettre du texte « C » et la ligne de la première lettre de la clé « P » et on obtient « R ». On poursuit avec les deuxièmes lettres « O + A = O », puis on continue avec les troisièmes lettres « R + R = I », et ainsi de suite …

On obtient le message codé suivant :

C	**O**	**R**	**R**	**E**	**S**	**P**	**O**	**N**	**D**	**A**	**N**	**C**	**E**	**C**	**H**	**I**	**F**	**F**	**R**	**E**	**E**	
P	**A**	**O**	**L**	**O**	**S**	**A**	**R**	**P**	**I**	**P**	**A**	**O**	**L**	**O**	**S**	**A**	**R**	**P**	**I**	**P**	**A**	**O**
R	**O**	**F**	**C**	**S**	**K**	**P**	**F**	**C**	**L**	**P**	**A**	**Q**	**P**	**Q**	**Z**	**I**	**W**	**U**	**Z**	**T**	**E**	

Pour décoder, il suffit de se placer dans la ligne de la première lettre P de la clé et chercher la colonne de la lettre R = C.

Le chiffre bilitère de Francis Bacon (1561-1626)

C'est un chiffre de stéganographie qui n'utilise que des conbinaisons de A et de B. Publié dans son ouvrage *The Advancement of learning* de 1605, repris dans on ouvrage *De dignitate et augmentis scientiarum* de 1623 :

A	B	C	D	E	F	G	H	I-J	K	L	M	N
aaaaa	aaaab	aaaba	aaabb	aabaa	aabab	aabba	aabbb	abaaa	abaab	ababb	ababb	abbaa

O	P	Q	R	S	T	U-V	W	X	Y	Z
abbab	abbba	abbbb	baaaa	baaab	baaba	baabb	babaa	babab	babba	babbb

Un exemple codé

P	A	O	L	O		S	A	R	P	I
abbba	aaaaa	abbab	ababb	abbab		baaab	aaaaa	baaaa	abbba	abaaa

Ce chiffre préfigure le codage binaire de l'informatique par 0 et 1 en *binary digit* ou *bit* c'est-à-dire le code ASCII.

LE CHIFFRE DE PAOLO SARPI

Après son excommunication *latæ sententiæ* (fulminée le 30 septembre 1606), après les deux attentats auxquels il a réchappé (le 5 octobre 1607 puis en novembre 1607), après l'attaque sur ses lettres destinées à Castrino qui sont saisies par le nonce à Paris et envoyées au cardinal Borghese le 2 septembre 1610, Sarpi convient de la nécessité de couvrir sa correspondance avec les réformés de France du manteau du secret.

Dès le 12 mai 1609, Sarpi s'intéresse à la question du chiffrement des correspondances comme il en fait état dans sa lettre à Groslot, relative aux travaux du mathématicien Jacques Aleaume, disciple de François Viète :

- Se monsignor Aleaume riducesse in methodo la risolutione delle cifre, farebbe opera molto degna.
- Si monsieur Aleaume transformait en méthode sa résolution des chiffres, il ferait œuvre utile.

C'est dans sa lettre du 25 novembre 1609 à Francesco Castrino (un réformé italien réfugié à Paris) qu'il fait la première allusion à un nécessaire chiffrement de leurs relations épistolaires :

- Vostra Signoria ha dato fuoco alla machina ch'io haveva per mente, con dirmi ch'è necessario una cifra,
- Votre Seigneurie a mis le feu à la machinerie que j'avais en tête, en me disant qu'un chiffre est nécessaire,

Paolo Sarpi a des talents mathématiques indéniables et, depuis 1600, il est en contact avec Aleaume qui lui fait connaître le mathématicien dalmate Marino Ghetaldi ; en conséquence, il est parfaitement armé pour constituer lui-même son chiffre et, comme il l'écrit à Castrino, deux heures lui seront suffisantes. Il informe son correspondant de l'envoi de ce chiffre, dans sa lettre du 9

décembre. Après accusé de réception du chiffrement, c'est à partir du 5 janvier 1610 qu'il en annonce l'emploi.

Quand il définit son chiffre, Paolo Sarpi précise à Jérôme Groslot de l'Isle qu'il le veut imparfait car cette imperfection-même complexifie la tâche du déchiffreur non-autorisé :

> • La cifra bisogna che sia imperfetta, come fatta da me che in quella professione non intendo (27 avril 1610 à Groslot).
> • Le chiffre doit être imparfait, comme je le fais moi qui ne suis pas un professionnel.
>
> • La nostra ciffra, sì come è tanto secura che è impossibile levarla, così ha questo diffetto che un minimo fallo di chi la scrive, la rende inintelligibile et anco che la interpreta ha bisgno di starci molto diligente (08 novembre 1611 à Groslot).
> • Notre chiffre -qui est si sûr qu'il est impossible de le décrypter- présente le défaut que la moindre erreur de celui qui écrit le rend inintelligible et le déchiffreur aussi doit être très acharné.

Ceci explique pourquoi Paolo Sarpi n'a pas utilisé les services des secrétaires-chiffreurs de la chancellerie secrète de la Sérénissime. Cela lui aurait été d'autant plus facile que, d'une part, il jouit d'un accès très libéral aux archives secrètes et au personnel qui les gère et, d'autre part, une relation d'estime et d'amitié le lie à Giovanni Battista Lionello (1588-1622), notaire de la chancellerie ducale et secrétaire d'ambassade attaché au chiffre.

En outre, Sarpi veut également un chiffre évolutif et il évoque le *suplemento della cifra* (28 septembre 1610 à Groslot) ou son *amplificatione* (07 décembre 1610 à Groslot). Toutefois, il reconnaît qu'il rencontre des problèmes pour dresser un chiffre commun au français (langue utilisée par Groslot pour lui écrire[14]) et à l'italien (langue qu'il utilise lui-même pour répondre) ; ainsi, son premier chiffre avec les huguenots de France ne comprenait-il pas la lettre « x », inconnue en italien et il l'ajoute plus tard, en octobre 1610.

En plus, s'il veut contrer tout déchiffrement par l'analyse fréquentielle des lettres, Sarpi doit tenir compte de ces fréquences des lettres et il peut penser à crypter par syllabes, mais ces fréquences syllabiques sont très différentes en français ou en italien :

> • Ho più volte pensato di ampliar la cifra, con note per le sillabe più usate, ma perché non sono le medesime quelle della lingua francese et dell'italiana, non ho saputo come fare. Le più usitate appresso a noi sono quelle che entrano nel declinar i verbi ma la declinatione francese è tanto diversa che quelle non servono niente. Quanto alla lettera 'x', per non confonderla con le nulle, il suo carattere potrà essere 22 et così ho notato nella mia cifra. (12 octobre 1610 à Groslot)
>
> • Plusieurs fois, j'ai eu l'intention d'augmenter notre chiffre de notes sur les syllabes les plus courantes mais, parce qu'elles sont différentes en français et en italien, ne n'ai pas su comment faire. Les sylllabes les plus courantes sont, chez nous, celles qui composent la flexion verbale mais la

[14] Longtemps, il a été écrit que Sarpi échangeait avec ses correspondants en latin : ainsi Griselini, *Memorie aneddote*, p. 222 ; mais les fréquentes allusions de Sarpi dans ses lettres à Grslot pour évoquer ses difficultés à chiffrer pour les deux langues en même temps sont parmi les nombreuses preuves du contraire. La preuve matérielle indéniable est un morceau de lettre, écrite et signée de la main de Jérôme Groslot de l'Isle (Bib. Querini Stampalia, IX 16, 370, f. 142v) qui montre à l'évidence que Groslot lui écrivait en français. Quelques années plus tard, Philippe Duplessis-Mornay emploie également le français, après plusieurs échanges en latin.

déclinaison française est si différente que cela ne sert à rien. Quant à la lettre 'x', pour ne pas la confondre avec les nulles, elle pourra recevoir le chiffre 22, comme je l'ai noté dans mon chiffre.

Cette idée du chiffrement/déchiffrement par syllabe provient de la méthode de « découvrement » ou cryptanalyse de François Viète telle qu'exposée dans son *Deschiffrement d'une lettre escripte par le commandeur Moreo au roy d'Espaigne son maitre* (du 28 octobre 1589), Tours, Mettayer, 1590[15] :

• Il faut remarquer toutes les sortes de figures, soit chiffre ou jargon, et nombrer combien elles sont de fois, puis remarquer toutes les sortes de figures qui précèdent ou qui suivent, et conférer les plus fréquentes afin de découvrir les mêmes mots et les mêmes valeurs et n'y épargner ni le labeur ni le papier … et enfin par hypothèses on pourra parvenir à la résolution. [Après avoir établit des règles pour discerner les voyelles des consonnes], par la marque des finales et hypothèses se distingueront les voyelles des voyelles et les consonnes des consonnes, et par leur rareté et fréquence, leur individu.

Finalement, dans sa lettre du 26 avril 1611, Sarpi nous donne une longue explication de l'algorithme de composition de son chiffre. Malgré la longueur de ses explications, il reste difficile d'élucider sa démarche :

• Desiderando continuar la communicatione per lettera con Vostra Signoria, la quale non possiamo trattenere senza ciffra, né intieramente se ella non è facile, per questa causa ho più volte pensato di ampliar quella che sino al presente è stata tra noi, et se mi è attraversato impedimento insuperabile, volendo fare che possi servire alla lengua francese et italiana. Finalmente io ho dato nella presente, la qual mando a Vostra Signoria, che non ha bisogno di nissuna attentione di mente né inquisitione di caratteri, così per esser scritta come per esser interpretata, ma il solo copiare basta. Nello scrivere si camina per li numeri arabici et si copia per li numeri romani, donde le parole restano confuse, sì che non è possibile cavarci senso. Quello che haverà da deciffrare piglia le parole così confuse et le mette per li numeri romani, et poi le legge per li numeri arabici. La carta si mette sotto a un foglio bianco, dove trasparendo le linee, serve per sempre. Li spazij che sono crociati si tralasciano vacui, il che serve acciò ché, se uno per qualche caso inventasse quelli doi numeri -10 et 117- che sono radici della compositione, resti però confuso per il vacuo. Il numero delli pieni è 104 : quando la cosa da scrivere portasse manco parole, se ne puol aggionger tante di altra materia che venga al numero et, quando portasse più parole che tal numero, si replica la seconda et la terza volta et più, quanto fa bisogno. Io ho tentato un gran ciffrista, il quale non è stato sufficiente di interpretarmi un concetto scritto, onde mi vado credendo haver trovato cosa di competente uso. Mando insieme un essempio, acciò Vostra Signoria possi con quello supplir a qualche mancamento che io havessi usato nel volermi esprimere. Se questa piacerà a Vostra Signoria, ella potrà usarla immediate. Io non la userò sin ché non ho risposta da lei della ricevuta (26 avril 1611 à Groslot)[16].

• Désirant poursuivre notre communication épistolaire qui ne peut aller sans chiffre, ni sans un chiffre facile, j'ai pour cette raison pensé améliorer celui que nous avons jusqu'à présent utilisé entre nous et j'ai rencontré un très grand problème car je voulais qu'il serve en français comme en italien. Finalement, je suis parvenu à cela ; il n'y a besoin ni d'une attention particulière ni d'une recherche de caractères, pour écrire comme pour décrypter, il suffit de copier. Pour écrire, on suit les chiffres arabes et, pour copier, les chiffres romains donc les mots sont mélangés et leur sens ne peut être saisi. Celui qui déchiffrera devra prendre les mots et les classer suivant les chiffres romains et puis les lire suivant les chiffres arabes. Il faudra mettre la lettre sous un papier blanc où les lignes transparaissent, une bonne fois pour toutes (NdT : *cela semble ressembler à la grille de Cardan)*. Les espaces marqués d'une croix doivent rester vides de sorte que, si quelqu'un trouve ces deux nombres —10 et 117— qui sont les bases de la composition du chiffre, il soit toutefois gêné par ces vides. Le nombre des pleins est de 104 : si le texte à écrire comporte moins de mots, on peut en ajouter jusqu'à parvenir à ce

[15] Marco Panza, « François Viète : between analysis and cryptanalysis », in *Studies in History and Philosophy of Sciences*, vol. 37 (2006), n°2, p. 269-289.
Peter Pesic, « François Viète father of modern cryptanalysis », in *Cryptologia*, vol. 21 (1997), n°1, p. 1-29.
[16] Lettre 1611-04-26 à Groslot.

nombre et, si ce texte en comporte plus, il suffit de répéter une seconde ou une troisième fois, voire plus, comme de nécessaire (Ndt : *cela semble être une clé comme dans la grille de Vigenère*). J'ai interrogé un grand chiffreur qui n'est pas parvenu à décrypter un texte écrit, donc je crois avoir trouver quelque chose d'efficace. Je vois joins un exemple afin que vous puissiez ainsi suppléer à toute lacune. Si cela vous satisfait, vous pourrez l'utiliser immédiatement. Pour ma part, je ne l'utiliserai pas avant que vous n'en accusiez réception.

Le chiffre finalement établi par Sarpi nous est connu : BnF *Dupuy* 111, f. 100-101 : *Chiffre escrit de la main du père Paul*, document annexé à la lettre du 9 décembre 1609. Ces tables semblent symmétriques c'est-à-dire qu'elles établissent les normes pour le chiffrement et pour le déchiffrement.

Si on tente une analyse de ce chiffre, on peut remarquer que Sarpi semble avoir composé un chiffre combinatoire c'est-à-dire qu'il a pris des éléments à divers systèmes. Il a des chiffrement littéraux par substitution où chaque lettre en clair a un cryptage constant. On peut en établir le tableau, en prenant pour modèle le *carré de Polybe*, les lignes 2, 5, 6, 9 et 0 sont nulles ; c'est-à-dire qu'elles peuvent être incluses pour brouiller le déchiffrement d'un décodeur non-autorisé.

	1	2	3	4	5	6	7	8
1			D	H			I	O
2		x						
3	Z			C			G	L
4	P		U				B	F
5								
6								
7	M		Q	T				A
8	E		N	R			S	
9								
0								

Afin d'éviter que l'analyse fréquentielle ne permette de casser son chiffre, Sarpi introduit des éléments de stéganographie où un mot en clair est caché par un bigramme [lettre+chiffres]. Cela l'oblige à dresser 5 listes de mots cryptés que l'on peut faire entrer dans des manières de tableaux sans que cela n'apporte d'information complémentaire mais pour faciliter la mémorisation (et partant le travail du chiffreur) Sarpi a choisi une lettre-clé que nous avons tenté d'expliciter. Les termes grisés en italique sont des ajouts faits par Castrino pour compléter les listes de Sarpi ; en conséquence, nous ne les avons pas inclus dans notre analyse.

Tableau des **U** (clé : ce sont les mots **U**tiles ou **U**suels)

1	se		**11**	la		**21**	di		**31**	del
2	et		**12**	li		**22**	tra		**32**	dal
3	overo		**13**	le		**23**	contra		**33**	in
4	non		**14**	come		**24**	dove		**34**	con
5	ma		**15**	per		**25**	senza		**35**	che
6	più		**16**	quando		**26**	re		**36**	perchè
7	molto		**17**	adunque		**27**	to		**37**	abenchè
8	poco		**18**	qui		**28**	va			
9	sotto		**19**	costì		**29**	V.S.			
10	il		**20**	di		**30**	al			

Tableau des **R** (clé : ce sont surtout des substantifs et quelques adjectifs)

1	sospetto		**28**	calunnia		**55**	leggiero
2	pretesto		**29**	disgusto		**56**	ordinario
3	instruttione		**30**	frutto		**57**	abandonato
4	intentione		**31**	libro		**58**	spirituale
5	concordia		**32**	corrispondenza		**59**	mondano
6	pratica		**33**	consequenza		**60**	espresso
7	diligenza		**34**	controversia		**61**	principio
8	protettione		**35**	pericolo		**62**	mezo
9	raggione		**36**	mutatione		**63**	fine
10	commercio		**37**	honore		**64**	negotio
11	copia		**38**	silentio		**65**	impedimento
12	lettera		**39**	quiete		**66**	zelo
13	luoco		**40**	pericolo		**67**	conseglio
14	tempo		**41**	espeditione		**68**	resolutione
15	occasione		**42**	mandato		**69**	speranza
16	beneficio		**43**	pensiero		**70**	intelligenza
17	arte		**44**	fatiche		**71**	confidenza
18	beneplacito		**45**	matrimonio		**72**	avantaggio
19	resposta		**46**	secreto		**73**	aggiuto
20	aviso		**47**	buono		**74**	persecutione
21	complemento		**48**	necessario		**75**	*rettore*
22	evangelio		**49**	facile		**76**	*assemblea*
23	dottrina		**50**	utile		**77**	*primo presidente*

24	conversatione	**51**	vero	**78**	*nuntio*
25	differenza	**52**	dubio	**79**	*triumvirato*
26	guerra	**53**	nuovo		
27	cosa	**54**	vicino		

On notera que le mot *pericolo* figure à deux reprises : r35 et r40 : erreur ou calcul pour un terme qui peut être important ?

Tableau des **G** (clé : ce ne sont des verbes à forte valeur **G**rammaticale)

1	havere	**13**	debe	**25**	persuade	**37**	*Boillon*
2	essere	**14**	ho	**26**	dubita	**38**	*cortegiani*
3	assiste	**15**	ha	**27**	insiste	**39**	*Maurizio*
4	va bene	**16**	disse	**28**	ottene	**40**	*conte de Soissons*
5	fa	**17**	dice	**29**	comunica	**41**	*la regina*
6	pote	**18**	è	**30**	dà	**42**	*Epernon*
7	bisogna	**19**	fu	**31**	*armata*	**43**	*Conti*
8	tratta	**20**	sarà	**32**	*frontiera*	**44**	*casa di Ghisa*
9	spera	**21**	afferma	**33**	*stati*	**45**	*Concini*
10	posso	**22**	nega	**34**	*Fiandra*	**46**	*Contestabile*
11	può	**23**	vince	**35**	*delfino*	**47**	*governatore*
12	debo	**24**	perde	**36**	*Dighiera*		

Tableau de **T** (clé : ce sont généralement des **T**itres)

1	Malcontenti	**17**	figlio	**33**	papa
2	politici	**18**	fratello	**34**	cardinale
3	giesuiti	**19**	gentilhuomo	**35**	vescovo
4	papisti	**20**	moglie	**36**	imperator
5	confessionisti	**21**	Republica	**37**	ellettore
6	reformati	**22**	soldato	**38**	re
7	puritani	**23**	capitano	**39**	principe
8	ugonoti	**24**	fanti	**40**	duca
9	collegati	**25**	cavalli	**41**	ambasciator
10	spia	**26**	ministro	**42**	secretario
11	prete	**27**	predicator	**43**	agente
12	frate	**28**	Signore	**44**	consegliero
13	religione	**29**	confessor	**45**	Parlamento
14	doni	**30**	nave	**46**	*cardinal du Perron*
15	denari	**31**	marchese	**47**	*sig. de Suilly*
16	entrata	**32**	conte	**48**	*padre Coton*

Tableau des **M** (clé : ce sont tous des termes de géographie, comme sur une **M**appemonde)

1	Austria		**19**	Nansau		**37**	Milano
2	Boemia		**20**	Haga		**38**	Napoli
3	Danimarca		**21**	Ambsterdam		**39**	Sicilia
4	Sassonia		**22**	Bruselles		**40**	Fiorenza
5	Palatinato		**23**	Anversa		**41**	Parma
6	Carintia		**24**	Italia		**42**	Mantoa
7	Turrino		**25**	Germania		**43**	Geneva
8	Vertemberg		**26**	Ongaria		**44**	Svizzeri papisti
9	Brandeburg		**27**	Polonia		**45**	Svizzeri evangelici
10	Cleves		**28**	Spagna		**46**	Sig. Castrino
11	Donavert		**29**	Indie orientali		**47**	Sig. de l'Isle
12	città		**30**	Indie occidentali		**48**	Fra Paulo
13	Condé		**31**	Francia		**49**	*Presidente De Thou*
14	Soisson		**32**	Paesi Bassi		**50**	*Gillot*
15	Villeroi		**33**	Inghilterra		**51**	*Leschassier*
16	Sellerì		**34**	Scocia		**52**	*Bociello*
17	Parigi		**35**	Venetia			
18	Leone		**36**	Roma			

1610-02-03.A Castrino

De la main de Fanzano, partiellement chiffrée, signée *Antonio Bianchi m48*, de Venise.
Source : BnF, *Dupuy* 111, f. 33r.
Editions précédentes : M. Busnelli, 1931, II, lettre XXXI, p. 74-76.
M. Busnelli, 1986, lettre XXI, p. 126-128.

Al molto illustre signor colendissimo, il signor […][17]

Molto illustre signor colendissimo

La lettera di Vostra Signoria delli 29 decembre, che già 15 giorni doveva arrivar qui, è venuta insieme con l'altra delli 12 genaro et ha tardato tanto il corriero, che bisogna scrivere in fretta.

Incomincierò dalla prohibitione de libri, se ben alcuni son vietati ad instanza de giesuiti, altri però son prohibiti non senza qualche loro offesa, come li opuscoli del Mariana[18], historico spagnol nominato, censurati solo perché diffende la loro opinione del divino agiuto efficace contro li dominicani. E' molto facile in Roma il prohibir un libro et qui in Italia li scrittori sono tanto assuefatti che non ne tengono il conto, come cotesti. Io tengo per cosa certa, et Vostra

[17] Le nom du destinataire a été "caviardé" sur le pli mais la majuscule et le jambage du *t* sont encore reconnaissables.
[18] Juan de Mariana (1536-1624) SJ, *Tractatus VII : De adventu B. Jacobi apostoli in Hispaniam ; Pro editione vulgata ; De spectaculis ; De monetæ matatione; De die mortis Christi ; De annis arabum ; De morte et immortalitate*, Coloniæ aggrippinæ, Antonij Hierati, 1609, 444 p.

Signoria lo vederà dall'evento, che non sarà retrattata la prohibitione dell'aresto[19], ma sarà ben con qualche arte interposto dilatione alli dissegni di costì, si che forsi il tutto anderà in oblivione ; ma, se questo non sarà et che qualche cosa si faccia, voglio ben pregare Vostra Signoria che mi faccia parte immediate di qualunque cosa sia riuscita, mandandomi, se sarà possibile, copia formale. L'ardimento usato dalli padri giesuiti nelle prediche mostra che habbino maggiori fondamenti che quanto è l'estesa di Francia ; altrimenti sarebbe stata gran patia. Io dubito che le radici poste da loro in cotesto regno vivendo l'altro re, coperte doppo di un poco di terra, si siano in questi tempi ingrossate, si che adesso possino germogliare senza temer l'agricoltore.

Le preparationi alla guerra, de quali Vostra Signoria ne fa mentione, sono molto grandi et le cause di eccitarla maggiori ma son tanto solito a veder l'acqua sino in terra et poi sparir le nuvole che congietturo dover esser così ancora et dover esser causa di fermar ogni motto quella stessa che ha fermato li passati. Potrei ingannarmi, ma chi conosce le proprie debolezze interiori et coperte, fa saviamente a contentarsi di mostre et non venir a fatti che le possino publicare.

Qui è nuova che lo Spinola sij chiamato in Spagna; questo può esser o per darli carico altrove, o per levarli da quel loco. *M28* [Spagna] rimette *t15 u33 m25* [denari in Germania] assai. *T33 g3* [Il papa assiste] a *38 81 18 41 18 38 13 18 25* [Leopoldo], cosa che farà forsi chiarire *t38 u21 m31* [il re di Francia] che *g15 r71* [ha confidenza] d'haverlo per se. *U31 u11 r26 u21 71 17 25 38 78 83 90 28 69* [Della guerra di Milan] vi è qualche cosa di vero, ma tutto sta secondo l'inviamento di *m10* [Clèves]. *T36* [L'imperatore] è perduto affatto. *T33 g8 u33 r47 r70 u34 m35 u5 g18 r17 u21 m28* [Il papa tratta in buona intelligenza con Venetia ma è arte di Spagna] quale ha voluto *74 25 18 56 83 17 34 69 78 u26 u10 t40 u21 m7* [tonicare il duca di Turrino]. La repentina partita del corriero quando credeva che differisse alcune hore di più, mi fa esser breve per questa volta et dirli con queste sole parole *u35 u32 m15 u2 u32 t41 u31 t38 u18 g18 u34 73 43 81 84 17 59 71 18 83 95 17 78 20 u35 m48 g29 u34 t6 u21 m31* [che dal Villeroi et dal ambasciator del re qui è con querimonia che Fra Paulo comunica con reformati di Francia] causa *u36 u4 87 34 84 17 43 81 u21 87 43 78 71 78 83 18* [perché non scrive di sua mano]. Resto tutto alli servitij di Vostra Signoria, pregando Dio che li doni ogni felicità.

Di Vinetia il 3 febraro 1610
Di Vostra Signoria molto illustre

Devotissimo servitore
Antonio Bianchi *m48* [Fra Paulo]

Sarpi posséde autant de chiffre qu'il a de correspondants voire avec l'ambassadeur Foscarini, il en a deux. Comme toujours, ses lettres ne sont pas intégralement chiffrées mais seuls les noms de personnes et quelques phrases clés sont cryptées. Avec Foscarini, Sarpi met en place un système par substitution nominale ; c'est-à-dire qu'un nom remplace un nom. Exemple : *Verona* pour signifier l'Allemagne et donc, *veronese* pour allemand. Parfois, l'association du mot et de son cryptage répondent à une forme de logique ; ainsi dans la chiffre avec Foscarini l'*empereur* est-il crypté en *Giulio* (qui évoque, bien évidemment, Jules César) ou bien les *hérétiques* sont-ils *rossi* (c'est-à-dire rouges commes le feu qui doit les brûler. Mais cela relève plus de l'imagination et des jeux d'association du chiffreur.

	1	2	3	4	5	6	7	8
1								
2			N	G	D		F	
3		P		C	R		M	
4		E	T		B		I	
5		U,V	S	O			A	
6								
7		H		Q	L			

[19] L'*Arrestum contra Joannem Castellum, Goannis Passeratii "Præfatiuncola in disputationem de ridiculis"* (Lugduni Batavorum, Lodovici Elzeverii, 1595) émis par le Parlement de Paris le 27 décembre 1594 contre Jean Chastel et contre Jean Passerat (1534-1602) a été, dans un premier temps, interdit puis rétabli, suite aux interventions françaises, comme le prévoit Sarpi et l'explique Jacques-Auguste de Thou, dans son *Histoire.*

8								
9								
0								

Chiffre à Foscarini

Un exemple extrait de sa lettre 1608-06-25 :

> *si fa sempre qualche machinatione 34 54 23 43 35 54 51 75 57 90 52 47 43 57 10 37 47 57 [contro la vita mia]*

les nombres nuls permettent de marquer la coupure entre les mots.

Le même texte, chiffré pour Castrino, aurait été :

34 18 83 74 84 18 – 38 78 – 43 17 74 78 – 71 17 78