Le premier essor de la cryptographie en France (1510-1630)

Camille Desenclos

LE PREMIER ESSOR DE LA CRYPTOGRAPHIE EN FRANCE (1510 –1630)[1]

Camille Desenclos

Le travail de renseignement est au coeur d'un véritable paradoxe : il doit demeurer invisible pour porter ses fruits mais s'incarne dans une intense production documentaire synthétisant à la fois la somme d'informations collectées et les décisions en résultant. Seule preuve tangible de son existence, l'écrit est essentiel au fonctionnement et à la qualité d'un appareil de renseignement autant qu'il peut en causer la perte. Objet de toutes les convoitises et de tous les dangers, la production documentaire ne peut donc se conformer aux règles habituelles d'écriture, de transmission mais aussi de conservation et doit faire l'objet d'une protection supplémentaire. Si la dissimulation est essentielle à la protection de certains acteurs du renseignement, dont la participation doit demeurer ignorée ou invisible, l'écrit ne peut qu'être ponctuellement dissimulé, une absence totale de production documentaire, notamment de la part d'une ambassade, étant plus suspecte encore. La matérialité de l'écrit ne pouvant être occultée, son contenu doit l'être. Si certains procédés de stéganographie, notamment l'encre invisible, peuvent y contribuer, la cryptographie demeure le procédé le plus sûr, et de fait le plus usité, pour protéger l'information avant, pendant et après sa transmission.

Peu présente dans les sources médiévales, la cryptographie semble se généraliser soudainement au XVI^{e} siècle. Si la corrélation entre son essor et l'établissement de relations diplomatiques permanentes entre les principaux États européens ne peut être niée, cet essor ne doit pas être réduit à la seule diplomatie. Effet de mode ou résultat d'une démultiplication des besoins de protection dans un contexte politique instable, la cryptographie s'impose dans les pratiques épistolaires politiques du second XVI^{e} siècle, conduisant à une diversification de ses acteurs mais aussi à une démultiplication des pratiques cryptographiques, au-delà de la seule sphère diplomatique, productrice principale, mais non unique, de documents chiffrés. Cette visibilité soudaine de la cryptographie, grâce à la diplomatie, révèle aussi en creux toute la difficulté de l'étude des pratiques cryptographiques modernes, confrontée à une triple déformation – institutionnelle, matérielle et archivistique – de la perspective.

[1] Cette contribution s'appuie sur un projet de recherche, au long cours, mené en partenariat avec la Bibliothèque nationale de France (« Naissance et essor de la cryptographie en France, XVI^{e}- XVII^{e} siècles ») et dont la première phase, actuellement en cours, consiste en l'identification et datation des tables de chiffrement et dépêches chiffrées conservées par l'institution.

Apparition ou révélation ?

Si son observation tient souvent de l'heureuse rencontre pour la période médiévale[1], le chiffre se fait omniprésent dans les dépêches diplomatiques françaises à la fin des années 1520[2]. La diplomatie constitue incontestablement le principal vecteur du développement, à l'époque moderne, des pratiques cryptographiques dans le royaume de France : tous les documents chiffrés produits pendant le premier quart du XVI^e^ siècle émanent de représentants français à l'étranger. Cette démultiplication des sources cryptographiques, notamment dans les collections de la Bibliothèque nationale de France, est néanmoins trompeuse.

L'hypothèse la plus communément admise repose sur une dissémination, au tournant du XVI^e^ siècle, de la pratique cryptographique dans toute l'Europe depuis la péninsule italienne, confrontée un siècle plus tôt au besoin accru d'échanges protégés avec la démultiplication des représentations diplomatiques[3]. Si l'origine italienne de la cryptographie moderne est indiscutable[4], le lien avec la pratique diplomatique, tout comme sa temporalité mérite d'être davantage nuancé. Bien que des représentations permanentes se multiplient sous le règne de François I^er^[5], la diplomatie permanente n'apparaît pas soudainement au début du siècle[6] : des relations diplomatiques suivies existaient préalablement et se sont progressivement incarnées dans de longues ambassades, certes extraordinaires, mais dont la pratique continue de s'observer tout au long de l'époque moderne, tandis que les représentations permanentes ne s'institutionnalisent que fort progressivement[7].

De la même manière que la diplomatie permanente ne naît pas soudainement au début du XVI^e^ siècle, la cryptographie s'immisce progressivement dans les pratiques diplomatiques. Dès la fin du XIV^e^ siècle, des dépêches sont chiffrées et décryptées[8]. La pratique demeure néanmoins ponctuelle et surtout inégalement mobilisée dans les divers États européens[9]. En réalité, le soudain volume de dépêches chiffrées à partir de la seconde moitié des années 1520 est moins dû à l'émergence d'une nouvelle pratique scripturale qu'à une pratique archivistique encore aléatoire : les correspondances produites pendant le premier quart du XVI^e^ siècle nous sont, en partie, parvenues sous la forme de copies – sans mention ni report du chiffrement – ou d'épaves, à l'image de cette

---

[1] Stephen J. Harris, « Anglo-Saxon Ciphers », dans Katherine Ellison, Susan Kim (dir.), *A Material History of Medieval and Early Modern Cihers. Cryptography and the History of Literacy,* Routledge, New York / Londres, 2018, pp. 65-79.

[2] Dès 1526, 33 % de la correspondance conservée de Nicolas Raincé, représentant français à Rome, avec Anne de Montmorency est chiffrée (Bibliothèque nationale de France [désormais BnF], fr. 2984).

[3] Donald E. Queller, *The office of ambassador in the middle ages,* Princeton university press, Princeton, pp. 140-141. Pour autant, la cryptographie ne naît pas au *Quattrocento*.

[4] Jean-Marie Moeglin (dir.), Stéphane Péquignot, *Diplomatie et « relations internationales » au Moyen Âge (IX^e^ – XV^e^ siècle),* PUF, Paris, 2017, pp. 642-645.

[5] D'un seul représentant permanent en 1515, la diplomatie française passe à dix en 1547 (Alain Tallon, *La France et le concile de Trente*, École française de Rome, Rome, 1997, pp. 21).

[6] Jean-Marie Moeglin, « La place des messagers et des ambassadeurs dans la diplomatie princière à la fin du Moyen Âge », *Études de lettres,* 3 (2010), pp. 11-36 ; Stéphane Péquignot, « Les diplomaties occidentales et le mouvement du monde », dans Patrick Boucheron (dir.), *Histoire du monde au XV^e^ siècle*, Paris, Fayard, 2009, pp. 709-723.

[7] Lucien Bély, *L'art de la paix en Europe,* Paris, P.U.F., 2007, p. 41-67.

[8] Jean-Marie Moeglin, Stéphane Péquignot, *Diplomatie et « relations internationales … »*, *op. cit.,* pp. 642-645.

[9] Les royaumes d'Angleterre et d'Aragon, mais aussi de France, ne paraissent recourir au chiffre qu'à la fin du XV^e^ siècle (*ibid.,* pp. 644).

dépêche chiffrée de Louis de Solliès à Florimond Robertet, en date du 8 juillet 1513, rare vestige de la correspondance entre les deux hommes, conservée dans un recueil de « *lettres escrites du règne de Louis XII [et de François Ier] touchant les affaires de l'Estat* »[1]. Si la conservation des dépêches est loin d'être systématique par la suite, l'importance des lacunes pour les correspondances du début du XVIe siècle empêche, outre une analyse quantitative, toute appréhension du degré d'imprégnation de l'écriture cryptographique dans les pratiques épistolaires de la diplomatie[2].

Les sources directes comme indirectes[3] convergent néanmoins toutes vers une pratique cryptographique déjà établie au sein de la diplomatie française au début du XVIe siècle, tandis que le recours au chiffre est immédiat pour toutes les représentations permanentes nouvellement établies. La lettre de Louis de Solliès est ainsi intégralement chiffrée, à l'exception de la formule finale de politesse, et s'y observe déjà le report d'un déchiffrement interlinéaire, pratique encore largement usitée au milieu du XVIIe siècle. La pratique cryptographique au sein de la diplomatie est déjà quotidienne et n'appartient plus à l'extraordinaire. L'établissement de représentations permanentes lui donne en réalité une surface bien plus large. La production documentaire de la diplomatie étant accrue par la multiplication des acteurs et l'augmentation de la fréquence épistolaire, la pratique devient automatiquement plus visible dans les sources qui nous sont parvenues.

Une absence de spécialisation dans la pratique

La diplomatie française ne cherche cependant nullement à s'emparer de manière exclusive du chiffre. Au contraire, les conditions dans laquelle la pratique cryptographique se développe contribuent à une plus ample diffusion. Bien que celle-ci se généralise à l'aune de l'établissement progressif de représentations permanentes et de l'intensification des échanges entre les principaux États européens, elle n'est liée à aucune institution. En 1513, Louis de Solliès adresse en effet ses dépêches, pourtant chiffrées, à Florimond Robertet, trésorier de France et secrétaire des finances. De même, Nicolas Raincé, également agent à Rome, adresse, en 1526, les siennes à Anne de Montmorency, alors grand maître de France. Si l'un et l'autre, tant en raison de leurs charges – Florimond Robertet coordonne l'expédition des dépêches en tant que secrétaire des finances et Anne de Montmorency la réception des ambassadeurs en tant que grand maître – que de leur proximité avec le roi, instrumentent une grande partie de la correspondance diplomatique, ils n'en constituent pas pour autant des ministres des Affaires étrangères avant l'heure[4]. Institués par un règlement du 1er avril 1547, les secrétaires d'État ne s'organisent pas immédiatement par compétences, mais par zones

---

[1] BnF, Dupuy 261, fol. 121.

[2] Cette déformation créée par la conservation lacunaire des dépêches diplomatiques s'observe avec plus de force encore pour l'époque médiévale, ne permettant pas de dater avec précision l'adoption de la pratique cryptographique par la diplomatie française (Jean-Marie Moeglin (dir.), Stéphane Péquignot, *Diplomatie et « relations internationales… »*, *op. cit.*, pp. 642).

[3] Une dépêche adressée par François Ier à ses ambassadeurs en Angleterre mentionne ainsi, fortuitement, le déchiffrement de la lettre que l'ambassadeur français auprès de l'empereur lui a envoyée (BnF, fr. 5761, fol. 11-12 ; cité et transcrit par Monique Garant-Zobel : « Lettres échangées entre François Ier et ses ambassadeurs à Londres (août-octobre 1518) », dans *Bibliothèque de l'École des chartes,* 112 (1954), pp. 118).

[4] Bernard Chevalier, « Florimond Robertet (v. 1465-1527) », dans Cédric Michon, *Les conseillers de François Ier*, Presses Universitaires de Rennes, Rennes, 2011, pp. 99-116 ; Thierry Rentet, « Anne de Montmorency (1493-1567). Le conseiller médiocre », dans *ibid.,* pp. 279-309.

géographiques, regroupant indistinctement – et aléatoirement en fonction des titulaires des charges –, dans un même portefeuille provinces et États étrangers[1] et augmentant d'autant la potentielle surface d'utilisation du chiffre. Dès 1570, une première spécialisation s'observe par l'attribution de la Maison du roi et de la gendarmerie à Simon Fizes, baron de Sauve ; celle-ci n'est cependant ni automatique ni définitive. Il faut attendre le règlement du 1er janvier 1589 pour voir rassemblée entre les mains d'un seul la gestion des Affaires étrangères.

Cette absence d'institutionnalisation de la diplomatie au XVIe siècle n'est pas sans conséquence pour la pratique cryptographique. Mobilisée, dans un premier temps, dans un contexte diplomatique, elle est en réalité exercée, certes par des ambassadeurs au degré de professionnalisation par ailleurs très divers, mais aussi par des officiers royaux en charge à la fois d'affaires extérieures et intérieures, selon la conception du gouvernement de l'État propre à ce premier XVIe siècle. Ni leur pratique épistolaire – rien, si ce n'est le contexte d'écriture, ne distingue une dépêche politique d'une dépêche diplomatique – ni leurs attributions ne viennent dissocier leur pratique diplomatique de leur pratique politique. De ce fait, il n'est guère étonnant de voir se déployer une 'écriture cryptographique hors du contexte diplomatique[2], et ce sans qu'il ne s'agisse d'un phénomène de porosité, ni de transfert, des usages. Le manuscrit français 3029 de la Bibliothèque nationale de France contient ainsi plusieurs mémoires intégralement chiffrés, émanant probablement de l'amiral de Bonnivet ou de Louis de La Trémoille, à l'attention de Florimond Robertet. Si ces mémoires ne sont ni datés ni signés, ils font partie d'un recueil cohérent de dépêches, tant dans la date que dans les origines. Or, aucune d'elles n'a été écrite en dehors des frontières du royaume et leur contenu permet de les dater du début des années 1520. S'il n'a pas lieu de faire de Florimond Robertet le seul secrétaire à manier le chiffre, la présence de mémoires chiffrés, hors usage diplomatique, vient ici rappeler qu'avant d'être une pratique associée à la diplomatie, la cryptographie répond à un besoin de dissimuler l'information pour protéger les intérêts du royaume de France et qu'il n'a jamais été question d'en limiter l'usage aux seules correspondances diplomatiques. Il serait néanmoins intéressant d'identifier avec précision l'épistolier à l'origine de ces mémoires chiffrés. Contrairement à l'amiral de Bonnivet, Louis de La Trémoille n'a en effet réalisé aucune mission diplomatique, du moins en dehors des frontières du royaume[3] et son recours au chiffre témoignerait d'une pratique encore moins cloisonnée qu'on n'a pu le penser. À l'inverse, les dépêches adressées par l'amiral de Bonnivet à Florimond Robertet – et conservées dans ce recueil – datant de l'été 1521, lorsque Bonnivet conduit l'offensive française en Navarre, des mémoires rédigés en chiffre par l'amiral constitueraient une première preuve d'un usage militaire du chiffre, bien antérieur aux premières sources jusqu'à présent identifiées[4].

---

[1] Sur la constitution et l'évolution de la charge de secrétaire d'État, voir Bernard Barbiche, *Les institutions de la monarchie française à l'époque moderne*, Presses Universitaires de France, Paris, 2012, p. 181-193. Plus spécifiquement sur le secrétariat d'État des Affaires étrangères, voir également Madeleine Haehl, « Introduction », dans *Les Affaires étrangères au temps de Richelieu : le secrétariat d'État, les agents diplomatiques (1624-1642)*, Peter Lang, Bruxelles, 2006, pp. 1-14.

[2] Bernhard Bischoff, « Übersicht über die nichtdiplomatischen Geheimschriften des Mittelalters », *Mitteilungen des Instituts für Österreichische Geschichtsforschung,* 62 (1954), pp. 1-27.

[3] Laurent Vissière, dans Cédric Michon, *Les conseillers de François Ier,* Presses Universitaires de Rennes, Rennes, 2011, pp. 131-143.

[4] L'usage militaire du chiffre reste, à ce stade de nos recherches, très marginal. Si tant l'histoire des institutions – un secrétariat d'État de la guerre se structure très tardivement (Hélène Michaud, « Aux origines du secrétariat d'État à la guerre : les règlements de 1617-1619 », *Revue d'histoire moderne et*

La seule différence entre les usages politiques et diplomatiques se situe en réalité dans la fréquence d'emploi. Le chiffre est systématique en contexte diplomatique : tous les agents disposent d'une table pour chiffrer, en cas de besoin, leur correspondance avec le pouvoir royal. D'autres tables leur sont par ailleurs octroyées, notamment pour correspondre avec les autres agents français, sans qu'il soit possible de déterminer si des tables leur étaient fournies, avant leur départ, pour correspondre avec l'ensemble de ceux-ci ou seulement certains d'entre eux ; ou encore si leur obtention intervenait en fonction des besoins, une fois à l'étranger. Néanmoins, si des tables de chiffrement sont systématiquement fournies aux ambassadeurs ordinaires et extraordinaires – et parfois changées en cours de mission en cas de suspicion –, des tables d'usage diplomatique peuvent également être conçues pour d'autres acteurs, directs ou indirects, de la diplomatie française – informateurs et pensionnaires notamment[1].

À l'inverse, dans un contexte politique, seul le besoin – et non la charge ou l'institution – donne naissance à la table de chiffrement. Les acteurs, tout comme les systèmes cryptographiques restent, eux, identiques entre usages politique et diplomatique[2]. Cette grande proximité s'avère favorisée voire renforcée par les conditions dans lesquelles les tables de chiffrement sont conçues. Si la présence au service du roi de cryptographes comme François Viète ou Antoine Rossignol est attestée – tout comme leur participation à la fois à la cryptanalyse des dépêches interceptées et probablement à la conception de tables de chiffrement –, les rédacteurs quotidiens de ces tables demeurent grandement méconnus. Il est vraisemblable que l'élaboration de celles-ci ait été réalisée ou supervisée par un clerc, puis par le premier commis du secrétaire d'État des Affaires étrangères, également en charge du chiffrement et du déchiffrement des dépêches[3]. Les inflexions observées dans les tables conçues en août 1616 – présence accrue de caractères numériques – et à l'inverse le retour aux caractères alphanumériques en avril 1617[4], soit lors de la disgrâce de Pierre Brûlart, vicomte de Puisieux, puis à son retour comme secrétaire d'État des Affaires étrangères

---

contemporaine, 1972 (19), pp. 395-411) – que des archives – le Service historique de la Défense ne conserve de fait que peu de documents antérieurs à 1630 et le seul chiffre antérieur qui y soit conservé est … d'usage diplomatique (Service historique de la Défense, GR1A6, fol. 373, table de chiffrement entre Sébastien de Juye et Gilles de Noailles, 1578) – expliquent pour partie ce silence, il paraît impensable que le nombre et l'éloignement des campagnes militaires menées tout au long du XVI^e^ siècle, et ce quelles que soient leurs conditions (présence du roi notamment), n'aient donné lieu à aucun rapport ou même billet chiffré.

[1] L'exemple le plus connu est certainement la correspondance, chiffrée, entre Henri IV et Maurice de Hesse (*Correspondance inédite de Henri IV roi de France et de Navarre avec Maurice le Savant landgrave de Hesse*, éd. C. von Rommel, Paris, 1840). Le chiffrement est maintenu après la mort de Henri IV mais utilisé beaucoup plus rarement (BnF, fr. 15927, fol. 366), témoignage évident de la confiance induite par la relation personnelle entre le landgrave et Henri IV, mais aussi de la distension des relations entre les deux pays avec l'évolution de la politique française dans l'Empire.

[2] Seule adaptation observable entre chiffres politiques et diplomatiques (en contexte étatique), les noms présents dans le nomenclateur diffèrent, ce dernier étant adapté au lieu d'envoi ou de résidence.

[3] Camille Desenclos, « Transposer pour mieux transporter : le chiffrement dans les correspondances diplomatiques du premier XVII^e^ siècle », dans Thérèse Bru, Solène de la Forest d'Armaillé (dir.), *Matière à écrire. Les échanges de correspondance du XVI^e^ au XIX^e^* siècle, Presses Universitaires de Vincennes, Paris, 2017, pp. 139-142.

[4] Dès mai 1617, Benjamin Aubéry du Maurier reprend le chiffre précédemment utilisé avec Puisieux (Claire Martin, *Mémoires de Benjamin Aubéry du Maurier : ambassadeur protestant de Louis XIII (1566-1636)*, Droz, Genève, 2010, pp. 125), tandis que Jean de Péricard, appointé comme ambassadeur en septembre 1616 voit son chiffre changer en mai 1617 (BnF, fr. 16131, fol. 57, lettre de Jean de Péricard à Pierre Brulart, vicomte de Puisieux, 30 mai 1617).

tendent à le suggérer. Cette absence de spécialisation, ou du moins l'absence de toute mention suggérant l'existence d'un « bureau du chiffre », semble être la règle pour cette première modernité, tant dans les usages que dans la conception des tables. Si le perfectionnement des systèmes cryptographiques repose sans nul doute sur une étroite collaboration avec des cryptographes, sinon de formation du moins d'expérience, la conception des tables paraît être laissée aux mêmes mains que l'écriture des dépêches destinées au chiffrement. La facilité notamment avec laquelle des tables de chiffrement sont établies pour des besoins ponctuels tendent enfin à suggérer une conception de tables de chiffrement bien plus ouverte et partagée que l'on ne pourrait le penser. Les papiers de Jacques Bongars, résident français auprès des princes protestants de l'Empire (1593-1611), contiennent en effet nombre de tables qui, au regard de la forme et de l'écriture, paraissent avoir été élaborées par Bongars lui-même. Bien que nombre de ces tables demeurent simples (nomenclateurs ou jargons), plusieurs tables, autographes et donc a priori non réalisées par le premier commis, témoignent d'une technicité proche de celle des tables produites par le secrétariat d'État[1] et d'une appropriation, aussi large que réelle, de la pratique cryptographique.

Une dernière distinction mérite enfin d'être établie, entre usages étatique, para-étatique et extra-étatique, quand bien même la conception de l'État demeure embryonnaire et explique pour beaucoup cette grande diversité d'acteurs et d'usages de la cryptographie au XVI^e^ siècle. La pratique cryptographique sort en effet rapidement du seul giron de l'État. Néanmoins, à l'image de l'instauration de représentations permanentes, les guerres de religion constituent pour ce dernier usage un miroir grossissant, sans qu'il soit possible de déterminer si elles ont fait naître un besoin nouveau ou si elles l'ont amplifié. En effet, les correspondances chiffrées les plus anciennes ne répondant pas à un besoin d'administration du royaume (affaires intérieures ou extérieures) – et à ce jour identifiées – datent de la seconde moitié de la décennie 1570[2], empêchant par-là d'observer d'éventuelles évolutions tant quantitatives que qualitatives d'un tel usage. Cette pratique extra-étatique ne s'arrête cependant pas avec les guerres de religion et tend à s'observer dès lors qu'un conflit, ouvert ou couvert, avec l'autorité royale s'observe[3]. Si elle n'a pas perdu sa vocation première de protection de l'information, la cryptographie est devenue autant une pratique politique qu'une pratique culturelle, désormais amplement partagée, des officiers royaux aux Grands du royaume[4].

S'il n'est guère étonnant que la pratique se soit diffusée au-delà de la diplomatie, probablement par l'entourage même du roi, la question du transfert des compétences techniques reste posée. Les dépêches extra-étatiques témoignent en effet d'une technicité similaire dans la pratique du chiffre : le même système cryptographique (la substitution homophonique) s'applique. *A priori* surprenant, ce recours n'est nullement le résultat d'un travail d'espionnage ou d'une fuite malencontreuse. Non seulement, tous les États européens recourent à ce même système – avec certes des spécificités –, mais rien ne vient interdire, si ce n'est le vol de tables ou de dépêches, le recours à ce système.

[1] BnF, fr. 7131, fol. 227.
[2] BnF, fr. 4717.
[3] Quelques cas de chiffre extra-étatique ont déjà été documentés, notamment pour les révoltes huguenotes du règne de Louis XIII (Jean-Robert Armogathe, « Le chiffre en péril : cryptographie et double langage au XVII^e^ siècle », *Comptes rendus des séances de l'Académie des inscriptions et Belles-Lettres,* 158-2 (2014), pp. 929).
[4] Une majeure partie des sources extra-étatiques chiffrées, à ce jour retrouvées, pour la fin du XVI^e^ siècle émanent en effet du duc de Nevers.

De fait, nombre de cryptographes ou concepteurs de tables sont probablement au service simultané de plusieurs princes.

Cette utilisation du chiffre, dans un contexte extra-étatique, va néanmoins au-delà de la simple mobilisation du système de substitution homophonique. Les tables de chiffrement présentent un degré de perfectionnement similaire au chiffre diplomatique de la même époque[1] et aucune erreur majeure dans l'écriture du chiffre ne s'observe. La principale différence entre les chiffres étatiques et extra-étatiques ne tient pas en réalité pas à leur technicité mais à leurs conditions de production : le chiffre diplomatique peut et doit être uniforme. Produites par un même bureau, dans un même objectif, les tables diplomatiques reposent sur les mêmes mécanismes, allant jusqu'à réutiliser des tables anciennes ou encore en usage[2]. À l'inverse, il y a autant de chiffres extra-étatiques que d'utilisateurs et de besoins. La pratique cryptographique ne se conçoit en effet pas en termes de nouveauté, ou même de technicité, mais en termes de performance. Le chiffre extra-étatique est donc simplement adapté à des besoins conjoncturels et ne reposant sur aucune permanence institutionnelle, d'où les importantes fluctuations observées dans la qualité des tables. Tous les utilisateurs du chiffre ne disposent pas nécessairement de cryptographes à demeure, prompts à produire régulièrement de nouvelles tables ; mais toute table, même conçue à la hâte, peut répondre au besoin d'immédiateté né d'un conflit, à condition d'être régulièrement modifiée.

Un perfectionnement technique du chiffre

Contrairement à l'idée commune, la pratique cryptographique française est, dès son essor au début du XVI^e^ siècle, déjà bien loin des antiques systèmes de transposition. Ainsi, l'une des plus anciennes dépêches retrouvées à ce jour, celle de Louis de Solliès adressée à Florimond Robertet[3], présente déjà un système de substitution mono-alphabétique : chaque lettre de l'alphabet est remplacée par un signe cryptographique. Néanmoins, la technicité demeure faible : le nombre de caractères correspond au nombre de lettres dans le texte en clair et chaque lettre est systématiquement remplacée par le même caractère ; seuls quelques rares mots codiques – un mot est représenté par un seul caractère cryptographique – viennent freiner l'analyse des fréquences et donc la cryptanalyse. Moins avancé que ses voisins méridionaux, le royaume de France voit de fait ses dépêches régulièrement décryptées dans la première moitié du XVI^e^ siècle[4].

Néanmoins, si l'étude des pratiques cryptographiques peut s'appuyer sur un imposant corpus de dépêches et de mémoires chiffrés, la cryptanalyse demeure dans l'ombre. Sa nature la contraint plus encore au secret – l'avantage obtenu ne peut être conservé que si le décryptage demeure insoupçonné – et ne donne lieu à aucune production documentaire distincte. Rien ne peut venir distinguer une dépêche déchiffrée d'une dépêche décryptée, et compte tenu des modalités de constitution des fonds,

[1] Voir notamment BnF, fr. 3995, fol. 14, table de chiffrement utilisée entre le duc et la duchesse de Nevers, 1585.

[2] Camille Desenclos, *Les mots du pouvoir : la communication politique de la France dans le Saint-Empire au début de la guerre de Trente Ans (1617-1624),* thèse de doctorat, École nationale des chartes, 2014, t. 1, pp. 304-305.

[3] BnF, Dupuy 261, fol. 121.

[4] Nicole Lemaitre, « La correspondance diplomatique de la Renaissance comme document historique ? Les lettres de Georges de Selve, ambassadeur à Rome (1537-1538) », dans Bernadette Cabouret (dir.), *La communication littéraire et ses outils : écrits publics, écrits privés,* Éditions du CTHS, Paris, 2018, pp. 101.

notamment pour le XVI^e siècle, la présence de dépêches étrangères, ou de langue étrangère, ne constitue nullement un indice fiable. À l'inverse, la présence de certains recueils de dépêches, nommément identifiées comme interceptées et décryptées – à l'image du *Livre de plusieurs lettres quy ont esté surprises pendant la ligue du roy d'Espagne Phelippe second*[1] –, constituent des preuves d'une activité de cryptanalyse par le pouvoir royal français. Ces rares mentions d'un décryptage, par ailleurs toujours silencieuses sur l'auteur de la cryptanalyse, se retrouvent cependant majoritairement sur des documents produits, et interceptés, pendant la Ligue et passent sous silence des pratiques, peut-être plus quotidiennes, notamment autour de correspondances diplomatiques.

Quelle que soit l'ampleur des pratiques françaises en la matière, la menace que fait peser les interceptions et tentatives de cryptanalyse adverses conduit à une transformation majeure du système cryptographique, passant de la substitution mono-alphabétique à la substitution homophonique. Pour éviter que le chiffre ne puisse être cassé par une simple analyse des fréquences – les caractères les plus fréquents correspondraient aux lettres les plus fréquentes dans la langue utilisée –, plusieurs caractères cryptographiques sont attribués à une même lettre. Plus la lettre sera fréquente, plus le nombre de caractères cryptographiques sera élevé. Par ailleurs, des caractères dépourvus de valeur – ou à l'inverse permettant le redoublement d'un caractère (voire son annulation) – sont introduits pour empêcher plus encore l'analyse des fréquences en cas d'interception des dépêches. Enfin, la généralisation de nomenclateurs vient compléter ce dispositif, tout en écourtant et simplifiant le temps d'écriture[2].

Parallèlement, le recours accru au chiffre conduit au perfectionnement des pratiques cryptographiques, notamment le choix des caractères afin de faciliter et accélérer l'écriture du chiffre. Les caractères présents dans la dépêche de Louis de Solliès prennent en effet majoritairement l'apparence de symboles (carré, triangle inversé, astérisque, etc.), particulièrement délicats à former. Au fil du XVI^e siècle, les caractères cryptographiques se rationalisent donc à la fois pour faciliter l'écriture, le déchiffrement et rendre le chiffre moins visible en cas d'interception et d'ouverture des dépêches. Alors que les symboles sont majoritaires dans la première moitié du XVI^e siècle, ils s'effacent ainsi devant des caractères latins et grecs, d'abord modifiés puis simples, puis devant des nombres[3].

Ces évolutions demeurent pourtant bien éloignées des systèmes complexes développés par les cryptographes et, jusqu'au milieu du XVII^e siècle, science et pratique cryptographique évoluent parallèlement[4] sans se rejoindre autrement que par le biais de quelques acteurs communs[5]. S'appuyant notamment sur le système établi par Leon

---

[1] BnF, fr. 3941.

[2] Camille Desenclos, « Écrire le secret quotidien. Pratiques de la cryptographie au sein de la diplomatie française (XVI^e siècle – premier XVII^e siècle) », dans *Spies, espionnage and secret diplomacy in the early modern period*, dir. G. Braun, S. Lachenicht, Stuttgart : Kohlhammer, 2021, pp. 85-103.

[3] Sur l'évolution des caractères cryptographiques aux XVI^e et XVII^e siècles, voir *ibid.*

[4] Sur l'écart entre science et pratique cryptographique à l'époque moderne, voir notamment Benedekt Lang, « Real-Life Cryptology : Enciphering Practice in Early Modern Hungary », dans Katherine Ellison, Susan Kim, *A Material History of Medieval and Early Modern Ciphers. Cryptography and the History of Literacy,* Routledge, New York, 2018, pp. 223-240.

[5] Auteur d'un *Traicté des chiffres ou secretes manieres d'escrire* (Paris, 1586), Blaise de Vigenère est aussi au service du duc de Nevers (Ariane Boltanski, *Les ducs de Nevers et l'État royal. Genèse d'un compromis (ca 1550 – ca 1600),* Droz, Genève, 2006, pp. 308-322) et, bien que son activité la plus connue soit littéraire,

Battista Alberti[1], la science cryptographique ne cesse de se perfectionner avec l'invention de la substitution double de Giambattista della Porta[2], perfectionnée ensuite par Blaise de Vigenère[3], qui ne s'appuie plus sur des caractères cryptographiques mais sur un double alphabet que l'on combine grâce à un mot-clé. Ces systèmes sont évidemment plus sûrs que la substitution homophonique ; ils ne sont pourtant pas utilisés, en raison de leur plus grande complexité et de la lenteur d'écriture à laquelle ils contraignent[4]. Quelle que soit la qualité des concepteurs des tables de chiffrement, leurs utilisateurs ne sont ni cryptographes ni même diplomates ou militaires de carrière[5]. L'usage ne peut donc être technique, y compris dans un contexte diplomatique, et ce d'autant plus que l'absence de spécialisation entre usage politique et diplomatique demeure pendant une majeure partie de l'époque moderne. Certes, certains agents diplomatiques peuvent s'appuyer sur un secrétaire d'ambassade ; cette assistance demeure cependant réservée aux seuls ambassadeurs et, pas plus que pour ces derniers, l'expérience, et la recommandation, ne constituent le mode privilégié de recrutement, bien devant leur éventuelle habileté avec le chiffre. Celui-ci doit donc pouvoir être utilisé et manipulé sans difficulté par tous. L'information doit être transmise rapidement et ne peut donc supporter un temps de chiffrement et de déchiffrement trop long, d'où le recours à des systèmes facilement maniables par les agents, notamment les résidents qui doivent chiffrer eux-mêmes leurs dépêches. Sans cesse plus utilisée, la cryptographie demeure hors des sphères mathématiques. De fait, si un perfectionnement s'observe bien, celui-ci porte sur un seul et même procédé, la substitution homophonique ou substitution à représentations multiples, mobilisée dans la très grande majorité des sources cryptographiques jusqu'au milieu du XVIIe siècle et l'introduction des systèmes à répertoire, dont le plus connu reste à ce jour le Grand Chiffre conçu par Antoine Rossignol.

Cette rapidité d'écriture progressivement induite par le perfectionnement du système de substitution homophonique n'entraîne pourtant pas une multiplication du recours au chiffre. En 1535, George de Selve, ambassadeur à Venise, chiffre déjà 70 % des dépêches qu'il adresse au cardinal du Bellay, alors à Rome[6]. Le progrès est intangible : il accélère le temps d'écriture et ralentit le temps de décryptage. Les fréquences

---

voire apologétique, il est fort probable qu'il ait également contribué à l'élaboration des tables de chiffrement pour le duc. Inversement, Charles Brulart de Léon rédige un *Traicté des chiffres* (BnF, fr. 17538, fol. 48sq, v. 1630) à partir de son expérience diplomatique antérieure. Si certains conseils peuvent s'appliquer à la pratique, les systèmes cryptographiques présentés (notamment sous forme de roue) demeurent inappliqués.

[1] Leon Battista Alberti, *De componendis cifris*, Venise, 1568. Sur le traité d'Alberti, voir notamment Nella Bianchi Bensimon, « Le *De componendis cifris* de Leon Battista Alberti », dans Bernard Darbord, Agnès Delage (dir.), *Le partage du secret. Cultures du dévoilement et de l'occultation en Europe, du Moyen Âge à l'époque moderne,* Armand Colin, Paris, 2013, pp. 227-238.

[2] Giambattista della Porta, *De Furtivis literarum notis vulgo de ziferis,* Naples, 1563.

[3] Blaise de Vigenère, *Traité des chiffres ou secretes manieres d'ecrire*, Abel Langelier, Paris, 1586.

[4] Seules deux tables s'appuyant sur le système, simplifié, de Vigenère ont été retrouvées à ce jour : BnF, fr. 4724, fol. 136, « Chiffre baillé par le Père François Ybernois », v. 1620 ; BnF, fr. 4725, fol. 68, « Chiffre donné par M. Simon », v. 1610.

[5] La question de la professionnalisation ou du moins spécialisation des diplomates a fait l'objet de nombreuses études (voir notamment Indravati Félicité (dir.), *L'identité du diplomate (Moyen Âge – XIX^e siècle). Métier ou noble loisir ?*, Garnier, Paris, 2020). En l'absence de toute formation dédiée avant le début du XVIII^e siècle, les critères présidant au choix d'un agent diplomatique pour une mission reposent majoritairement sur l'expérience, les capacités de négociation, les qualités curiales et, pour certains postes, un goût des langues ou un certain statut nobiliaire.

[6] BnF, Dupuy 265.

pourtant demeurent variables tout au long du XVI^e^ siècle[1] et rappellent le rôle du chiffre dans la pratique épistolaire, qu'elle soit politique ou diplomatique : une réponse à un besoin conjoncturel et non un outil structurel dont il convient de se saisir à tout prix. L'existence ponctuelle ou régulière de chiffrement à l'échelle d'une correspondance ou même l'absence de tout chiffrement ne constituent en cela pas des solides preuves pour juger de l'appropriation de la pratique cryptographique par une institution ou par une catégorie sociale. Le recours au chiffre demeure le résultat d'un choix, conscient, de l'épistolier pour protéger sa dépêche en fonction d'un contexte donné[2]. Ni à l'échelle d'une correspondance ni à celle d'une dépêche, le chiffrement systématique n'est donc la règle. L'absence du recours systématique au chiffrement intégral peut néanmoins paraître étonnante. Une protection idoine des documents, dépêches ou mémoires, envoyés tendrait en effet vers un chiffrement intégral. La seule présence d'une signature, d'une date, d'une adresse fournit déjà de nombreuses informations à un cryptanalyste, notamment la langue utilisée et le contexte d'écriture pas – et donc les noms et sujets principaux pouvant être mentionnés dans la dépêche. Pourtant, seule une infime minorité de documents chiffrés, souvent des mémoires, ne présentent aucune de ces informations. Si la conservation lacunaire des correspondances fausse peut-être la proportion totale de ces documents intégralement chiffrés dans la masse initialement produite, elle permet surtout d'estimer plus précisément le degré de protection attendu des dépêches. Il s'agit moins d'empêcher toute tentative de cryptanalyse – les systèmes cryptographiques demeurent trop faibles pour cela – que de les ralentir, sans trop entraver le travail d'écriture et de lecture. Dès lors que le chiffrement est suffisamment conséquent pour empêcher que le contenu soit simplement deviné par déduction, le degré de protection attendu est atteint.

*

Le chiffre constitue, au début de l'époque moderne, une protection temporaire et non définitive. Aucun chiffrement ne tend à s'observer dès lors qu'il n'y a pas besoin de transmettre une information à un tiers, quelle que soit sa distance physique ou politique. Il sert à protéger l'information le temps de sa transmission, mais non au-delà. De fait, la présence régulière d'un déchiffrement, interlinéaire ou marginal, directement inscrit sur la dépêche chiffrée originale, confirme cette temporalité limitée de la protection recherchée par le recours au chiffre. Dès lors que la transmission est assurée, la maniabilité de l'information prédomine, notamment par le biais d'une lecture plus aisée du contenu de la dépêche en cas d'alternances de passages en clair et chiffrés. Rien ne vient donc protéger le document une fois reçu, si ce n'est la destruction volontaire[3].

[1] Une première analyse des fréquences cryptographiques dans les correspondances diplomatiques de la première modernité a déjà été réalisée dans Camille Desenclos, « Écrire le secret quotidien… », *op.cit*.

[2] Dans certains cas, le recours au chiffre est également conditionné par des contraintes matérielles. Bien que relativement peu technique, le chiffre demeure long à écrire, nécessitant de passer par plusieurs phases de brouillon. Certains diplomates se justifient ainsi de ne pas recourir au chiffre par manque de temps (Camille Desenclos, « Transposer pour mieux transporter … », *op.cit.,* pp. 134-135).

[3] De nombreux mémoires et dépêches nous sont parvenus sans déchiffrement. Il n'est néanmoins pas certain que cette absence soit liée à une volonté consciente de protéger le contenu du document. Le déchiffrement pouvant être reporté certes en interligne ou en marge mais également sur un feuillet

Si les épistoliers requièrent occasionnellement que leur dépêche soit détruite après lecture[1], le simple fait que nous ayons connaissance de cette requête témoigne du non-respect de cette consigne et interroge quant à la mise à exécution de semblables demandes. Bien que la conservation parfois intégrale de certaines correspondances diplomatiques chiffrées puisse constituer un premier élément de réponse, les modalités de constitution des fonds diplomatiques comme politiques freinent considérablement l'analyse de cette pratique, dans la mesure où il est impossible d'identifier avec certitude l'origine de certaines lacunes, comme par ailleurs d'estimer finement les fréquences de recours au chiffre. La conservation d'une typologie documentaire qui, elle, devait être systématiquement détruite après usage – la table de chiffrement – suggère néanmoins une faible attention accordée au chiffre, dès lors que celui-ci a fait l'office recherché – protéger la transmission – et ce d'autant plus facilement que le système cryptographique étant partagé, jusqu'au milieu du XVII^{e} siècle, par la majorité des États européens, l'éventuel dévoilement d'une table de chiffrement, désormais inutilisée, ne constituerait nullement un danger pour la sécurité des futures dépêches chiffrées.

Camille Desenclos

distinct, notamment dans le cas de documents intégralement chiffrés, l'inviolabilité de ces documents peut devoir à une simple perte, au gré des recompositions des fonds et collections, desdits feuillets.

[1] Dès le Moyen Âge, la destruction volontaire d'une dépêche après lecture s'observe ; elle vient cependant en remplacement du chiffre, encore exceptionnel dans sa pratique (Stéphane Péquignot, *Au nom du roi. Pratique diplomatique et pouvoir durant le règne de Jacques II d'Aragon (1291-1327),* Casa de Velazquez, Madrid, 2009, pp. 118). Cette pratique perdure néanmoins à l'époque moderne, après la généralisation de l'usage du chiffre (Jean-Marie Ribera, *Diplomatie et espionnage : les ambassadeurs du roi de France auprès de Philippe II,* Honoré Champion, Paris, 2007, pp. 389-390).