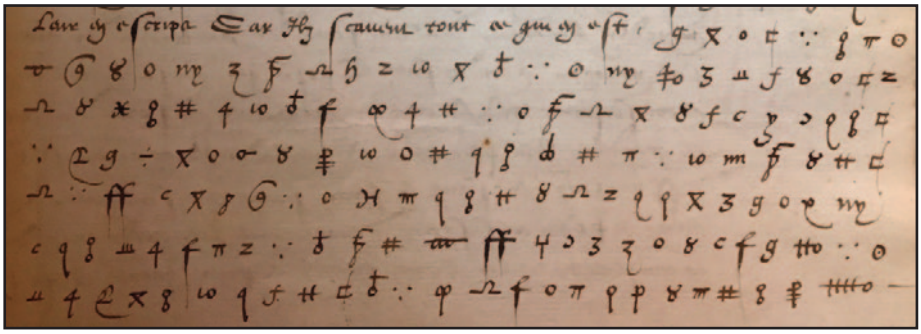
Naissance et essor de la cryptographie en France, XVI^e^-XVII^e^ siècles

Camille Desenclos[1]

Bien que sur un sujet classique pour des cryptologues, la conférence de Camille Desenclos, maître de conférences à l'université de Haute Alsace, était originale par son angle de vue. Son but essentiel n'était pas d'étudier la technique cryptographique en elle-même mais son éventuelle valeur politique. Faut-il voir dans le chiffre une simple forme technique de sécurisation de l'information, au perfectionnement constant, ou au contraire une coconstruction commune entre l'information politique et son support scriptural ?



Une dépêche chiffrée de la collection de la BNF

Pour répondre à cette question, il fallait se confronter aux sources cryptographiques elles-mêmes, non les traités théoriques, non les sources les plus connues aux pratiques aussi exceptionnelles que leurs rédacteurs, mais à la multitude de ces lettres chiffrées quotidiennement par les commis des secrétaires d'État, par les diplomates, mais aussi par tous ces nobles en rébellion contre leur souverain. Tel est le projet de recherche de Camille Desenclos, qui a reçu le soutien de la Bibliothèque Nationale de France, lieu où se trouvent ces archives car, jusqu'à l'arrivée de Richelieu au pouvoir en 1624, à quelques exceptions près, les archives étatiques, quel que soit par ailleurs le ministère à l'origine de leur production, ne sont pas conservées dans des services d'archives, mais à la Bibliothèque nationale en tant que papiers privés.

Compte tenu de l'extraordinaire richesse des collections de cette institution, toutes les sources cryptographiques ne sont pas inventoriées. Pour les collections les plus anciennes, des descriptions précises, parfois à la lettre, existent. Rarement cependant elles précisent si les lettres sont chiffrées, encore moins s'il existe un dé-

[1] Ce résumé de la conférence de Camille Desenclos a été rédigé par Hervé Lehning.

chiffrement pour ces mêmes lettres ; l'identification des tables de chiffrement est elle aussi aléatoire. En effet, pour nombre de dépêches, les tables de chiffrement existent encore. Alors qu'elles devaient pourtant être systématiquement détruites à l'issue de la correspondance, elles ont régulièrement été conservées, y compris par les services diplomatiques, et constituent aujourd'hui les sources les plus fiables afin d'accéder au contenu de dépêches non encore déchiffrées ou dont le déchiffrement aurait été perdu. Seul problème, ces tables se trouvent rarement dans le même manuscrit que les dépêches qu'elles ont permis de chiffrer. De nombreuses lettres ne peuvent donc être lues alors que les sources permettant de le faire existent.

Le vocabulaire utilisé pour décrire ces documents pose aussi problème. Au mieux, celles-ci sont désignées comme « clef », voire comme « table », mais le plus souvent, elles sont simplement qualifiées de chiffres, sans donc qu'une distinction entre table et lettre chiffrée puisse être effectuée à la seule lecture du catalogue. Ce problème n'est pas dû à la Bibliothèque nationale, mais à l'absence totale de normalisation du vocabulaire d'époque pour qualifier le chiffre. Outre les sources elles-mêmes, ce projet de recherche a obligé Camille Desenclos à réfléchir au vocabulaire moderne du Chiffre, ne serait-ce que pour décrire ensuite les sources cryptographiques ainsi recensées et identifiées. Ce vocabulaire se trouve souvent en marge ou en dos des documents, souvent des tables de chiffrement, pour identifier celle-ci, notamment dans le cadre d'un envoi postal. Une sémantique du chiffre s'est rapidement détachée autour de cinq termes : jargon, chiffre, clef, déchiffre et table.

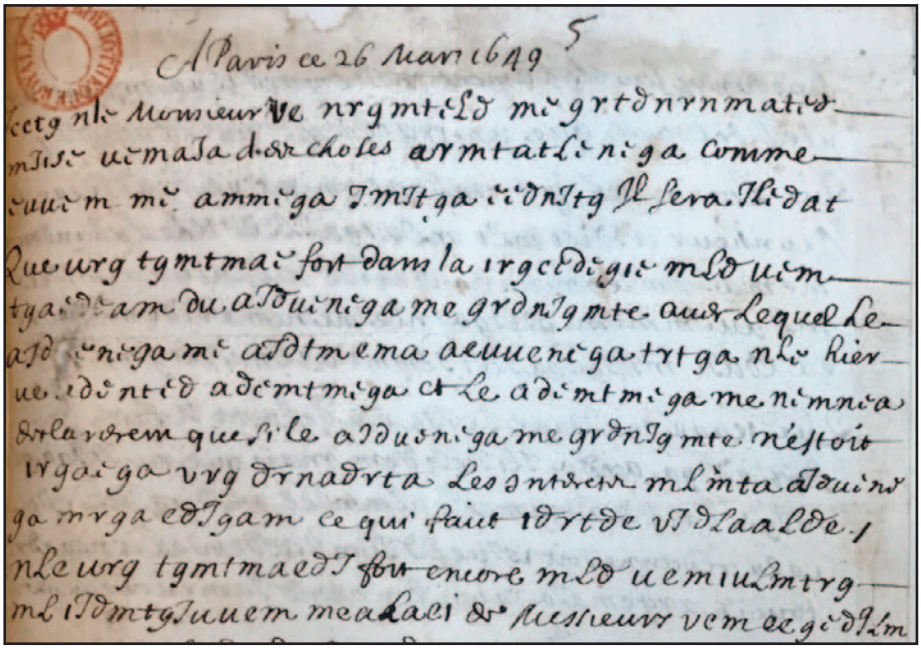
Le terme de « jargon » fait directement référence à une pratique d'époque, peu recommandée depuis en raison de la protection relative ainsi offerte à l'information. Jamais un jargon n'a été désigné sous un autre terme dans les mentions apposées au dos des documents. À l'inverse, le terme de chiffre est utilisé de manière bien plus lâche. Si le terme « chiffre » est le plus régulièrement utilisé pour désigner les tables de chiffrement, il se retrouve parfois au dos de mémoires intégralement chiffrés. La confusion tient à l'utilisation concomitante de « en chiffre ». Si le verbe déchiffrer est utilisé par les contemporains, le verbe chiffrer l'est bien moins. Mais, trouver une normalité dans les usages sémantiques autour du chiffre est une gageure à divers niveaux : les mentions marginales n'indiquent jamais la nature ou la typologie du document, par exemple table. Le plus souvent, les tables de chiffrement, envoyées en guise de pièce jointe ou remises en main propre, ne contiennent aucune indication au dos, ou tout au plus le nom du destinataire. Le terme de « table » surtout est une projection contemporaine, fort commode néanmoins pour mieux distinguer, à des fins d'études : documents chiffrés, jargons, tables de chiffrement et tables de déchiffrement, mais ne correspond à aucune réalité de l'époque et explique la difficulté à identifier dans les collections les sources cryptographiques.

Ce problème sémantique néanmoins ne se pose que pour une partie des collections de la Bibliothèque nationale. Les autres collections, présentes au sein du département des Manuscrits, ne sont en effet que brièvement décrites, par exemple « *Relations diplomatiques et militaires entre la France et l'Allemagne, années 1617-1618* », sans jamais recourir à un vocabulaire cryptographique, normalisé ou non. À

la lecture des catalogues et bases de données, on n'a donc aucun moyen de connaître le contenu exact de ces précieux manuscrits. Pourtant, l'exemple tout juste mentionné désigne en réalité un manuscrit regroupant l'ensemble de la correspondance diplomatique envoyé par les agents français présents en Allemagne au roi de France et au secrétaire d'État, plusieurs dizaines de lettres chiffrées s'y trouvent donc. Une grande partie des sources cryptographiques, au sens de lettres chiffrées, des XVI^e^ et début du XVII^e^ siècle nous demeurait scellée, avant la mise en projet.

La première phase du projet de Camille Desenclos consiste donc en un repérage et un recensement exhaustif de l'ensemble des tables de chiffrement et dépêches chiffrées conservées au département des Manuscrits. L'objectif est à terme de regrouper en une même ressource, en l'occurrence un guide méthodologique (qui fera l'objet d'une publication papier, dans toutes les bonnes librairies), l'ensemble des éléments descriptifs afin de faciliter l'étude de ces sources. Parallèlement également, Camille Desenclos participe à une amélioration de certaines notices, décrivant des ressources cryptographiques, de la Bibliothèque nationale pour rendre ces sources accessibles avant l'achèvement de ce projet de recherche.

Par ailleurs, son travail concerne uniquement les tables et les lettres originales présentant un chiffre, avec déchiffrement ou non, sans critère de langue, nombre de lettres du XVI^e^ siècle étant en latin en raison des liens forts du royaume de France avec le Nord de la péninsule italienne. Naturellement, si un traité non édité venait à être identifié, il ne serait pas exclu, comme cela a été le cas pour le « *Traité des chiffres et la manière dont s'en servir pour le secret de l'Estat* » de Charles Brulart de Léon, traité



Document où les parties chiffrées peuvent passer inaperçues

manuscrit rédigé à la fin des années 1620, unique exemplaire trouvé à ce jour et que Camille Desenclos espère avoir le temps prochainement d'éditer intégralement. Cependant, l'histoire de la cryptographie théorique n'est pas au cœur de son projet, contrairement à la pratique cryptographique.

Depuis 2015 et le début de ce projet, Camille Desenclos dépouille systématiquement l'ensemble des manuscrits présents à la Bibliothèque nationale et susceptibles de contenir des matériaux chiffrés, à savoir les manuscrits contenant des documents originaux. Au sein de ces manuscrits, repérer les lettres chiffrées n'est pas toujours aisé, les tables se distinguent d'elles-mêmes par leur mise en forme particulière. Souvent, la présence de caractères cryptographiques est rapidement visible : des nombres ou encore des caractères grecs se distinguent de nos caractères latins. Plus encore, la présence d'un déchiffrement en marge ou en interligne, comme il était souvent de coutume pour faciliter la lecture du contenu de la lettre, très rarement intégralement chiffrée, attire également rapidement l'œil. Cette visibilité du chiffre néanmoins n'est pas toujours aussi évidente, ce qui s'explique par les besoins initiaux de protection. Lors de l'ouverture d'une lettre, notamment par des services adverses, la présence de caractères cryptographiques indiquait immédiatement la haute valeur du contenu de la lettre interceptée.

En conclusion, cette conférence nous a convaincus que Camille Desenclos serait une bonne recrue pour notre association à laquelle elle apporterait une vision différente de la cryptologie.

Jean-Louis Desvignes remercie Camille Desenclos