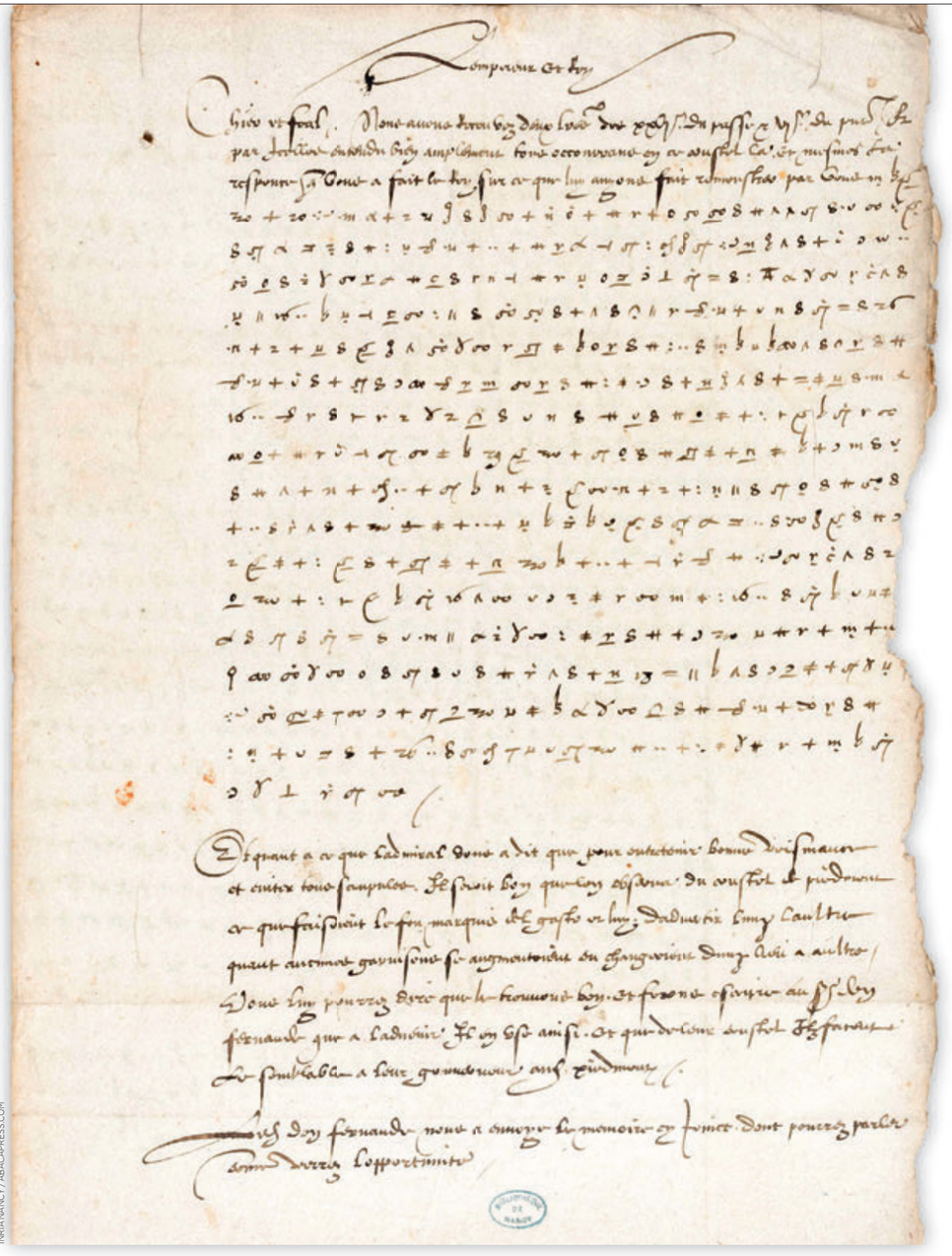


INRIA NANCY / ABACAPRESS.COM

La missive, rédigée en 1547 par Charles Quint et adressée à son ambassadeur auprès du roi de France, comporte quelques passages en clair et de longues séquences chiffrées.

Cryptographie

La correspondance codée de Charles Quint n'a plus de secrets

Une coopération entre cryptographes, informaticiens et historiens a permis de lever le voile sur une lettre « codée » du XVIe siècle. Un système de chiffrement complexe qui permettait à l'empereur de communiquer notamment avec son ambassadeur auprès de François 1er, son ennemi le plus redoutable.

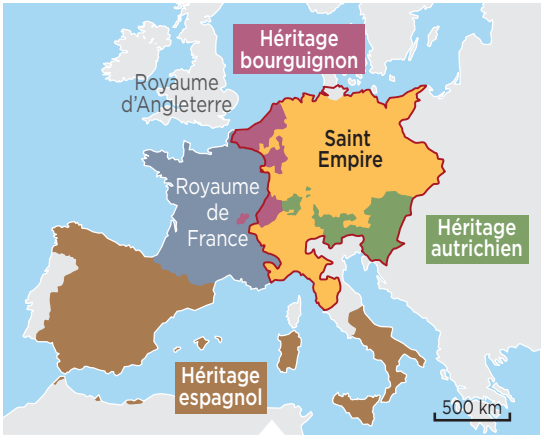
Par Marine Benoit @marin_eben

Lorsqu'un matin de décembre 2021, Cécile Pierrot découvre les pages brunâtres et couvertes de symboles, l'émerveillement la saisit : « *À ce moment-là, je réalise que non seulement la lettre existe bel et bien, mais qu'elle est aussi dans un état de conservation exceptionnel.* » Cette lettre, il s'agit de celle adressée le 22 février 1547 par Charles Quint à son ambassadeur en France Jean de Saint-Mauris. La missive a deux particularités : elle est écrite dans un langage codé et semble avoir totalement échappé aux historiens durant près de cinq siècles, au point qu'il soit tentant de se demander si, sans la détermination de Cécile Pierrot, chercheuse en cryptographie au Laboratoire lorrain de recherche en informatique et ses applications (Loria/université de Lorraine), elle ne serait pas encore restée plusieurs siècles au fond d'un tiroir. Le début de l'aventure autour de cette lettre historique se situe en 2019, lorsqu'au cours d'une soirée, une connaissance parle à Cécile Pierrot d'une « *mystérieuse lettre chiffrée signée de la main de Charles Quint* ». Après une rapide recherche sur Internet, la cryptographe ne trouve nulle trace du document et en déduit que son existence est une légende. Mais voilà que deux ans plus tard, la scène se répète. « *On évoque à nouveau cette lettre au cours d'un dîner. Mais cette fois, la personne n'en a pas seulement entendu parler,* raconte la chercheuse, *elle l'a vue de ses propres yeux, à Nancy.* » Problème : ce témoin précieux ne sait plus où il l'a aperçue. Cécile Pierrot convainc alors sa colocataire, employée au musée des Beaux-Arts nancéien, de mener l'enquête. Par un jeu de bouche-à-oreille, l'amie remplit sa mission : elle établit que la lettre repose sur une étagère du fonds des autographes de la bibliothèque Stanislas. Pourquoi là-bas ? « *Nul ne le sait,* répond la chercheuse. *On ignore aussi depuis quand elle s'y* ▸

CONTEXTE

Un empire menacé par les princes luthériens

Depuis 1494, les guerres d'Italie voient s'affronter rois de France et rois d'Espagne. Néanmoins, des périodes de trêves rythment les campagnes militaires. Le moment où Charles Quint écrit sa lettre à Jean Saint-Mauris s'inscrit dans l'une de ces périodes de « calme avant la tempête ». Le souverain européen le plus puissant de la première moitié du XVIe siècle, dernier monarque à entretenir le fantasme d'un « empire chrétien unifié », est en février 1547 très préoccupé par une rébellion des princes allemands luthériens dirigée par Jean-Frédéric de Saxe et désignée sous le vocable de ligue de Smalkalde, du nom de la ville où princes et villes ont conclu leur alliance. Ceux-ci réclament la reconnaissance du luthérianisme, interdit en vertu de l'édit de Worms de 1521, et sont soutenus par François 1er, ennemi de toujours de Charles Quint. À peine un mois après la rédaction de la lettre, le roi de France meurt et cède son trône à son fils Henri II.



BRUNO BOURGEOIS

La domination européenne de Charles Quint s'est constituée à la suite de trois successions dynastiques et de son élection à la tête du Saint Empire en 1519.

trouve. Elle n'a même pas de cote [référence qui permet de retrouver un document dans une bibliothèque]. » Quoi qu'il en soit, Cécile Pierrot se tient quelques semaines plus tard face au délicat document, prête à relever le défi : découvrir ce que l'empereur du Saint Empire romain germanique avait de si secret à dire à son représentant dans le royaume de son grand rival, François 1er.

« *En voyant la lettre écrite sur pas moins de trois pages, complète et parfaitement lisible, et en partant du principe que celle-ci a été rédigée à la Renaissance, une période précoce pour la cryptographie, j'ai d'abord pensé que j'allais la déchiffrer en quelques heures, deux jours tout au plus.* » Présomption de cryptographe moderne ! Cécile Pierrot confesse en riant qu'il lui faudra plusieurs mois pour en venir à bout. « *Le système de chiffrement était bien plus complexe que je ne l'avais imaginé.* » La mathématicienne découvre en effet que le texte compte plus d'une centaine de symboles, ce qui écarte d'emblée le fait qu'un symbole puisse correspondre à une lettre de l'alphabet. De plus amples recherches lui confirment justement que la mode cryptographique de l'époque consiste à attribuer un symbole à des bigrammes ou à des trigrammes, autrement dit à des assemblages de deux ou trois signes — généralement des lettres de l'alphabet —, formant eux-mêmes un phonème.

Mais ce n'est pas tout : elle découvre que Charles Quint était un adepte des symboles « nuls », c'est-à-dire qui ne correspondent à rien et qui n'ont d'autre fonction que d'embrouiller le lecteur. Face à cette complexité, Cécile Pierrot encode la lettre entière en Python, un langage informatique qui lui permet de réaliser de premières analyses statistiques. De cette manière, la chercheuse peut établir la fréquence des symboles, mais aussi comparer le texte avec un autre de la même époque, traduit également en Python. En l'occurrence avec *Pantagruel*, publié par Rabelais en 1532. Mais au bout de quarante-huit heures, l'ordinateur est à la peine. Et la chercheuse de conclure alors que la puissance de calcul ne lui permettra pas d'aboutir en un temps raisonnable.

Un bond de géant après quatre mois de tâtonnement

« *Il allait falloir faire les choses à l'ancienne. J'ai donc appelé des collègues pour leur demander de jouer avec moi* », plaisante la jeune femme. Ainsi débarquent dans la partie deux autres chercheurs en informatique du Loria, Paul Zimmermann et Pierrick Gaudry, spécialistes de la factorisation des nombres entiers. De février à juin 2022, tous trois avancent à petits pas, entre observations à l'œil nu et réponses obtenues grâce à l'ordinateur. Ils voient notamment des motifs apparaître : trois ou quatre symboles d'affilée se répètent plusieurs fois et, à deux endroits, pas moins de 11 symboles sont alignés dans le même ordre, signe qu'ils tiennent sans doute là un mot entier. « *Malgré tout, nous n'arrivions pas à don-*


CEDRIC JACQUOT/MAXPPP

« En voyant la lettre, complète et parfaitement lisible, j'ai pensé que j'allais la déchiffrer en quelques heures, deux jours tout au plus »

Cécile Pierrot, chercheuse en cryptographie au Loria (CNRS-université de Lorraine), à Nancy

ERIC VANDEVILLE / AKG IMAGES

Le roi François Ier et l'empereur Charles Quint signent un traité le 18 juin 1538, appelé la paix de Nice, mettant fin à la huitième guerre d'Italie et instaurant une trêve de dix ans entre les deux belligérants, après vingt-cinq années d'affrontements.

ner du sens à ce que l'on voyait, même en ayant quelques certitudes », se rappelle Cécile Pierrot. « *Après quatre mois à tâtonner, nous avons estimé qu'il nous fallait un coup de pouce dans un domaine que nous ne maîtrisions pas et qui pourrait peut-être nous mettre sur de nouvelles pistes.* » Ils contactent alors Camille Desenclos, historienne à l'université de Picardie Jules-Verne et spécialiste des relations entre la France et le Saint Empire. Par un heureux hasard, il se trouve que l'experte mène justement un projet d'étude sur l'essor de la cryptographie dans la France des XVIe et XVIIe siècles. Toutefois, la sollicitation est une première pour elle : « *Je suis régulièrement approchée par des amateurs mais jamais par des chercheurs en cryptographie,* confesse-t-elle. *J'étais donc ravie de me lancer dans cette collaboration inédite.* » Camille Desenclos donne aux cryptographes l'information qui leur manquait : il existe à la bibliothèque municipale de Besançon plusieurs dépêches codées de Charles Quint dont le déchiffrement, c'est-à-dire la « traduction » des symboles cryptographiques en clair, fut établi dans la marge au moment de leur réception par leur destinataire. « *À ce moment-là, on fait un bond de géant* », raconte Cécile Pierrot. Car même si des symboles diffèrent entre les courriers, leur méthode de chiffrement est la même. En quelques jours seulement, les chercheurs parviennent alors à reconstituer l'essentiel du système. « *La méthode de Charles Quint est en réalité assez traditionnelle pour le milieu de XVIe siècle* », affirme Camille Desenclos. Mais cette dernière présente une spécificité méconnue que la dépêche de Nancy est l'occasion d'étudier : les voyelles sont figurées par un simple point autour des consonnes, les faisant disparaître un peu à la manière de l'arabe. « *C'est ce qui a rendu la tâche des cryptographes si compliquée.* »

Les pièces du puzzle finissent par s'assembler

Reste quelques mystères à éclaircir, comme une poignée de symboles isolés. Il y a notamment cette « épingle » *(lire l'encadré p. 86)*, qui apparaît à la fin d'une phrase entièrement chiffrée dans laquelle Charles Quint interroge son ambassadeur sur les intentions du roi de France depuis que celui-ci a appris le trépas de la personne désignée par ledit symbole. Cécile Pierrot a l'intuition qu'il s'agit d'un monarque, puisque l'épingle ressemble beaucoup au symbole désignant un roi dans d'autres lettres de Jean Saint-Mauris. Pourtant, Camille Desenclos est formelle : aucun roi n'est mort en janvier ou février 1546, date qui figure au bas de la lettre. « *Après réflexion, j'ai compris que la date n'était pas celle que l'on croyait, pour la simple raison que dans la première moitié du XVIe siècle dans la chancellerie impériale, les changements d'années s'effectuaient encore à Pâques* », détaille l'historienne. Les pièces du puzzle s'assemblent enfin : la missive a en réalité été écrite le 22 février 1547, soit moins d'un mois après le décès d'Henri VIII

CEDRIC JACQUOT/MAXPPP

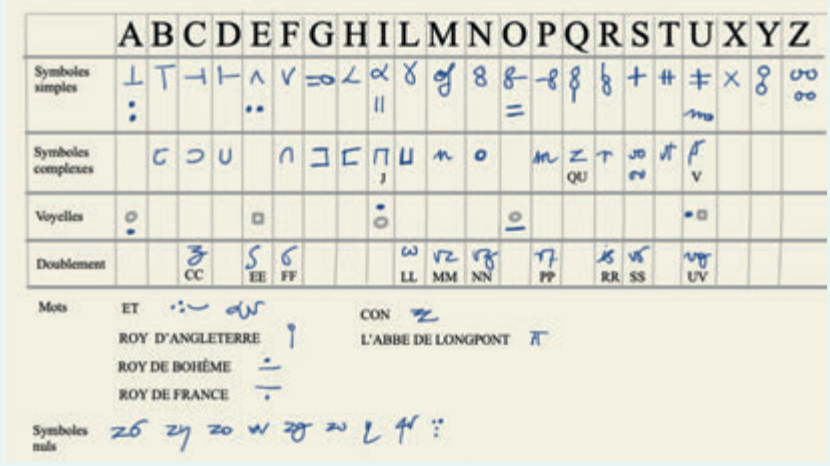
« Nous n'avions aucune lettre de l'empereur à Jean Saint-Mauris sur cette année 1547. La dépêche de Nancy a permis de remplir un creux »

Camille Desenclos, historienne à l'université de Picardie Jules-Verne, spécialiste des relations entre la France et le Saint Empire

MÉTHODE

Une clé de chiffrement à plusieurs niveaux de complexité

Les cryptographes de Charles Quint n'ont pas facilité la tâche de leurs successeurs du XXIe siècle ! Le tableau ci-contre expose de façon claire les trois grandes astuces employées pour brouiller les pistes des ennemis qui auraient intercepté l'échange. La première consiste à chiffrer sous la forme d'un simple point ou trait toute voyelle lorsque celle-ci est précédée d'une consonne. Ainsi, les syllabes formées d'une voyelle et d'une consonne deviennent des symboles complexes agrémentés d'un point ou d'un trait correspondant à la voyelle souhaitée (seule la position du point autour du symbole change). Ce qui nous conduit à la seconde difficulté : on remarque justement qu'aucun point ou trait ne correspond à la lettre E. Tous ont été volontairement supprimés lorsqu'ils sont liés à une consonne ! Un symbole complexe qui ne comprend aucun point ou trait cache donc forcément un E. Troisième difficulté : la présence de symboles nuls, disséminés parfois au beau milieu d'un mot, et qui doivent être ignorés. Pour le reste, la méthode est plus traditionnelle : chaque lettre a son symbole simple (pour les voyelles, lorsqu'elles commencent des mots ou suivent une autre voyelle, et pour les consonnes, lorsqu'elles ne sont pas suivies d'une voyelle), tout comme les lettres doublées (deux M, deux N…) et certains mots entiers, tous référencés ici. Attention, « con » n'est pas un terme grossier : il s'agit d'une abréviation fréquemment utilisée à l'époque.



BIBLIOTHÈQUE STANISLAS DE NANCY, INRIA NANCY

d'Angleterre, survenu le 28 janvier. Mais alors que dit cette lettre ? Beaucoup de choses sur l'état d'esprit de Charles Quint. *« Nous n'avions aucune lettre de l'empereur à Jean Saint-Mauris sur cette année-là et la dépêche de Nancy nous a permis de remplir un creux »*, se réjouit Camille Desenclos. La prose désormais déchiffrée révèle trois préoccupations majeures du monarque en cette période d'accalmie dans les conflits qui opposent depuis près d'un demi-siècle les rois de France aux rois d'Espagne. *« Accalmie toute relative puisque, au début de l'année 1547, la tension est à son comble entre François Ier et Charles Quint. »* Ainsi, les objectifs de l'empereur sont de maintenir la paix avec le roi français pour ne pas éparpiller ses forces, de mettre fin au conflit qui l'oppose à la ligue de Smalkalde *(lire l'encadré p. 84)*, et d'éviter les assassinats… à commencer par le sien. Charles Quint fait en effet état d'une rumeur qui le tracasse au plus haut point : Pierre Strozzi, chef de guerre au service de François Ier dont le nom est brouillé par des symboles nuls, aurait formulé devant son roi l'intention de l'assassiner. Charles Quint cherche ainsi à vérifier auprès de Saint-Mauris l'exactitude de ces informations et, le cas échéant, il explique vouloir savoir comment François 1er a réagi aux paroles de Pierre Strozzi. *« À cette époque se mène aussi en Europe une virulente guerre de l'information — ou plutôt de la désinformation —, qui consiste en la propagation de rumeurs infondées destinées à embrouiller et déstabiliser les puissances ennemies,* détaille Camille Desenclos. *Il est possible que cette histoire d'assassinat soit l'une d'entre elles. »*

Outre les informations précieuses que la lettre a fini par livrer, son décryptage est un exemple inédit de collaboration fructueuse entre cryptographes et historiens. *« Sans l'aide de Camille Desenclos, nous aurions sans doute mis un temps considérable à la déchiffrer »*, avoue Cécile Pierrot, qui reconnaît également avoir pris goût au décryptage de documents historiques, elle qui d'ordinaire planche sur des systèmes de chiffrage bancaires ou biométriques. Cela tombe bien car selon Camille Desenclos, 2 à 5 % des documents historiques chiffrés le restent encore à ce jour. ■