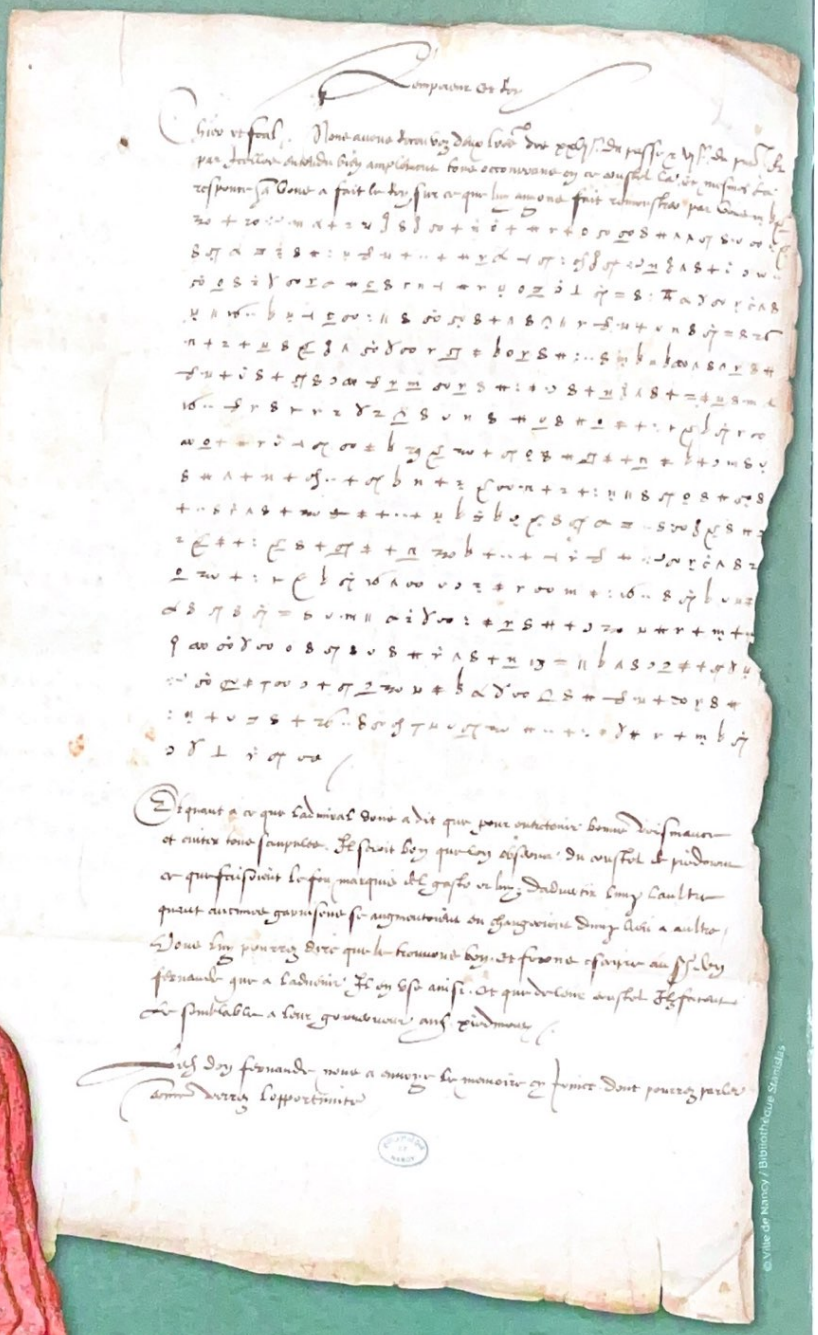
Quand la SCIENCE lit le courrier des MONARQUES

Au début de l'année 2023, deux équipes de chercheurs et de chercheuses ont réussi à lire des lettres de Charles Quint et de Marie Stuart. Pourtant, ces missives étaient chiffrées. Pour les décoder, ils ont usé d'ordinateurs, d'algorithmes et d'ingéniosité.

Par Charlotte Mauger

© Wikimedia Commons



© Ville de Nancy / Bibliothèque Stanislas

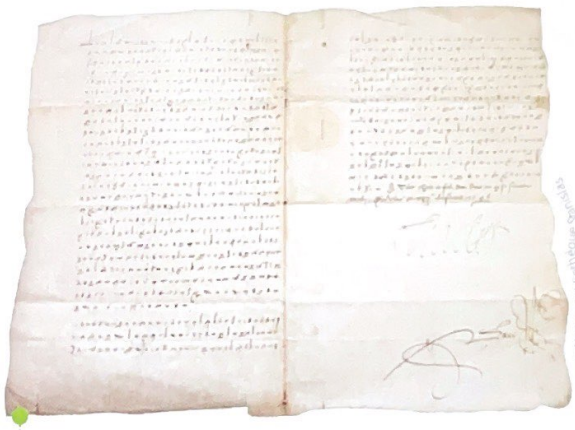
En 1578, Marie Stuart, ancienne reine d'Écosse, est désormais la prisonnière de sa cousine, la reine Élisabeth Ier d'Angleterre. Dans ses missives, elle s'épanche notamment sur ses conditions de détention et de santé.

Nous sommes en 1574 et l'empereur **Charles Quint** prend sa plume pour écrire à son ambassadeur en France, **Jean de Saint-Mauris**. Pour plus de discrétion, le monarque choisit de **chiffrer son message**. Quelques années plus tard, en 1578, **Marie Stuart** correspond, elle aussi, grâce à des **missives codées** avec l'**ambassadeur de France en Angleterre.**

Ces deux têtes couronnées ne se doutent pas que 450 ans après, deux équipes de chercheurs et chercheuses perceront les secrets de leurs lettres. Tombés dessus par hasard, ces passionnés de codes secrets ont réussi à **reconstruire les clés de déchiffrement**, c'est-à-dire la façon de passer du message codé à un texte lisible par tous.

Une centaine de symboles inconnus

La lettre de Charles Quint et les 57 de Marie Stuart se ressemblent un peu : une accumulation de symboles illisibles sur du papier jauni. **Ici, chaque lettre de l'alphabet et chaque nom a été remplacé par un ou plusieurs signes.** Par exemple, dans celle de Charles Quint, les « A » en début de mot deviennent des « T » à l'envers ou des « : ». Pour savoir ce qui est écrit, il faut retrouver le ou les symboles qui camouflent chaque lettre, puis reproduire le texte. Donc, retrouver que « : » est un « A » et le remplacer dans le courrier.



© Ville de Nancy / Bibliothèque Stanislas

Au premier coup d'œil, la lettre de Charles Quint paraît incompréhensible...

Pour cela, les deux équipes ont commencé par entrer les successions de symboles dans leurs ordinateurs. « À la main, il n'était pas possible de faire le travail car il y a plus de 100 symboles ! », explique **Cécile Pierrot** qui a participé au déchiffrement de la lettre de Charles Quint. Grâce à l'outil informatique, ils ont pu faire des calculs plus rapidement et faire tourner des **algorithmes**. « Cette transcription, c'est ce qui a pris le plus de temps ! », avoue George Lasry, qui lui a travaillé sur les lettres de Marie Stuart.

© Ville de Nancy / Bibliothèque Stanislas

Voici les scientifiques qui ont percé les secrets du message de Charles Quint : Cécile Pierrot, Camille Desenclos, Paul Zimmermann et Pierrick Gaudry (de gauche à droite).

Impossible de tester toutes les possibilités

Après cela, une idée toute bête pour déchiffrer ces courriers est de tester toutes les possibilités. On pourrait associer au hasard la centaine de symboles aux lettres de l'alphabet et aux noms importants (comme les rois). « Ensuite, on remplace dans le texte et on voit si cela donne quelque chose de lisible », explique Cécile Pierrot.

Cette méthode est simple, mais elle a un problème : **il y a bien trop d'associations possibles**. Il faudrait plus que des milliards de milliards d'années pour toutes les tester ! Il faut trouver autre chose.

Identifier les symboles les plus fréquents

En français, certaines lettres sont très communes, le « e », le « n » ou le « s ». Dans un message codé, les symboles qui remplacent ces lettres, eux aussi, sont plus présents que les autres. **Étudier le nombre d'occurrences d'un signe donne des indices sur la lettre qu'il remplace.** « Par exemple, dans la lettre de Charles Quint, le symbole « 8 » était le plus présent. Immédiatement, on savait qu'il ne pouvait remplacer que le « e », le « s » ou le « n » », explique Cécile Pierrot. Effectivement, ils ont montré ensuite que c'était le « n » qui était dissimulé ici.

Cette méthode est très efficace pour casser les **chiffrements dits par substitution**, ceux pour lesquels une lettre est remplacée par un unique symbole. Mais les codes de ces messages sont plus complexes, notamment car les lettres sont remplacées par plusieurs signes et non un seul.

Les ordinateurs à la rescousse

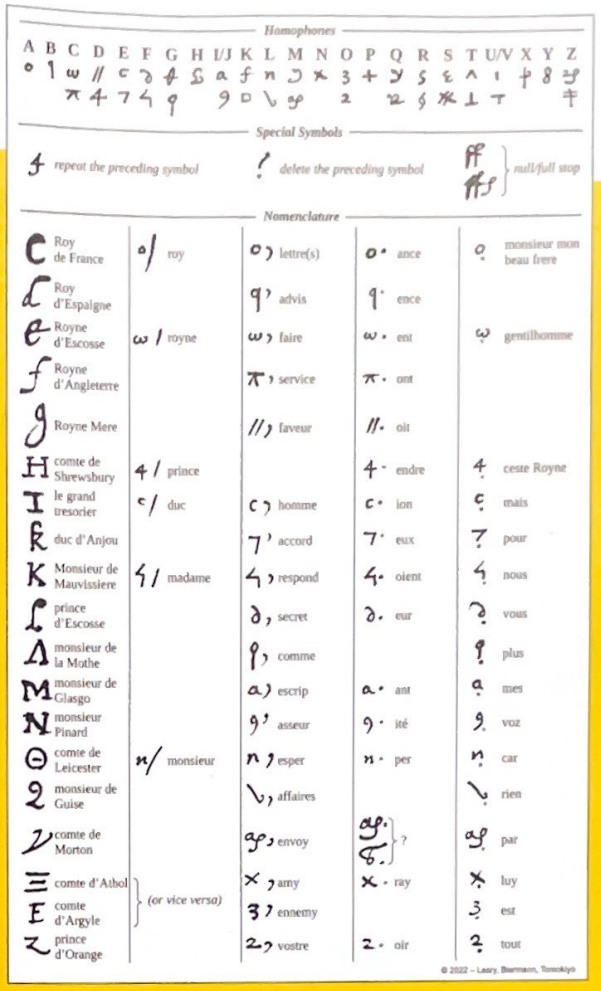
Alors, comment faire ? **George Lasry** a eu une idée : **développer un algorithme qui assigne au hasard des symboles aux lettres**, déchiffre le message avec cette clé et donne une note à ce déchiffrement. « À chaque étape, l'ordinateur regarde si les terminaisons courantes du français apparaissent (comme « -ons » ou « -ent ») et donne une note à la traduction en fonction », explique le chercheur en informatique.

Plus ces terminaisons sont présentes, plus le décodage est proche. L'ordinateur continue de modifier l'association des lettres et symboles à l'étape d'après, tout en conservant les bonnes associations des étapes précédentes. Au fur et à mesure, les lettres se dévoilent et enfin les chercheurs devinent l'identité - encore inconnue pour eux - de son autrice : c'est Marie Stuart !

Il existe de nombreuses techniques pour chiffrer des messages : pour les découvrir, replongez-vous dans le dossier du *Cosinus* n° 224 !

À VOUS DE JOUER !

Voulez-vous chiffrer un message comme Marie Stuart ?
Rien de plus simple : chacune des lettres de votre message doit être remplacée par son ou l'un de ses symboles selon le tableau ci-contre.



Homophones

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

Special Symbols

repeat the preceding symbol — delete the preceding symbol — null/full stop

Nomenclature

Roy de France	roy	lettre(s)	ance	monsieur mon beau frere
Roy d'Espaigne		advis	ence	
Royne d'Escosse	royne	faire	ent	gentilhomme
Royne d'Angleterre		service	ont	
Royne Mere		faveur	oit	
comte de Shrewsbury	prince		endre	ceste Royne
le grand tresorier	duc	homme	ion	mais
duc d'Anjou		accord	eux	pour
Monsieur de Mauvissiere	madame	respond	oient	nous
prince d'Escosse		secret	eur	vous
monsieur de la Mothe		comme		plus
monsieur de Glasgo		escrip	ant	mes
monsieur Pinard		asseur	ité	voz
comte de Leicester	monsieur	esper	per	car
monsieur de Guise		affaires		rien
comte de Morton		envoy	?	par
comte d'Athol	(or vice versa)	amy	ray	luy
comte d'Argyle		enneemy		est
prince d'Orange		vostre	oir	tout

Pour déchiffrer, c'est le contraire : il faut troquer le symbole contre la lettre qu'il dissimule. Entraînez-vous avec cette phrase !

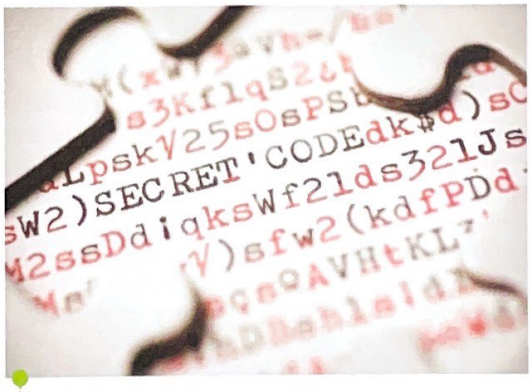
qsoiz +3is oizas //cwδaddsc wc ycεεoθc cwsaʌ oicw nc w3//c //c yosac εʌiosʌ

Réponse p. 48.

Un coup de chance

Et parfois, la chance s'invite dans l'enquête. Alors qu'ils se creusaient les méninges sur le courrier de Charles Quint, Cécile Pierrot et ses collègues ont bénéficié d'un gros coup de pouce. Camille Desenclos, chercheuse en histoire, a retrouvé d'autres lettres adressées au même destinataire, Jean de Saint-Mauris, et chiffrées de la même manière.

Or, dans l'une d'entre elles, l'ambassadeur de Charles Quint en France a écrit la traduction de la lettre dans la marge. « C'était une véritable pierre de Rosette : on avait face à nos yeux le texte chiffré et le texte déchiffré ! Cela nous a donné une grande partie des symboles », se rappelle Cécile Pierrot. Ne leur restait plus qu'à combler les trous. Et voilà que la lettre de Charles Quint, elle non plus, n'a plus de secret !



© WNDCOLORS / Adobe Stock

Charles Quint et Marie Stuart étaient loin de s'imaginer que, bien des siècles plus tard, de nouvelles technologies permettraient de briser le secret de leurs correspondances. Dans 10 ou 100 ans, nous serons peut-être aussi victimes d'une telle innovation !