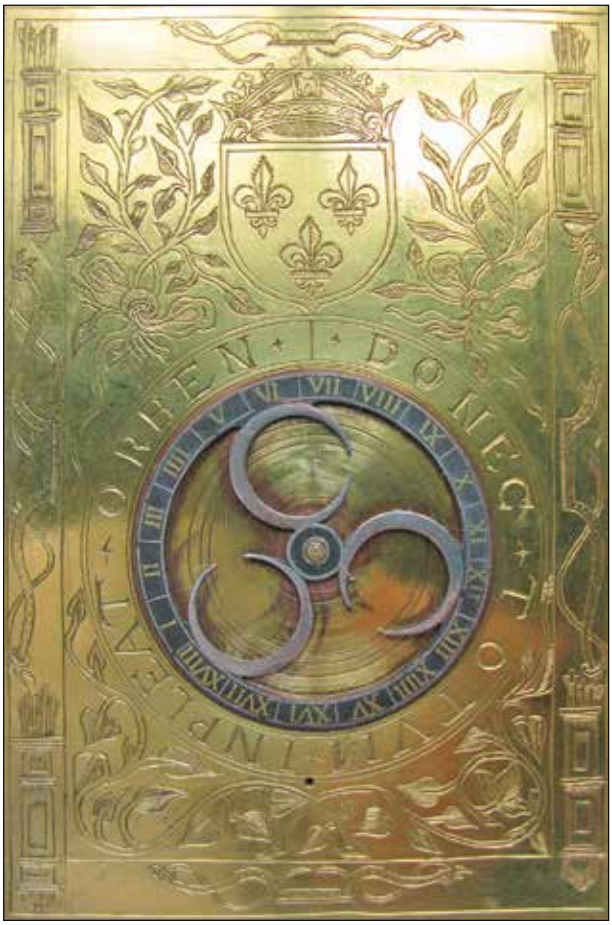
Analyse de la boîte à chiffrer d'Henri II

Hervé Lehning

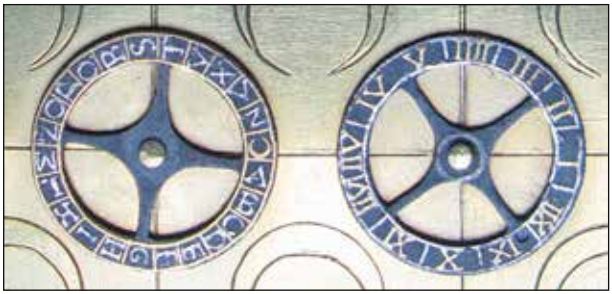
Le fonctionnement de la boîte à chiffrer et déchiffrer d'Henri II, exposée au musée de la Renaissance au château d'Écouen, a été oublié depuis longtemps et semble n'avoir jamais été redécouvert. En vue d'une exposition sur les secrets d'État aux archives nationales, le conservateur a demandé à l'ARCSI si l'un de ses membres pouvait étudier la question. Cet article est le résultat de notre étude au vu de l'objet, ainsi que de l'histoire de la cryptographie.

L'objet baptisé « boîte à chiffrer et déchiffrer » du musée d'Écouen fut acquis en 1843 par le musée de Cluny en tant qu'instrument astrologique. Il fut reversé au musée de la Renaissance d'Écouen à sa création en 1977, mais en tant que boîte à chiffrer. Il ressemble à un livre composé de quatre pages.

Pages 3 et 4 de la boîte à chiffrer



Page 2 de la boîte à chiffrer, la page 3 est semblable



Détail de deux cadrans de la page 1

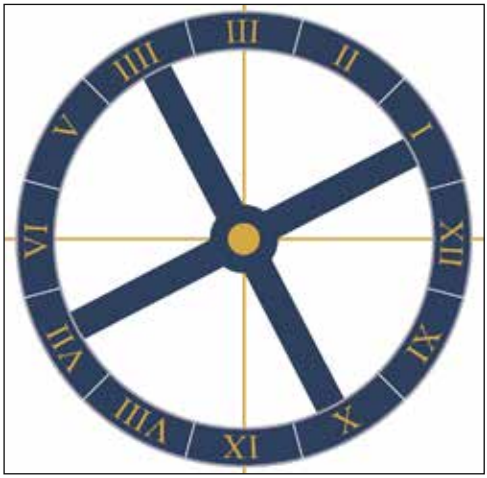
Détail de deux cadrans de la page 4

La première page du livre est constituée de 24 cadrans répartis en quatre colonnes de six. Chaque cadran est une petite roue à quatre rayons, formant une croix, pouvant tourner autour de son moyeu et dont la jante est divisée différemment selon les colonnes. En colonnes 1 et 3, elle est divisée en 24 angles de 15°, chacun portant un symbole. Dans le sens des aiguilles d'une montre : ABCDEFGHIKLMNOPQRSTVXYZ○. Les lettres de A à Z sont argentées et inscrites dans le sens de la circonférence. Les absences des lettres J, U et W sont classiques en cryptographie, les lettres I et J d'une part et U, V et W d'autre part étant souvent confondues. L'ajout d'un C doré et tourné de 90° est plus original. La présence de ces cadrans alphabétiques confirme l'hypothèse actuelle selon laquelle cette boîte servait à chiffrer. Le rapport à l'astrologie semble plus douteux. Même si le nombre 12 évoque les 12 signes du zodiaque, on ne voit pas bien à quoi correspondraient alors les cadrans alphabétiques.

La visée d'une lettre devait se faire à l'horizontale à droite, position où elle est facile à lire. Sur la figure suivante, il s'agit donc de la lettre A. Nous avons de plus constaté qu'aucun mécanisme ne relie les cadrans entre eux. Ils sont donc indépendants les uns des autres.

Cadran alphabétique de la page 1

En colonnes 2 et 4, les roues sont divisées en 12 angles de 30° chacun portant un nombre entre I et XII. Les inscriptions sont disposées comme sur une horloge, mais dans le sens inverse. La visée d'un chiffre devait se faire à la verticale en haut car elle était alors facilitée par son orientation et le quadrillage de la page. Sur la figure suivante, il s'agit donc du chiffre III. Le nombre 12 étant la moitié de 24, ces cadrans numériques peuvent être mis en regard avec les cadrans alphabétiques, un nombre correspondant alors à deux lettres.



Cadran numérique de la page 1

La seconde page est constituée d'un cadran numérique plus grand, subdivisé en 18 angles de 20° chacun numérotés de I à XVIII comme sur une horloge. Il comporte trois rayons en forme de croissants dont la disposition fait penser que la manière naturelle de le faire tourner est le sens inverse des aiguilles d'une montre.

Grand cadran numérique des pages 2 et 3

La troisième page est identique à la seconde. Le fait que ce nombre 18 n'est ni multiple ni diviseur de 12 et de 24 exclut une mise en regard directe de ces grands cadrans avec les petits. La quatrième page est semblable à la première. Cependant les roues des colonnes 1 et 3 n'ont que deux rayons et celles des colonnes 2 et 4 ont des rayons en forme de croissants. D'autre part, les cadrans numériques se trouvent maintenant en colonnes 1 et 3, les chiffres sont orientés dans le sens de la circonférence et les cadrans alphabétiques en colonnes 2 et 4. Les chiffres des cadrans numériques sont maintenant pleinement lisibles quand ils sont à l'horizontale, à gauche. Cela peut signifier qu'elle s'utilisait à l'envers mais ce n'est pas certain.

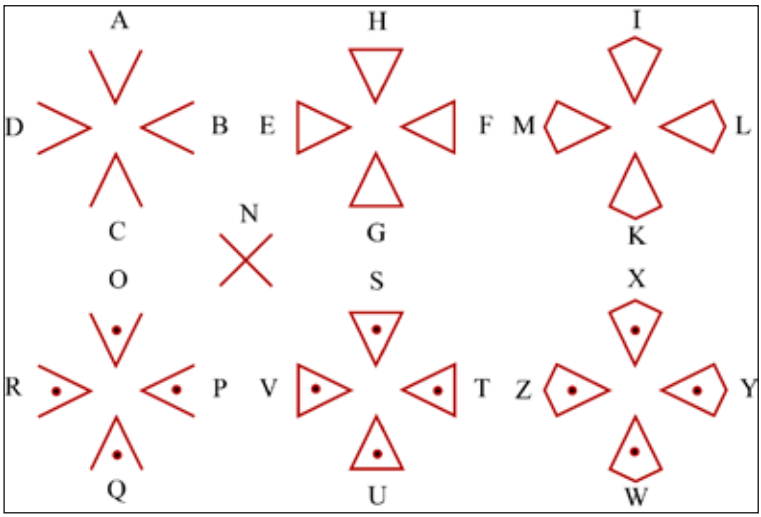
Les deux types de cadrans alphabétiques de la page 4 sont équivalents

Les cadrans numériques de la page 4

Ces différences de formes et de positions ne semblent pas pertinentes. Les pages 1 et 4, comme 2 et 3 devaient fonctionner de la même façon. Nous les considérerons donc comme identiques malgré les quelques différences matérielles.

Contexte de l'histoire de la cryptographie

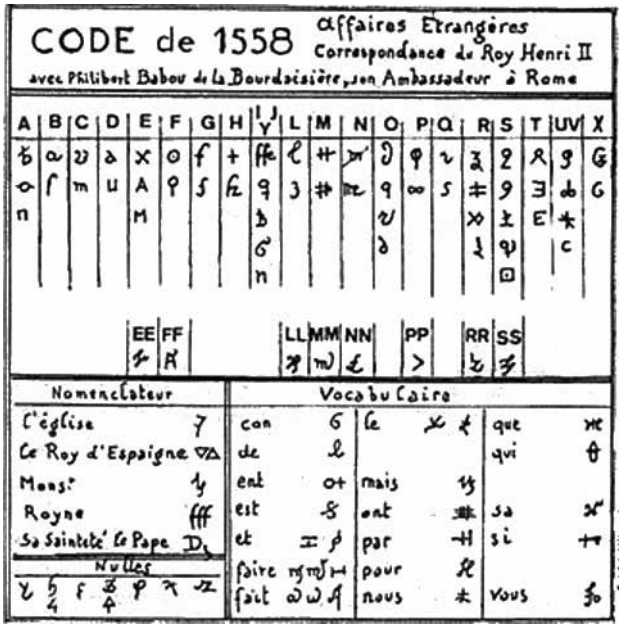
Pour continuer notre analyse, il convient de placer cet objet dans le contexte de l'histoire de la cryptographie. Les chiffres utilisés à la Renaissance ont succédé aux chiffres de l'Antiquité et du Moyen-Âge, qui étaient généralement de simples substitutions alphabétiques, un alphabet étant remplacé par un autre comme dans le chiffre des Templiers.



Substitution alphabétique utilisée par les Templiers

L'utilisation de la méthode des fréquences pour décrypter les messages chiffrés ainsi est attestée dès le IX^{e} siècle, quand Abu Yusuf Al-Kindi (801 – 873) l'expose très clairement dans son *manuscrit sur le déchiffrement des messages cryptographiques* (archives d'Istanbul). Les chiffres par substitutions alphabétiques n'assuraient donc plus efficacement le secret des correspondances depuis longtemps quand la boîte à chiffrer a été créée. Pour contourner la méthode des fréquences, les cryptologues de la Renaissance trouvèrent deux parades. La plus couramment utilisée était celle des substitutions alphabétiques homophones, où une même lettre pouvait être chiffrée de plusieurs façons différentes, auxquelles on ajoutait quelques nulles (c'est-à-dire des lettres ne signifiant rien, simplement destinées à fausser un peu plus les fréquences) et un nomenclateur pour chiffrer des mots d'usage courant comme « le pape », « son altesse » ou « guerre ». On trouve plusieurs chiffres de ce type utilisés au temps d'Henri II, comme l'attestent les papiers du baron de Fourquevaux (1508 – 1574) que rapportent Jean Brunon et Jean Barruol dans *Les Français en Italie sous Henri II* (Marseille, 1952). Voici par exemple celui utilisé par Philibert Babou de la Bourdaisière, cardinal et ambassadeur d'Henri II à Rome. Il est typique des chiffres de l'époque.

Élevée à la cour d'Henri II, Marie Stuart utilisa naturellement un chiffre comparable, ce qui lui coûta la vie. En effet, si les chiffres homophones ne sont pas vulnérables à la méthode des fréquences, ils le restent à celle du mot probable et, surtout, tout symbole décrypté le reste pour toujours. Le secret du chiffre tombe ainsi petit à petit et de façon irrémédiable.



Chiffre de Philibert Babou de la Bourdaisière fils

La seconde parade a été inventée plusieurs fois, il s'agit des chiffres par substitutions poly-alphabétiques. La première description connue de cette idée se trouve dès 1466 dans *De Componendis Cifris* de Leone Battista Alberti (1404 – 1472). Ce dernier y décrit un objet comportant deux disques concentriques, de tailles différentes, pouvant tourner autour de leur centre commun. Le plus grand est marqué des lettres de l'alphabet (sauf H, J, K, U, W, Y) plus les nombres de 1 à 4. Le plus petit est marqué d'un alphabet de 24 lettres.

Le cadran d'Alberti fait correspondre les lettres de A à Z (sauf H, J, K, U, W, Y) plus les nombres de 1 à 4 à des symboles dans le désordre.

A priori, ce système permet une substitution alphabétique qui devient polyalphabétique si on s'autorise à tourner la roue intérieure périodiquement, selon une règle convenue. Pour l'utiliser pour chiffrer, les correspondants devaient convenir d'une position initiale (par exemple : A et *x* se correspondant comme sur la figure qui suit), qui servait de clef, et d'une règle (par exemple : tourner le petit cadran d'un cran dans le sens des aiguilles d'une montre après avoir chiffré 4 lettres). Les nombres de 1 à 4 permettaient d'utiliser un nomenclateur, chaque combinaison de ces quatre nombres ayant une signification comme « pape », « sire » ou « assiéger ».

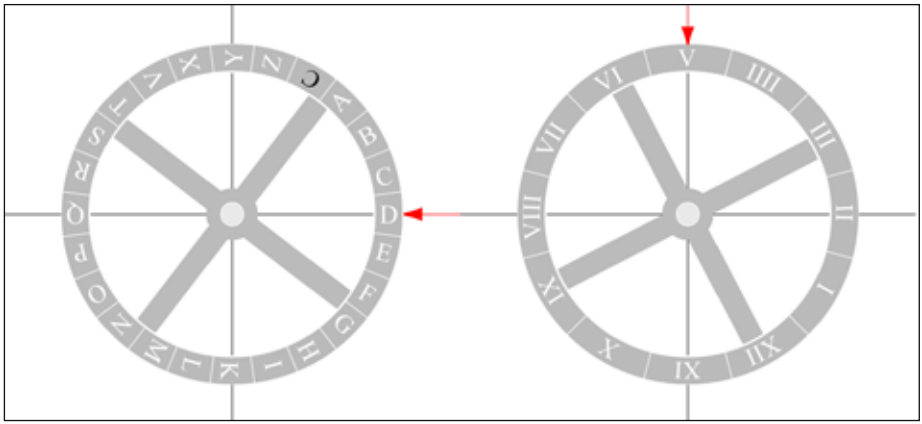
Cependant, le plus connu des inventeurs de chiffrements par substitution polyalphabétique est Blaise de Vigenère (1523 – 1596). Son système est parfaitement décrit dans son *Traicté des chiffres, ou Secrètes manières d'écrire* daté de 1586 (BNF). La substitution varie à chaque lettre selon une clef échangée entre les correspondants. Malgré ces inventions, les chiffres sont essentiellement restés des substitutions alphabétiques homophones jusqu'à l'avènement de la famille des Rossignols qui créèrent le Grand Chiffre de Louis XIV, qui était un dictionnaire chiffré, et était donc d'une autre nature. D'autre part, avant cette époque, l'habitude était restée de garder le découpage des mots, même si cela fragilise fortement les chiffres.

Pour finir cette étude historique, nous pouvons remarquer que cette boîte à chiffrer n'a eu aucune descendance directe, peut-être à cause de sa complexité et de sa difficulté d'utilisation. Il en est de même des chiffrements par substitution polyalphabétique qui ne furent guère utilisés avant le XIX^{e} siècle, sans doute à cause de la difficulté de leur usage sans instrument adéquat. L'exception de Marie-Antoinette, qui l'utilisait pour chiffrer une lettre sur deux, ce qui le rendait très vulnérable à l'attaque par mot probable, confirme cette impression.

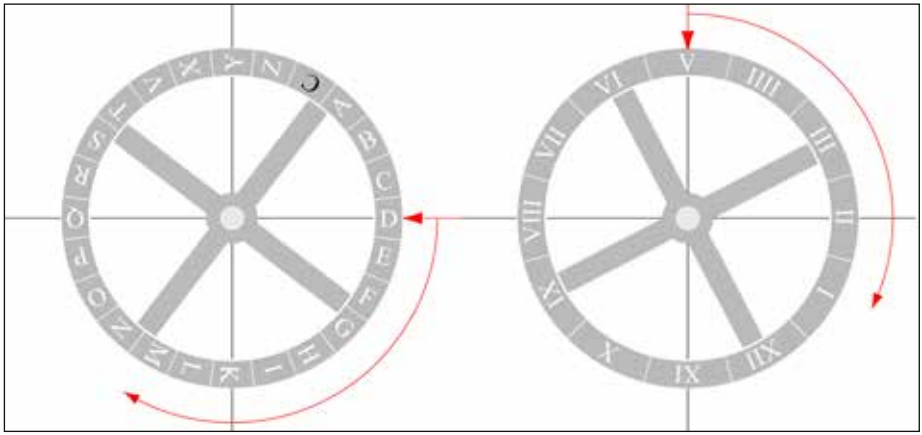
Substitution par paire de cadrans

Si on exclut les deux grands cadrans numériques, la boîte est composée de couples de cadrans alphabétiques et numériques. De façon assez naturelle, en positionnant le cadran alphabétique sur une lettre (D sur la figure) et le cadran numérique sur un chiffre qui jouera le rôle de clef (V sur la figure), on peut chiffrer la lettre selon la clef. Les essais d'utilisation effective montrent que ce n'était pas aisé car les cadrans sont petits (3,2 cm de diamètre) et les indications le sont encore plus et sont parfois à moitié effacées, mais cela peut être dû à l'usure du temps. Pour continuer notre étude, nous admettrons que le chiffrement s'effectuait bien de cette manière, en faisant opérer un cadran numérique sur un cadran alphabétique. Il s'agit de trouver la règle pour ce faire !

Bien entendu, cette règle faisait partie de la notice d'emploi de la boîte. Comme elle est perdue, nous ne pouvons qu'imaginer les règles les plus logiques et pas trop difficiles à appliquer. Dans tous les cas, elles doivent tenir compte des positions des deux cadrans. Une règle naturelle est d'effectuer sur le cadran alphabétique la rotation qui mène de V à I sur le cadran numérique. Si on utilise un compas, ou tout autre instrument permettant de reporter les distances, cela revient à porter la distance de V à I en D, ce qui donne M. Dans l'état actuel des cadrans, cela semble la seule façon sûre d'opérer mais nous pouvons admettre qu'une personne à la main sûre peut effectuer cette opération sans l'aide d'un quelconque instrument.



Couple formé d'un cadran alphabétique et d'un cadran numérique positionnés sur D et V



Une façon de faire opérer un nombre du cadran (V ici) sur une lettre (D ici) qui donne la lettre chiffrée (M ici)

Il est facile d'opérer de même en page 4, la règle que nous proposons ne tenant pas compte des formes des rayons des cadrans. Le symbole supplémentaire ○ peut servir à référer à un nomenclateur de 23 mots en faisant suivre ○ d'une lettre de A à Z. Par exemple, ○A peut signifier « l'église », ○B, « le roy d'Espaigne », *etc.* Si nous imaginons un nomenclateur du type de celui de Babou de la Bourdaisière, nous obtenons un tableau du type :

○A	○B	○C	○D	○E	○F	○G	…
L'église	Le Roy d'Espaigne	Monseigneur	Royaume	Sa Sainteté le pape	Faire	Faict	…

Un nomenclateur possible

On peut augmenter la taille du nomenclateur en faisant suivre ○ de deux lettres mais ce n'était sûrement pas le cas car les nomenclateurs de l'époque étaient plutôt courts. Le symbole ○ peut également représenter un espace ou une nulle, mais ces hypothèses nous semblent moins probables car peu conformes aux chiffres de l'époque.

Réglage des cadrans numériques

En admettant cette action des cadrans numériques sur les cadrans alphabétiques qui les jouxtent, il nous reste à voir comment les régler. La présence des deux grands cadrans numériques en regard des deux pages de petits cadrans fait penser qu'ils constituent la clef du système. Dans cette hypothèse, il semble logique de penser que la position de chaque grand cadran permet de définir les positions des 12 petits cadrans numériques de la page correspondante. Mathématiquement, cela signifie qu'il s'agit de produire une suite de douze nombres entre 1 et 12. Deux contraintes semblent naturelles. La première est que la suite soit obtenue de façon simple en manipulant le grand cadran, la seconde est que la suite soit aussi dispersée que possible. Pour comprendre les choix possibles, il est nécessaire d'examiner les mathématiques de l'époque, qui est juste antérieure à François Viète (1540 – 1603), le grand mathématicien et cryptologue français du XVI^{e} siècle. Par exemple, Pierre Forcadel, titulaire d'une chaire de mathématiques au Collège de France à partir de 1560, a écrit un livre d'arithmétique en 1556, nommé *L'arithméticque* (BNF), dans lequel il décrit en particulier les progressions arithmétiques, qui étaient donc d'usage courant pour un mathématicien de l'époque d'Henri II. D'autre part, les horloges mécaniques comme nous les connaissons avaient été inventées depuis deux siècles. Les cadrans chiffrés et leurs propriétés étaient donc bien connus.

Une idée naturelle pour un mathématicien disposant des connaissances dont fait preuve Pierre Forcadel dans son livre est de considérer un nombre de départ sur lequel on positionne le grand cadran et un incrément. Les deux peuvent constituer la clef, à moins que, par souci de simplicité, l'incrément soit toujours le même. La méthode n'explique pas directement le fait que les grands cadrans aient 18 positions et les petits, seulement 12. Cependant, ces deux nombres ont une propriété mathématique commune, celle d'avoir les mêmes facteurs premiers, 2 et 3. Plus précisément, $12 = 2^2 \times 3$ et $18 = 2 \times 3^2$. Un incrément de 2 ou 3 donnera des suites très régulières. Par exemple, si nous partons de la position 1 sur le grand cadran et utilisons l'incrément 2, c'est-à-dire tournons la roue de 2 crans douze fois de suite, nous obtenons 1, puis 3 = 1 + 2, et de même : 5, 7, 9, 11, 13, 15, 17. À ce niveau, nous repassons par 18 et obtenons ensuite à nouveau 1 puis 3 et 5. En reportant cela sur les petits cadrans, comme ils n'ont que 12 positions, les nombres sont réduits à leurs restes dans la division par 12, soit : 1, 3, 5, 7, 9, 11, 1, 3, 5, 1, 3, 5. Les mêmes réglages (1, 3 et 5) se retrouvent plusieurs fois. Le créateur de la boîte a pu vouloir éviter cela. Pour assurer la meilleure dispersion possible, le mieux est d'éviter 2 et 3 comme incréments et donc d'utiliser un nombre comme 4 ou 5. Pour éviter une manipulation trop lourde, il est peu probable, quoique possible, que l'incrément ait été supérieur. La clef se limiterait alors à la première position du grand cadran plus un incrément, sans doute inférieur à 5.

Dans cette hypothèse, si la clef est 2 pour la position initiale et 5 pour l'incrément, en utilisant le grand cadran, nous obtenons par une suite de rotations de ce cadran, sans le moindre calcul : 2, 7, 12, 17, 4, 9, 14, 1, 6, 11, 16, 3. En réduisant à 12, nous obtenons : 2, 7, 12, 5, 4, 9, 2, 1, 6, 11, 4, 3 ce qui permet de régler les petits cadrans numériques de la page 1. L'usage de 5, nombre premier avec 12, a l'avantage d'éviter d'obtenir une suite périodique et de mieux disperser la suite de nombres, ce que les mathématiciens de l'époque savaient.

On fait de même pour la page 4. Bien entendu, de nombreuses autres solutions sont possibles pour ce réglage des petits cadrans à partir d'une clef mais le dispositif peut

fonctionner ainsi, et les autres méthodes sont semblables. La seule chose étonnante *a priori* est que les grands cadrans aient 18 divisions et non 12. En fait, cela peut être considéré comme une complication volontaire des réglages des petits cadrans pour rendre la suite des décalages moins prévisible. Le choix de 18 s'explique alors sans doute par le fait que ce nombre a les mêmes facteurs premiers que 12.

Exemples de chiffrement

Pour illustrer notre propos, chiffrons le message « association des réservistes du chiffre et de la sécurité de l'information » avec les clefs II, V et X, V selon la méthode exposée. Nous commençons par régler les 24 cadrans numériques des pages 1 et 4 à l'aide des grands cadrans numériques des pages 2 et 3 que l'on positionne à II pour le premier et à X pour le second. En suivant la règle exposée ci-dessus, c'est-à-dire en les tournant 12 fois chacun de 5 dans le sens des aiguilles d'une montre, nous obtenons pour la page 1 : II, VII, XII, V, IIII, IX, II, I, VI, XI, IIII, III et pour la page 4 : X, III, II, VII, XII, V, IIII, IX, II, I, VI, XI. Ces réglages resteront les mêmes jusqu'à la fin du processus de chiffrement, même si on pourrait imaginer une règle plus complexe.

Nous réglons alors les 24 cadrans alphabétiques dans l'ordre de haut en bas et de gauche à droite, même si on peut une fois encore imaginer qu'on le fasse de gauche à droite et de haut en bas, ce qui serait d'ailleurs préférable pour des raisons cryptographiques comme nous le voyons plus loin, mais peu naturel vu l'objet. Nous faisons alors agir les cadrans numériques sur les cadrans alphabétiques et notons les résultats. Pour le premier, A + II = C, pour le second S + VII = F, *etc.* Tout se passe en fait comme dans la méthode de Vigenère, chaque numéro provoquant un décalage double donc. Il donne un décalage de 2 dans l'alphabet, VII, de 12. Nous obtenons : Cfqyiacttkt hzy trqnzmlseav qs loahfca lz yi nn qnimtiea fr i rtycryxanhr.

En guise d'exemple, le lecteur pourra décrypter le message : Kleyb sybk cvpc trsbwa c dpzzfizge an sxvsllg pfrmyte lqll ee dbgcl r ehtkheca kx keznp rc.

Solidité de l'algorithme de chiffrement proposé

Ce chiffrement est solide si le secret de l'algorithme sous-jacent est gardé. Ceci quel qu'il soit s'il reste du type décrit ci-dessus. Si le secret de l'algorithme n'est pas gardé, à cause d'une indiscrétion ou d'espionnage, mais que la clef reste secrète, il peut sembler solide pour l'époque. En effet, il utilise deux clefs, qui se décomposent chacune entre une position (de 1 à 18) et un incrément (théoriquement de 1 à 18 mais probablement petit : de 1 à 5), ce qui donne *a priori*, 18 x 5 = 90 possibilités pour chaque clef donc 902 = 8 100 possibilités en tout. Cependant, si les opérations s'effectuent comme décrit ci-dessus, le nombre d'essais à faire pour décrypter un message se réduit à deux fois 90. En effet, il suffit d'essayer les 90 clefs possibles du premier cadran sur les 12 premières lettres. Si elles forment une suite prononçable, il est probable que nous ayons trouvé la bonne clef. Par exemple, dans le message précédent, nous isolons les 12 premières lettres : Kleyb sybk cvp.

En réglant le premier cadran sur I et V, nous obtenons la suite de réglages : 1, 6, 11, 4, 3, 8, 1, 6, 5, 10, 3, 2 et donc les premières lettres Kaiqy… qui ne conviennent visiblement pas. Nous continuons ainsi. En réglant le premier cadran sur V et V, nous obtenons la suite de réglages : 5, 10, 3, 2, 7, 12, 5, 4, 9, 2, 1, 6 et les premières lettres : Bravo vous ave. La première

clef est visiblement la bonne. Il nous reste à trouver la seconde par le même procédé puis le message. Utilisé sous cette forme, le chiffrement est moins solide qu'il n'y paraît *a priori* si le secret de l'algorithme de chiffrement n'est pas gardé. Il est cependant possible de résister à cette méthode de décryptement en écrivant les messages sur les pages 1 et 4 réunies de gauche à droite et de bas en haut. Dans ce cas, 8 100 essais sont nécessaires et rendent improbable un décryptement avec les moyens de l'époque.

Type de chiffrement

Bien entendu, sauf découverte très improbable d'une notice d'emploi, ou de messages chiffrés en l'utilisant, nous ne pourrons jamais assurer avec certitude le fonctionnement exact de la boîte à chiffrer d'Henri II. Cependant, la disposition des cadrans par paire, un alphabétique et un numérique, rend très probable que le nombre du cadran numérique devait agir sur la lettre du cadran alphabétique pour la chiffrer. La façon la plus simple de faire étant d'opérer un décalage de la lettre en fonction du nombre, la seule incertitude est de savoir dans quel sens il s'opérait. Cette idée suppose que les cadrans alphabétiques étaient réglés à partir du texte à chiffrer, 24 lettres par 24 avec la possibilité d'un nomenclateur correspondant au symbole. Les cadrans numériques quant à eux devaient être réglés en fonction du grand cadran numérique correspondant. L'utilisation d'une clef indiquant la position initiale de celui-ci et d'un incrément plutôt petit est probable mais on peut imaginer des méthodes plus complexes.

Conclusion

Dans ce court article, nous avons montré pourquoi l'objet étudié nous semble bien avoir servi à chiffrer et déchiffrer et n'était pas, comme il a été avancé, un instrument astrologique. Nous avons également montré une méthode, compatible avec les connaissances de l'époque, pour utiliser cette boîte pour chiffrer, et donc également pour déchiffrer puisque ces deux opérations sont restées symétriques dans tous les chiffres jusqu'en 1976. La configuration des cadrans alphabétiques accompagnés des cadrans numériques rend quasiment certain que chaque couple a bien été conçu pour générer une substitution alphabétique. La présence d'un symbole surnuméraire (◡ ici) fait penser à l'utilisation d'un nomenclateur, qui faisait partie du secret partagé entre les correspondants. Ces deux points sont corroborés par le fait que tous les chiffres de l'époque sont fondés sur ce principe. La multiplicité de ces couples de roues milite pour un chiffre à substitution polyalphabétique. La position centrale des grands cadrans numériques fait penser qu'ils commandent les positions des petits cadrans numériques, et constituent donc la clef du chiffre. Nous avons montré comment cela pouvait se faire mais les possibilités sont nombreuses. Dans tous les cas, la complexité de la mise en œuvre de cette boîte à chiffrer explique sans doute qu'elle n'ait pas eu de descendance.

Références

On trouvera les références historiques citées sur le site de la BNF, les livres référencées sont disponibles sur Gallica et les passages importants dans mon ouvrage *L'univers des codes secrets de l'Antiquité à Internet* paru chez Ixelles en 2012.