

Information noyée, information cachée

JEAN-PAUL DELAHAYE

La dissimulation d'un message dans un autre – la stéganographie – est un art ancien et multiforme : Internet le ressuscite.

Pour préserver le secret d'un message, on en code le contenu : celui qui trouve le message ne peut, en principe, rien en tirer. Cependant le seul fait de savoir qu'il y a quelque chose de caché attise la curiosité, défie l'intelligence du lecteur, qui parvient parfois à le déchiffrer. L'histoire des services secrets regorge de tels cas.

Une idée ancienne, meilleure que le codage, est la stéganographie. Ce mot – ignoré de la plupart des dictionnaires – désigne l'art de dissimuler un message secret dans un message anodin. Ce dernier, parce qu'il n'attire pas l'attention, est plus impénétrable que la plus astucieuse des méthodes de cryptographie : ne voyant pas et ne sachant pas qu'il y a quelque chose de caché, le policier ou l'espion laisse passer le message apparemment anodin. *Internet* a ressuscité cet art de noyer l'information pour la masquer.

La stéganographie apparaît dès l'Antiquité. Ainsi Hérodote raconte qu'Histiée envoya à Aristagoras de Millet un esclave porteur d'un message sans importance, puis plus tard l'indication qu'il fallait le raser. Sur le crâne tatoué de l'esclave apparut alors le message indiquant que l'heure était venue de la révolte contre les Perses. Cette méthode ne s'applique pas aux cas d'urgence : plusieurs mois sont nécessaires entre le moment où l'on écrit le message sur le crâne tondu et celui où le porteur du message, dont les cheveux ont repoussé, peut être envoyé à travers les lignes ennemies.

L'encre sympathique est la plus connue des méthodes de stéganographie : vous écrivez votre message secret sur une feuille avec une encre invisible (par exemple, du jus de citron) que seul un traitement particulier fait apparaître (par exemple, la flamme d'une bougie) ; puis vous écrivez un message inno-

cent sur la même feuille, que vous faites parvenir à votre correspondant. Les Allemands, pendant la dernière guerre mondiale, utilisèrent une variante de ce procédé : ils cochaient les lettres d'un journal avec une encre invisible (spécifique, elle ne réagissait qu'à un produit particulier).

La crainte que des espions infiltrés ne communiquent par stéganographie des informations stratégiques importantes a amené des situations cocasses. Peu après Pearl Harbor, les États-Unis mirent sur pied un service de censure de plus de 10 000 personnes chargé de repérer et d'intercepter tous les messages suspects. Les parties d'échecs internatio-

nales étaient interdites, car on craignait que la liste des coups d'une partie ne masque une information utile à l'ennemi. Les timbres pour réponse contenus dans les enveloppes étaient échangés contre d'autres de même valeur, de peur qu'ils ne signifient quelque chose de convenu. Les dessins d'enfants joints aux lettres pour les grands-parents attendris étaient confisqués, car la censure pensait qu'une carte ou une information militaire importante pouvait s'y dissimuler. Seuls les textes clairs en anglais, français, espagnol ou portugais étaient autorisés.

L'office de censure décida aussi que les demandes de diffusion de disques formulées par lettres ou appels téléphoniques aux stations de radio locales ne seraient satisfaites qu'avec un délai variable, ainsi que les annonces concernant les chiens perdus. Cette consigne devait empêcher la diffusion de messages codés destinés aux U-boats du type « le convoi partira du port aujourd'hui ».

À la même époque, une nouvelle méthode de stéganographie fut introduite par les services secrets allemands : le micropoint, qui, utilisé comme ponctuation banale dans un texte quelconque, contient des informations que seul un fort grossissement peut révéler. Il ne fut repéré par le FBI qu'en 1941, ce qui permit ensuite de démanteler plusieurs réseaux d'espionnage. Le microfilm caché sous le timbre de l'enveloppe est aussi une belle idée de stéganographie chère à l'espionnage moderne.

La lettre de George Sand

Je suis très émue de vous dire que j'ai bien compris, l'autre jour, que vous avez toujours une envie folle de me faire danser. Je garde un souvenir de votre baiser et je voudrais que ce soit là une preuve que je puisse être aimée par vous. Je suis prête à vous montrer mon affection toute désintéressée et sans calcul. Si vous voulez me voir ainsi dévoiler, sans aucun artifice, mon âme toute nue, daignez donc me faire une visite. Et nous causerons en amis et en chemin. Je vous prouverai que je suis la femme sincère, capable de vous offrir l'affection la plus profonde et la plus étroite amitié, en un mot, la meilleure amie que vous puissiez rêver. Puisque votre âme est libre, alors que l'abandon où je vis est bien long, bien dur, et bien souvent pénible, ami très cher, j'ai le cœur gros, accourez vite et venez me le faire oublier. À l'amour, je veux me soumettre.

B.N.F.

1. Un texte peut en cacher un autre. Cette lettre de George Sand en illustre la possibilité. La gymnastique qu'implique la réussite d'un tel exercice demande, bien sûr, des dispositions favorables.

LA STÉGANOGRAPHIE PURE

Dans la plupart de ces exemples, le message secret est caché dans le support matériel du message : le papier, le cuir chevelu du messager, la forme microscopique des points, le timbre. Plus délicat est de cacher un message secret dans la forme même du texte du message, ce qui est pourtant nécessaire si le message anodin doit être télégraphié, imprimé, recopié par des tiers, photocopié, diffusé par la radio ou, aujourd'hui, par *Internet*.

Cette stéganographie où le message est présent dans les symboles mêmes du message anodin est la plus intéressante, et nous l'appellerons la *stéganographie pure* : le message anodin, même recopié, contient toujours le message secret.

Le langage convenu est la plus élémentaire des stéganographies pures. Au XIV^e siècle, la papauté utilisait un tel code où, par exemple, Égyptien signifiait gibelin et où les

enfants d'Israël désignaient les guelfes. Ce genre de convention est utilisé dans les argots professionnels, où des doubles sens ne sont compris que des initiés.

La méthode des lettres repérées est aussi un moyen de stéganographie pure très apprécié. Bien sûr, l'acrostiche (la première lettre de chaque mot ou vers constitue le message caché) en est l'exemple le plus connu, mais d'innombrables variantes moins évidentes ont été inventées. Ainsi, au milieu du XVII^e siècle, sir John Trevanion, partisan de Charles I^{er}, fut arrêté par les hommes de Cromwell et enfermé au château de Colchester. Alors qu'il attendait une condamnation à mort, on lui remit une lettre dont on peut penser qu'elle avait été soigneusement examinée par ses gardiens. Il remarqua toutefois que certaines virgules étaient étrangement placées et repéra alors qu'en prenant la troisième lettre après chaque signe de ponctuation il obtenait le message *Panel at east end of chapel slides* (le panneau à l'extrémité Est de la chapelle peut glisser). Il demanda à être seul dans la chapelle pour y prier et... s'évada.

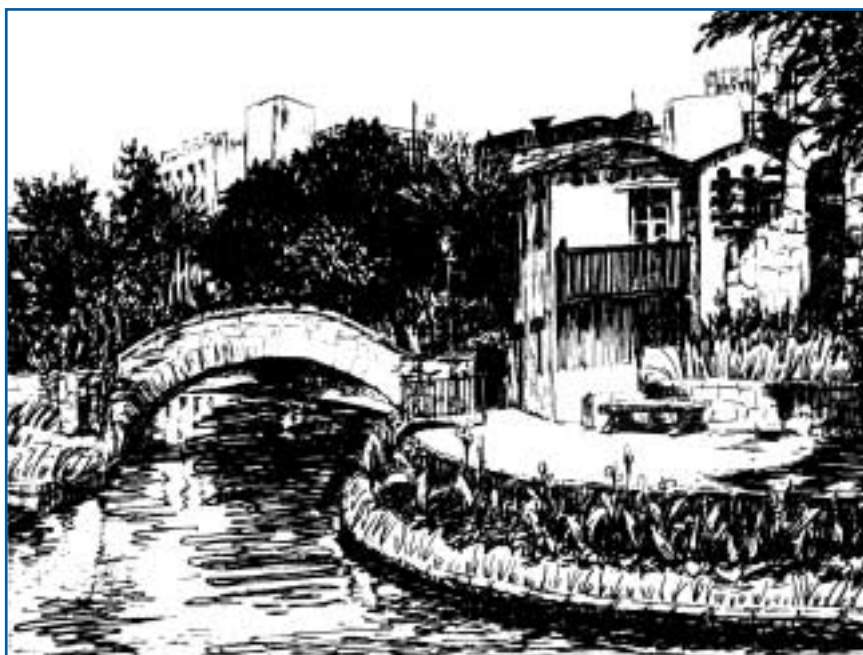
Dans le livre de D. Hofstadter *Gödel, Escher, Bach*, un message a été codé par une méthode de lettres absentes : c'est un exemple où la stéganographie ne fait pas perdre de place, mais au contraire en fait gagner. Dans la version française, à la page 454, il manque trois lettres qui sont un «f», un «i» et un «n».

Bien des exemples de messages par lettres marquées pourraient être cités, comme celui du «nègre» qui laisse son nom caché dans le manuscrit qu'il rédige pour un autre. Il n'empêche que le plus magnifique exemple de stéganographie pure appartient à la littérature française et je vous invite à lire attentivement le texte que George Sand envoya à Alfred de Musset. En faisant l'inverse de l'opération consistant à lire entre les lignes, vous découvrirez un ardent message qui éclaire les sentiments romantiques.

Une tradition de stéganographie pure est bien sûr la contrepétrie, aussi nommée art de décaler les sons. Il s'agit d'un art plus pratiqué qu'on ne le croit et auquel même les plus sérieuses des revues s'adonnent discrètement (parfois à l'insu des auteurs inattentifs). Un spécialiste physicien, auteur régulier de *Sur l'album de la Comtesse*, en glisse dans la plupart des phrases qu'il prononce, ce qui est gênant et brouille l'écoute.

DES STÉGANOGRAPHIES CHEZ LES VIRUS

La biologie moléculaire est si pleine de merveilles qu'il n'est pas surprenant d'y rencontrer des situations assimilables à de la stéganographie.



D. Kahn

2. Dessin comportant un message caché. Le message est codé en Morse dans les herbes (longues ou courtes) du bord de la rivière. Une herbe longue est un trait, une herbe courte un point. Le message signifie : *Compliments of CPSA MA to our chief Col Harold R. Shaw on his visit to San Antonio May 11th 1945.*



Londres National Gallery

3. *Les ambassadeurs*, de Hans Holbein, 1533. Un crâne humain est caché dans le bas du tableau, qu'on ne «décode» qu'en regardant le tableau sous incidence rasante selon la direction de la flèche jaune (ajoutée). Ce genre de déformation appliquée à une image pour la cacher s'appelle une anamorphose. Très populaire aux XVII^e et XVIII^e siècles dans le Nord de l'Europe et en France, ce jeu avec la perspective captiva Descartes.

Les virus sont très petits et disposent donc de peu de place pour coder les protéines (les constituants de base des êtres vivants) qui les composent. Les virus cherchent en conséquence à utiliser au mieux la longueur de leur ADN. Les parties codantes d'un ADN, lorsqu'on en lit les lettres – appelées nucléotides – par groupes de trois décrivent une succession d'acides aminés (il y en a 20) qui constitue le «plan» des protéines. Le plus souvent, si on ne démarre pas la lecture au bon endroit, le message disparaît.

Dès qu'on a établi le contenu de génomes entiers, un phénomène étonnant est apparu : le codage, par une même séquence d'ADN, de deux protéines différentes. La première protéine est déterminée quand on groupe les lettres trois par trois à partir d'une position fixée, la seconde est obtenue en décalant la lecture d'un ou deux nucléotides, ce qui conduit à une suite de triplets différents qui code une autre protéine.

Dans la carte génétique du virus ϕ X174, un des premiers génomes dont la séquence complète de nucléotides a été identifiée, il existe deux endroits où un gène est entièrement inclus dans un autre. Ailleurs, un petit bout de séquence du génome viral a une triple fonction et constitue ainsi une sorte de «stéganographie à trois étages».

Le mécanisme d'épissage de l'ADN qui, en enlevant certaines parties des séquences génotypiques, extrait ce qui

donne les protéines, crée lui aussi des situations où un même texte code plusieurs choses à la fois. Avec ce mécanisme appelé épissage différentiel, il arrive que quatre protéines différentes soient concoctées à partir d'un même «texte» de base.

Chez les eucaryotes (les êtres vivants dont les cellules possèdent un noyau), seule une petite partie du génome code des protéines, et l'utilité du reste de l'ADN est mystérieuse. Nous savons lire le message caché de l'ADN, mais pas le message de surface (s'il existe) : la situation est une stéganographie inversée!

LA STÉGANOGRAPHIE DES DEVINS ET DES TRICHEURS

À l'opposé de la stéganographie naturelle, les bases des tours de «télépathie» sont complètement artificielles. En voici un exemple que vous pourrez pratiquer vous-même. Vous dites à l'un de vos amis que vous allez faire un exercice de transmission de pensée avec un télépathe que vous connaissez et avec lequel vous avez réussi à ajuster vos ondes cérébrales. Votre ami choisit une carte dans un jeu de cartes (si vous n'avez pas de jeu sous la main, il choisit sa carte mentalement). Votre ami vous indique la carte choisie : le roi de pique, par exemple. Vous composez alors le numéro de téléphone de votre ami «télépathe». Il décroche, vous dites : «Allô!, Monsieur

Dujardin, ici Jean, je voudrais tester notre ajustement mental, je vais penser à une carte, devinez laquelle.» Vous passez l'écouteur à votre ami présent et, au bout de quelques secondes pendant lesquelles vous faites toutes sortes de simagrées attestant que vous communiquez mentalement avec le télépathe, votre ami l'entend dire qu'il s'agit du roi de pique.

Le truc est, bien sûr, que le télépathe ne s'appelle Dujardin que si la carte choisie est le roi de pique, et que pour chaque autre carte il a un autre nom. La liste des noms associés aux cartes est écrite sur un petit papier que vous avez consulté rapidement avant de lui téléphoner et qu'il a près de son téléphone. Henry Broch, spécialiste français du paranormal, raconte qu'il a utilisé ce truc en confiant à une tierce personne le soin de donner le coup de téléphone, ce qui renforce encore l'effet. Bien d'autres trucs du même genre et nécessitant parfois l'apprentissage préalable de longues listes de phrases convenues sont utilisés par les professionnels du spectacle, conduisant parfois à des numéros époustoufflants. La communication secrète par gestes discrets intervient aussi dans ce genre de tours, ainsi bien sûr que dans de nombreuses méthodes de tricheries aux jeux de cartes.

L'IMMENSITÉ DE LA MER POUR SE CACHER

On comprend aisément que, lorsque le message anodin est long, il est aisé d'y glisser un autre message invisible pour le non-initié. Noyer de l'information passe facilement inaperçu si l'eau dans laquelle on noie le secret est disponible en grande quantité. Il n'y a d'obstacles à la stéganographie que lorsque le message anodin est court, comme c'est le cas pour les contrepèteries ou pour les tours de télépathie. Des résultats en théorie de l'information confirment qu'une petite quantité d'informations noyée par stéganographie dans une grande quantité d'informations est pratiquement indécélable.

Aujourd'hui, des milliards de données parcourent le monde, et l'utilisation de la stéganographie assure parfaitement la discrétion des messages qu'on peut vouloir masquer. Le service de censure dont nous parlions tout à l'heure, mis en place par le gouvernement américain après Pearl Harbor, n'aurait plus aucun sens, car il faudrait tout interdire : l'envoi de cassettes audio et vidéo ou de disquettes informatiques, les communications par fax, la télévision, et bien sûr les communications utilisant le réseau *Internet*. Les progrès techniques facilitent la vie des espions.

LA SUITE DE PROUHET-THUE-MORSE, UN MESSAGE FRACTAL

Un message s est composé de '0' et de '1', et est tel que l'opération f , qui transforme 01 en 0 et 10 en 1, donne des messages $f(s)$, $f(f(s))$, etc., tous intéressants. Quel est s ?

Si s commence par 0, alors s commence par 01 (car f doit pouvoir s'appliquer). Donc $f(s)$ commence par 0, et donc par 01 (car f doit pouvoir s'appliquer à $f(s)$). Donc $f(f(s))$ commence par 0, et donc par 01, etc.

On en déduit alors que :

$s = 0110100110010110 1001011001101001 1001011001101001 0110100110010110...$

Le message trouvé est la suite de Prouhet-Thue-Morse.

Si s commence par 1, on trouve que s est le message «en négatif» de la suite de Prouhet-Thue-Morse.

4. La suite de Prouhet-Thue-Morse possède des propriétés fascinantes, dont celle-ci : en prenant un élément sur deux de la

suite, on l'obtient à nouveau. Elle est donc «contenue en elle-même». Les objets fractals possèdent la même propriété : ils codent dans une partie d'eux-mêmes ce qu'ils sont globalement. On peut donc les considérer, eux aussi, comme des cas de stéganographie triviale (car le message codé est le même que le message support) infiniment profonde (car il y a un message codé dans le message, puis un autre encore dans le message codé, etc.).

L'INTERDICTION DE CACHER SON COURRIER ÉLECTRONIQUE

Certaines expériences faites récemment sur la stéganographie en utilisant des images ne laissent aucun doute sur la possibilité de transmettre secrètement et rapidement de grandes quantités d'informations sur le réseau *Internet*.

La méthode de transmission par les images numériques est facile à mettre en œuvre, en voici le principe. L'émetteur du message secret envoie une image à son correspondant, dans laquelle il a modifié quelques pixels dont l'emplacement a été convenu ; ces pixels ont été remplacés par d'autres dont les numéros codent les lettres du message (voir la figure 5). Si le nombre de pixels modifiés est assez faible, il est impossible de détecter quoi que ce soit en regardant l'image très peu modifiée qui circule sur le réseau. Le décodage est extrêmement facile : pour l'effectuer, il suffit de collecter les numéros codés dans les pixels aux emplacements convenus, de les interpréter pour reconstituer le texte secret que personne n'aura repéré dans l'image transmise. Des logiciels utilisant des versions perfectionnées de ce principe (et, pour certains, prenant en compte les difficultés introduites par les algorithmes de compression qui ne restituent pas parfaitement les images) peuvent être trouvés en passant par l'adresse *Internet* :

<http://adams.patriot.net/~johnson/html/neil/stegdoc/stegdoc.html>

Si l'on veut aujourd'hui surveiller tout ce qui transite par les réseaux informatiques, il ne suffit donc pas d'interdire par un règlement quelconque de coder les messages qui y circulent et d'aller ennuyer ceux qui ne respectent pas la loi, il faut aussi repérer tous les messages dissimulés par des méthodes de stéganographie, ce qui semble impossible. Pour rendre plus difficile encore la détection des messages cachés, les spécialistes recommandent de coder les messages que l'on noie. À la place d'images, on peut utiliser des sons ou des textes de programmes dans lesquels, par exemple, on redoublera certains blancs (ce qui est sans effet sur le fonctionnement du programme) pour marquer des emplacements spéciaux.

La loi française, une des plus répressives au monde en matière de cryptographie, est donc absurde et inutile malgré les modifications adoptées en juin dernier par les parlementaires. Elle restreint l'usage des méthodes cryptographiques, obligeant ceux qui veulent s'en servir à déclarer les méthodes qu'ils utilisent et à communiquer les clés de codage à des « tiers de



J.-P. Delahaye

5. Vous convenez avec votre compère d'une liste de pixels. Par exemple, ceux dont les coordonnées sont des multiples de 20. Vous remplacez dans une image *a* les pixels de la liste par d'autres correspondant aux numéros des lettres du message secret que vous voulez transmettre. Ici les lettres du mot «stéganographie» ont été codées chacune sur 8 digits, ce qui fait 112 digits, qui ont été placés dans l'image aux points de coordonnées multiples de 20. Le «0» est codé par un point blanc, le «1» par un point noir. Votre compère qui recevra l'image *b* saura la déchiffrer et en tirer le message secret. Personne ne verra et ne saura qu'il y a eu quelque chose de caché. Cette méthode (dont il existe des versions plus perfectionnées) pour transmettre des messages secrets sans que personne puisse soupçonner qu'un message est transmis ne paraît pas pouvoir être détectée.

confiance». À l'heure actuelle, les décrets d'application ne sont pas parus, mais il est probable que les tiers de confiance à qui on devra confier les clés seront aussi les vendeurs exclusifs des moyens de cryptographie autorisés et qu'en conséquence le cryptage sera cher, malcommode, incertain et hors de la portée du citoyen qui ne pourra cacher son courrier électronique (c'est le cas aujourd'hui).

Contrairement à ce que l'on considère comme naturel pour le téléphone et le courrier postal, le droit à avoir une correspondance privée n'existe donc pas sur les réseaux en France. Outre que la situation semble étonnante dans le pays des Droits de l'homme, une telle loi risque de pénaliser l'industrie française du logiciel et, d'une manière générale, toutes les firmes qui ont besoin de moyens sûrs pour protéger leurs communications.

Pourtant, si la loi gêne le citoyen honnête et la firme soucieuse de ses secrets, elle ne sert à rien contre ceux, qui pour des motifs invouables, souhaitent communiquer discrètement avec des compères à l'autre bout du monde et qui utiliseront – et utilisent déjà aujourd'hui – des méthodes de stéganographie.

Remarquons aussi que l'évocation de l'usage d'*Internet* par la Mafia ou par les réseaux pédophiles semble aux yeux de certains justifier toutes les censures et interdictions. Pourtant, le problème posé n'est pas très différent de celui du téléphone : a-t-on interdit l'usage du téléphone parce que les cambrioleurs

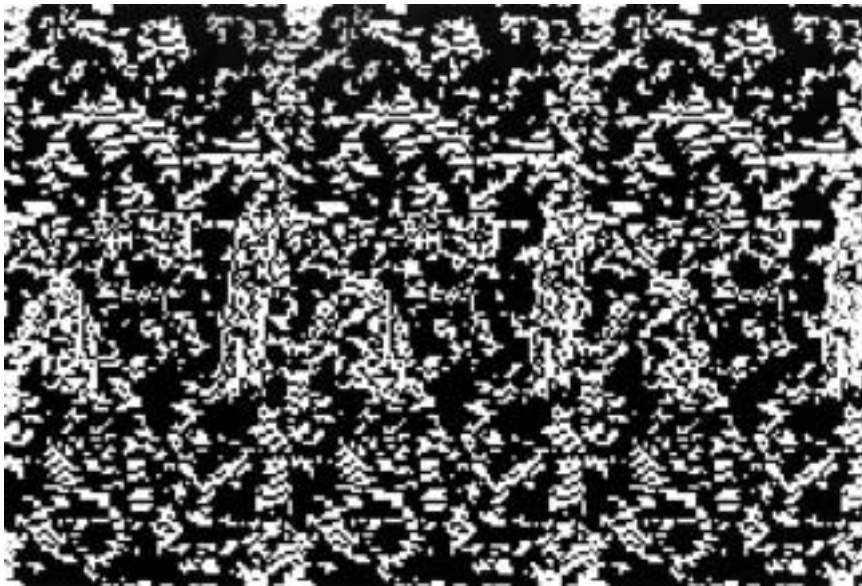
de banques ou les trafiquants d'enfants peuvent s'en aider pour monter leurs coups et organiser leurs trafics ?

LES MONOSTÉRÉOGRAMMES

Un autre type de stéganographie utilisant les images a été l'objet d'une mode récente : les monostéréogrammes. La possibilité de cacher une forme tridimensionnelle dans une image à motifs répétitifs, en faisant varier insensiblement le motif répété, est une découverte extraordinaire et crée une situation assez amusante en matière de codage. Les méthodes pour créer les monostéréogrammes sont fondées sur des procédés algorithmiques programmés. En revanche, le décodage des monostéréogrammes nécessite toujours un être humain. Ce n'est peut-être pas irrédicible, mais la situation mérite d'être notée : le codage est automatisé, le décodage non.

Ceux qui cherchent, parfois avec une ferveur quasi religieuse, des exemples de situations où l'homme est indubitablement supérieur à la machine et sont inquiets à propos de leur exemple favori (le jeu d'échecs), ou interprètent faussement les résultats d'indécidabilité de Gödel, devraient s'intéresser à ce cas étonnant.

Plus anciennes, mais dans la même veine picturale, les anamorphoses constituent une méthode de stéganographie qui a été pratiquée par de nombreux peintres : on ne découvre l'image cachée qu'en penchant le tableau ou en utilisant



J. Ninio

6. On a découvert récemment une nouvelle façon de cacher une image dans une autre. Pour voir l'image cachée (le mot «fin») : prenez l'image face à vous et collée contre votre nez et éloignez-la lentement : le relief va apparaître et le message. Patience. Ce stéréogramme a été mis au point par Jacques Ninio (ENS).

un miroir cylindrique. L'exemple le plus célèbre est celui du crâne caché dans le tableau de Hans Holbein *Les ambassadeurs*, peint en 1533.

QUELQUES RÉPONSES THÉORIQUES

L'idée qu'un message puisse comporter deux niveaux de lecture et même trois, comme nous l'avons évoqué à propos de la biologie, conduit à la question : est-il possible de créer des messages ayant une infinité de niveaux de lecture ? Que l'Univers soit un tel message est une idée qui nous amuse aujourd'hui, mais ne nous convainc pas, contrairement au Moyen Âge qui voyait des messages divins dans tous les objets du monde et trouvait séduisante cette perspective infinie de messages emboîtés. La théorie, par exemple, que chaque germe animal contient tous ses descendants enchâssés les uns dans les autres comme des poupées russes était communément admise, et en particulier fut défendue par Malebranche. Nous proposons de ramener le problème à une question mathématique précise.

Existe-t-il des messages infiniment profonds ? Pour simplifier le problème, imposons à la méthode de décodage d'être uniforme : pour lire le message de niveau n , on appliquera une méthode de décodage au message de niveau $n - 1$ et ce sera toujours la même méthode. La question rendue formelle est donc : «Peut-on créer une fonction de décodage f et un message infini M , tels que $M, f(M), f(f(M)), \dots$, soient des suites mathématiques intéressantes ?» (si l'on n'exigeait pas des

suites obtenues d'être intéressantes, la réponse serait trivialement oui).

Il existe sans doute plusieurs façons de répondre à cette question, je vais juste en présenter une. Imposons au message de n'utiliser que des «0» et des «1», et à la méthode de décodage d'être celle qui transforme chaque paire de symboles «01» en «0» et chaque paire «10» en «1». Remarquez que cela entraîne que le message de base et les messages codés ne contiennent que des paires «01» et «10».

Les contraintes sont maintenant tellement fortes que notre problème ne comporte plus que deux solutions (la seconde s'obtient en inversant le rôle des 0 et des 1 dans la première). Un peu de réflexion ou la lecture de la figure 4 vous les feront trouver.

Une des contraintes du problème semble avoir été oubliée : comment est-on certain que les messages codés à chaque niveau sont intéressants, ainsi que l'énoncé du problème le stipulait ? La réponse rappellera le paradoxe du plus petit nombre inintéressant (qui ne peut exister, car sinon il serait intéressant du fait de sa définition) et elle consiste à dire : (1) d'abord le message est le même à chaque niveau (c'est facile à vérifier) et donc il suffit de montrer que chacune des deux solutions est une suite intéressante ; (2) puisqu'il n'y a que deux solutions (et donc une seule à une inversion près des 0 et des 1), elles constituent des suites mathématiques remarquables et donc intéressantes.

La suite de profondeur infinie trouvée comme solution de notre problème possède toutes sortes de propriétés

remarquables. Elle s'appelle la suite de Prouhet-Thue-Morse et ne contient jamais trois fois consécutivement la même sous-séquence ; de plus, elle est stable lorsqu'on en enlève un élément sur deux (ce qui veut dire qu'une autre fonction de décodage que celle envisagée ci-dessus pourrait être utilisée) et c'est donc une sorte d'objet fractal : on la retrouve en elle-même en plus petit. Notons en passant que les objets fractals géométriques peuvent être vus comme des messages stéganographiques infiniment profonds se codant eux-mêmes.

LA STÉGANOGRAPHIE SUPERPURE ET DIEU

Toujours dans le domaine des mathématiques pures, Carl Sagan dans son roman *Contact*, dont le thème est la recherche d'intelligences extraterrestres envisageait un cas extraordinaire de stéganographie qu'on pourrait qualifier de «superpure» –, car le message anodin est le nombre π et ne contient donc rien d'arbitraire. En calculant les décimales assez loin, Carl Sagan imagine qu'on finit par y découvrir de longues plages composées essentiellement de zéros qui, lorsqu'elles sont alignées les unes contre les autres, font apparaître un dessin de cercle parfait. Cette improbable stéganographie dans un texte fixé de toute éternité était interprétée comme la signature d'une intelligence ayant précédé l'Univers. Si un jour on trouve un message dans les décimales de π (ce qui ne s'est pas produit aujourd'hui), alors je crois, comme Carl Sagan, qu'on pourra effectivement y voir une preuve absolue de l'existence de Dieu. N'avais-je pas dit que la stéganographie était importante ?

J. NINIO, *Stéréomagie*, Éditions du Seuil, Paris, 1994.

J. BALTRUSAITIS, *Anamorphoses*, Flammarion, Paris, 1984.

H. BROCH, *Le paranormal*, Éditions du Seuil, Paris, 1985.

J. GUISEL, *Guerres dans le cyberspace : services secrets et Internet*, La Découverte (Enquêtes), Paris, 1995.

D. R. HOFSTADTER, *Gödel, Escher, Bach ; les brins d'une guirlande éternelle*, Inter-Éditions, 1985.

D. KAHN, *La guerre des codes secrets : des hiéroglyphes à l'ordinateur*, Inter-Éditions, Paris 1980 (traduction de *The Codebreakers*, The Macmillan Company, New York, 1967).

B. SCHNEIER, *Cryptographie appliquée*, International Thomson Publishing, Paris, 1995.