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 époustouflants. 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 indécelable.

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 Prouet-Thue-Morse.

Si *s* commence par 1, on trouve que *s* est le message «en négatif» de la suite de Prouet-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.).

Document PLS

L'INTERDICTION DE CACHETER 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 clefs de codage à des «tiers de 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 clefs 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 cacheter 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 inavouables, 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 ?

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.

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 irrémédiable, 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