I. Définitions :

Stéganographie : (de stéganos caché et graphos écriture, comme cryptographie… alors où est la différence ?). La stéganographie est l'art de cacher un message (à l'intérieur d'un support quelconque). La stéganographie est l'art de cacher un message, alors que la cryptographie c'est coder (ou décoder) un message pour en cacher le contenu. Ce n'est pas coder un message pour en cacher le contenu qui serait la cryptographie.

Cryptographie : (de kruptos = caché et graphein = écrire) ensemble des techniques permettant de protéger une communication au moyen d'un code graphique.

Cryptologie : (de 'kryptos logos' soit 'mot caché') considérée comme la science du secret. Elle est composée de la cryptographie (codage) et du décryptement ou cryptanalyse (décodage).

Remarque : La stéganographie est l'art de cacher un message dans un support, alors que la cryptographie c'est coder (ou décoder) un message pour en cacher le contenu. La stéganographie peut être considérée comme une partie, une composante de la cryptographie.

La sécurité par l'obscurité :

La stéganographie repose sur l'idée de sécurité par l'obscurité : si personne ne sait qu'il y a un fichier caché, personne ne cherchera à le regarder ou le récupérer. Et avec tout ce qui passe sur l'internet, et le nombre de fichiers joints que les gens s'échangent, personne ne dispose de suffisamment de ressources informatiques pour scanner tous ces transferts d'images, sons et autres fichiers. Cela dit, certaines sociétés surveillent activement tous les envois de fichiers joints transitant par leurs réseaux informatiques internes, histoire de vérifier qu'aucun secret ne puisse en sortir.

Plausible Démenti :

De plus, il est beaucoup plus aisé à quelqu'un de nier avoir envoyé un message crypté et caché grâce à la stéganographie qu'à quelqu'un qui se serait contenté de seulement crypter le message avant de l'envoyer, puisque le chiffrement se voit à l'œil nu. A méditer... en plus, et dans l'hypothèse où l'on apprenne que l'image que vous avez envoyée à votre cousin Alfred contenait un fichier caché, qui peut prouver que c'est vous qui l'y avez placé, et qu'il n'était pas déjà présent lorsque vous l'avez trouvé ? Personne ne peut affirmer que vous saviez ce qu'il contenait réellement...

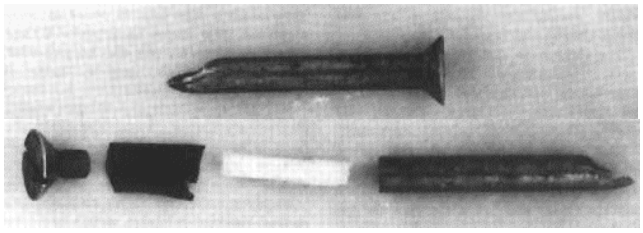
II. Quelques exemples célèbres :

Les grecs dans leurs messages, perçaient des petits trous d'aiguilles selon un code qui leur permettait d'envoyer un message codé inclus dans un message anodin.

Démératus réussit à prévenir Sparte de l'invasion de Xerxés en écrivant son message directement sur le bois de la tablette d'écriture, en dessous de la cire préparée pour écrire. Sa tablette semblait vierge de texte, il pu passer…

Toujours chez les grecs, il est arrivé de tatouer un message sur le crane d'un messager, qui partait quand ses cheveux avaient repoussé… Hérodote, un historien grec vivant au quatrième siècle avant Jésus-Christ, relate l'utilisation d'un des plus étrange moyen de communication que l'on connaisse. Un certain Histiée se trouvant à la cours de Perse et voulant prendre contact avec son gendre (le tyran Aristagoras de Milet) choisit un serviteur dévoué, lui rasa la tête, y tatoua le message et attendit la repousse des cheveux. Histiée l'envoya alors à Aristogoras avec instruction de lui raser le crane. L'ayant fait, celui-ci put lire le message. Il ne fallait pas être trop pressé, mais un petit coup de rasoir et la lecture se faisait sans problème.

Avec le temps on en vint à cacher des textes écrits à l'encre sympathique à l'intérieur de messages sans importance. Le passage d'une solution chimique révélait le véritable contenu.



Une petite illustration de l'imagination humaine avec ce message camouflé dans un clou, lui-même enfoncé dans une planche de bois :

Certains amoureux des lettres parvenaient à écrire « un texte dans le texte ». On citera l'exemple célèbre de correspondance entre George Sand et Alfred de Musset où le texte devait être lu selon une règle simple à trouver. Le document est connu, facile à retrouver sur internet…

Chaque semaine « le canard enchaîné », journal satirique, propose un titre stéganographique. Il s'agit d'une contrepèterie que pas tout le monde comprend.
Exemples de contrepèteries : pendant que le ministre de l'éducation nationale M. Allègre invectivait les profs, sur une pancarte on pouvait lire « assez de mots sinistres » qui se traduit en échangeant deux lettres… le m de mots et le s de sinistres. Le message change de sens !
Sur une autre pancarte on pouvait lire « mon métier professeur », si l'on intervertit le m et le t de métier avec le f et les deux s de professeur… c'est une contrepèterie très certainement indépendante de la volonté de son auteur, c'est amusant tout de même !

L'informatique offre une source extraordinaire de cachettes de messages à l'intérieur de tout ce qui peut se transporter tels que les messages électroniques, les documents partagés en réseau (internet est un grand réseau), les images ou les sons récupérés sur les pages de sites d'apparence insignifiante. Quelques exemples (on ne voit rien dans ce texte… dont le fichier contient peut être un message secret ! il faut pour chaque image utiliser un logiciel particulier, pas trop difficile à fabriquer, et encore moins à récupérer sur la toile) :

Actuellement, les virus, vers, chevaux de Troie et autres calamités pour nos ordinateurs utilisent la stéganographie… ils se cachent à l'intérieur de messages anodins, pour mieux envahire nos micros.

L'après 11 septembre 2001 à beaucoup fantasmé sur l'usage de la stéganographie. Les services secrets américains ont dit soupçonner les terroristes comme Ben Laden d'utiliser des sites internet contenant des images (par exemple) leur permettant de cacher leurs messages.

III. Où et comment cacher l'information secrète ?

Selon la forme sous laquelle l'information non secrète est transmise, différentes voies sont possibles pour cacher de l'information.

Texte :

Le placement des ponctuations, l'introduction de variations orthographiques ou typographiques, le choix entre des synonymes ou des formes grammaticales, l'espacement entre les mots sont des façons simples d'ajouter de l'information sans perturber l'information originale.
D'autres techniques plus subtiles mais aussi plus délicates à mettre en œuvre, consistent à offrir d'autres clefs de lecture en utilisant que certaines lettres ou les lettres dans un certain ordre.
On peut aussi utiliser un générateur de texte 'aléatoire' basé sur une sorte de 'grammaire'. Les choix faits pour la génération du texte correspondent au message secret.

Son :

De faibles variations, imperceptible pour l'oreille, dans les basses fréquences ou ce que l'on appelle le bruit de fond peuvent contenir une grande quantité d'information. Un grésillement infime peut cacher des secrets. Evidemment, ce bruit doit de préférence être transmis de façon numérique sans quoi les vrais pertes de transmission pourraient effacer entièrement le message caché.
Afin de rester indécelable, le bruit artificiel doit posséder les propriétés statistiques d'un vrai bruit de fond.

Image :

De la même manière que pour le son, des variations dans les basses fréquences de l'image peuvent contenir de l'information. Lorsque le transfert d'information est numérique, d'autres détails du codage de l'image, telle la palette de couleur, peuvent également contenir des informations. Pour le 'watermarking' on préférera reproduire plusieurs fois la signature dans les zones les plus contrastées pour que celle-ci résiste le plus possible à des modifications de l'image.

Autres :

Naturellement, il existe autant d'endroits où cacher de l'information qu'il existe de formats et de types de données, les plus fréquemment utilisés étant les plus anodins. On peut penser facilement aux formats multimédia, mais aussi aux formats de compression, d'archive et d'encodage. Même une simple page HTML peut contenir plus que ce vous pouvez y voir à travers votre outil de navigation.

Il existe aussi aux moins deux classes de techniques faisant partie de la stéganographie mais suffisamment particulières pour mériter un nom.

Filigrane (‘watermarking’) :

- Protéger les possesseurs de copyright sur des documents numériques en cachant une signature dans l'information de sorte que même une partie modifiée du document conserve la signature.
- Découvrir l’origine de fuites en marquant de façon cachée et unique chaque copie d’un document confidentiel.

Canal de communication secrète (‘cover channel’) :

- Permettre à des partenaires de communiquer de façon secrète en établissant un véritable protocole de communication secrète au dessus d’autres protocoles anodins.
- Permettre une communication non autorisé à travers les communications autorisé d’un firewall.

Ces techniques peuvent être utilisées par les agents secret, les mafias et les extra-terrestres qui tous veulent rester bien cachés. Naturellement, l’honnête homme a tout autant de raisons d’utiliser ces techniques.

Un argument utilisé par les états pour interdire la cryptographie est de dire que les citoyens honnêtes n’ont rien à cacher et de soupçonner tous ceux qui utiliseraient de telles techniques. Cette logique appliquée au courrier interdirait l’usage des enveloppes et n’autoriserait que les cartes postales.

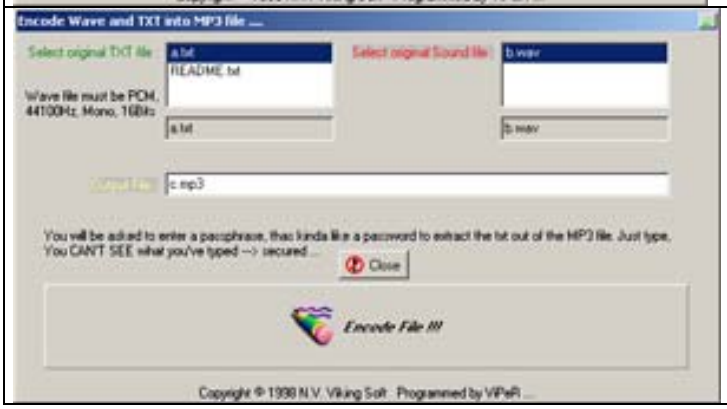
IV. Deux exemples en temps réel :

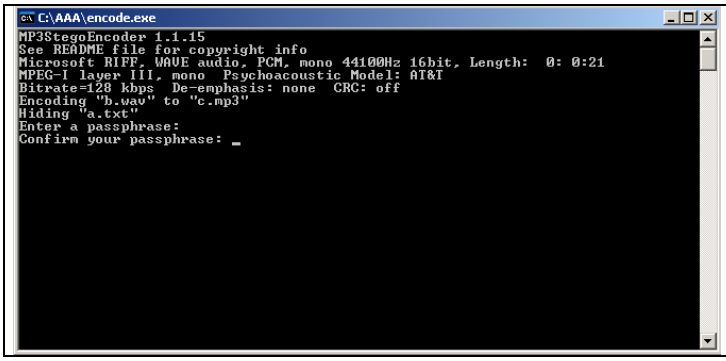
Une adresse internet où trouver de nombreux logiciels de stéganographie : http://www.stegoarchive.com/

Fichiers son :
Il faut récupérer un utilitaire sur internet (ou savoir le fabriquer…). Par exemple MP3Steno.

Adresse où récupérer : http://www.petitcolas.net/fabien/steganography/mp3stego/index.html

Décompacter dans un répertoire. Amener le fichier texte (a.txt) et le fichier son (b.wav qui est le début de la 40ième de Mozart) dans ce répertoire. ATTENTION : ce fichier wav doit être en mono, pas en stéréo. Rappel : le format wav prend beaucoup de place, compter 10 Mo par minute !

	Lancer MP3Steno.exe, qui propose codage ou décodage.
	Codage :montre les fichiers possibles. a.txt et b.wav Entrer le nom du fichier de sortie (ici c.mp3) en minuscules (il me semble). Cliquer sur Encode file.

	Il est demandé d'adjoindre un mot de passe… on peut appuyer sur Entrée. Et cela fabrique un vrai fichier MP3 qui ne diffère pas (musicalement) du premier. Le décodage s'obtient avec le même logiciel.

Contenu du message : ouvrir (par l'explorateur, le poste de travail…) le fichier portant l'extension .txt du même nom que le fichier MP3 créé. Texte du message : Ce message est secret bien qu'il s'affiche aux yeux, ou plutôt aux oreilles de tous.	Il suffit de choisir Decode txt puis d'entrer le mot de passe choisi. Il est créé le fichier c.mp3.txt

Fichiers image :

J'utilise le petit logiciel HIP 20 (Hide In Picture 2.0 Freeware) qui ne travaille que sur des bmp. Le logiciel JPGX toujours à capturer sur internet : ne "pèse" que 64 Ko et s'occupe du format jpeg.

	Après l'avoir décompacté dans un répertoire, hip20 par exemple, amener une image (format bmp uniquement) et un fichier texte. Lancer winhip.exe. Un petit explorateur apparaît. Aller dans le répertoire hip20 cliquer sur le nom de l'image. Une fenêtre avec menu (icones) apparaît. C'est hyper simple ! Inclure le message, mettre un éventuel mot de passe et sauvegarder. Fastoche !!! Et il suffit de cliquer sur l'icône de décodage pour aller dans l'autre sens, en donnant au fichier texte le nom qu'il nous plait.

En conclusion :

La stéganographie c'est facile (pour l'utilisateur), c'est compliqué (pour celui qui essaye de décoder), c'est amusant (entre copains), c'est inquiétant (services secrets, terrorisme), comme la langue, c'est sans doute la meilleure et la pire des choses !