TECHNIQUES DE STEGANOGRAPHIE

PIGNON Camille

Sommaire :

Introduction

Si la cryptographie est l'art de cacher le sens d'un message, la stéganographie, beaucoup moins connue et même absente de la plupart des dictionnaires, est l'art d'en cacher le contenu. Elle permet de faire passer une information sans que les personnes susceptibles de l'intercepter aient même conscience de son existence et ce au travers d'un support anodin appelé « stégo-médium » au contenu visiblement tout aussi anodin. C'est pourquoi il s'agit d'une arme redoutable dans l'art d'envoyer des données de manière sécurisée. Tout comme sa consoeur la cryptographie, la stéganographie existe depuis l'antiquité bien qu'à cette époque, il était beaucoup plus compliqué et long d'appliquer de tels procédés. Heureusement, avec l'avènement de l'informatique, cette discipline, tout comme beaucoup d'autres à nettement évoluer et permet aujourd'hui de masquer facilement et rapidement toutes sortes de données : texte, images, vidéos, bande sonore, bref tous les médias et moyens de communications contemporains. Couplé avec la cryptographie, elle permet une sécurité maximum à l'envoi d'informations et diminue grandement les risques d'interception et de prise de connaissance de ces données confidentiels par un « ennemi » ou à défaut une personne n'étant pas le destinataire visé du message.

Le but de cet article est de décrire les principales techniques de stéganographie d'avant et d'aujourd'hui : des techniques utilisées dans l'antiquité en temps de guerre ou par les espions à celles mises en oeuvre de nos jours et permises récemment grâce à l'informatique, dans le but de répondre à la question suivante : Comment peut-on cacher une information dans un support externe pour la transmettre de manière sécurisée? Encore une fois, les techniques sont nombreuses et toutes aussi efficaces si on ignore l'existence même d'un message. Entrons de suite dans le vif du sujet...

Anecdotes historiques

La plus vieille histoire dont on est connaissance à propos de la stéganographie remonte à l'époque d'Hérodote. C'est en effet dans son oeuvre Histoire, Livre V où il décrit comment Histiée qui voulait ordonner à Aristagoras de se soulever contre contre son roi Darius lui fit passer le message malgré la surveillance accrue sur les routes. Voici comment il s'y pris : il fit raser la tête de l'un de ses plus fidèles esclaves, écrivit le message sur son crâne et attendit que les cheveux repousse avant de l'envoyer à Milet, où se trouvait Aristagoras, avec pour ordre de dire à son arrivée qu'il fallait lui raser la tête. Ainsi celui-ci pu prendre connaissance de l'ordre de se révolter et c'est ce qu'il fit.

Voici l'extrait du livre V d'Histoires d'Hérodote qui relate cette anecdote :

[5,35] XXXV. Aristagoras ne put tenir la promesse qu'il avait faite à Artapherne. On exigeait de lui les frais de l'expédition, et cela l'inquiétait. Comme Mégabate l'accusait, il craignit qu'on ne lui imputât le mauvais succès de l'entreprise, et se crut sur le point d'être dépouillé de la souveraineté de Milet. Ces sujets de crainte lui firent prendre la résolution de se révolter. Sur ces entrefaites, il arriva de Suses un courrier qui lui enjoignait de prendre les armes. Cet ordre était empreint sur la tête du courrier. Histiée, voulant mander à Aristagoras de se soulever, ne trouva pas d'autre moyen pour le faire avec sûreté, parce que les chemins étaient soigneusement gardés. Il fit raser la tête au plus fidèle de ses esclaves, y imprima des caractères, et attendit que ses cheveux fussent revenus. Lorsqu'ils le furent, il l'envoya aussitôt à Milet, avec ordre seulement de dire, à son arrivée, à Aristagoras de lui raser la tête, et de l'examiner ensuite. Ces caractères, comme je viens de le dire, lui ordonnaient de se révolter. Histiée prit cette résolution, parce qu'il se trouvait très malheureux d'être retenu à Suses, et qu'il avait de grandes espérances que, si Milet se soulevait, Darius l'enverrait vers la mer pour lui amener Aristagoras. Il sentait, en effet, que, s'il ne suscitait point de troubles en cette ville, il n'y retournerait jamais.

Hérodote décrit aussi dans sa même oeuvre comment, voulant informer les Spartiates de l'attaque imminente des Perses, Démarate prit des tablettes de cire, racla la cire pour y écrire les informations directement sur le bois puis recouvrit les tablettes de cire à nouveau. De ce fait, elles passèrent inaperçu.

Les chinois de l'antiquité, quant à eux, écrivaient leurs messages sur de la fine soie qu'ils roulaient en boule avant de la recouvrir d'une couche de cire. Le messager n'avait plus qu'à avaler la boule et aller la donner au destinataire.

Au XVI siècle, Giovanni Porta découvrit comment cacher un message dans un oeuf dur :
On fabrique une encre à partir d'une once d'alun pour une pinte de vinaigre. Il suffit ensuite d'écrire sur la coquille de l'oeuf avec cette encre, celle-ci traverse la coquille et va « s'imprimer » sur le blanc dur de l'oeuf. Pour lire, il n'y aura plus qu'à l'éplucher pour pouvoir lire le message qui y est inscrit directement sur le blanc.

Bien sûr, la notion du mot « urgent » n'était pas la même à l'époque qu'aujourd'hui sans les moyens de transports et de communications actuels et il ne serait pas possible d'utiliser ce genre d'astuces de nos jours pour transmettre des messages de cette importance en urgence mais il s'agit des premières apparition de la stéganographie qui a conduit et inspirée toutes les autres.

L'encre invisible

Au Ier siècle avant J.-C., Pline l'Ancien décrivit comme fabriquer et utiliser l'encre invisible encore appelée « encre sympathique » avec le lait. Depuis lors, elle a beaucoup évoluée et divers moyens d'en fabriquer ont été trouvés, plus encore depuis les progrès des derniers siècles en chimie.
Voici divers moyens d'en fabriquer et comment l'utiliser :

Encres apparaissant avec une flamme :

- Le vinaigre, donnant une couleur rouge une fois chauffé.
- Le jus de citron, donnant une couleur brin-roux.
- L'oignon pressé qui donne une couleur noirâtre.
- Le jus de cerise qui devient vert après avoir été chauffé.
- La plupart des sucs ou acides provenant des fruits.
- Le lait qui tourne jaunâtre une fois chauffé.
- Depuis qu'ils existent, l'encre des effaceurs peut être utilisée et donne la même couleur que le jus de citron après avoir été chauffée.

Encres chimiques

- Un volume d'Eau-Blanche (ou Ether diéthylique) pour cinq d'eau.

L'encre apparaît en tamponnant avec un coton imbibé d'un dissolvant.

- Une moitié de laxatif (contenant de la phénolphtaléine), deux cuillères à café d'ammionaque et deux cuillères à soupe d'eau.

L'encre apparaît avec une solution de cristaux de soude dans l'eau.

- Un volume d'alun pour cent d'eau.

L'encre apparaît à la chaleur (grâce à un fer à repasser chaud par exemple).

- Chlorure de cuivre dilué.

L'encre apparaît à la chaleur et disparaît à nouveau lors du refroidissement.

- Cuivre dissout dans de l'acide chlorhydrique plus quelques gouttes d'acide nitrique.

Cette encre apparaît également à la chaleur.

- Solution de nitrate de cobalt dans laquelle du nitrate de nickel à été ajouté.

Il faut chauffer le support pour faire apparaître l'écrit.

- Solution aqueuse de chlorate de soude

On peut rendre l'écriture visible en passant sur le support une éponge légèrement imbibée de vitriol de cuivre.

- Un volume d'Eau Forte et trois d'eau.

L'encre apparaît en trempant la feuille dans l'eau.

Pour utiliser l'encre sympathique que l'on vient juste d'obtenir, il suffit d'utiliser une plume ou un pinceau que l'on imbibe avec la solution pour écrire sur un support quelconque : papier, carton, journal, etc. et d'y rajouter un message anodin écrit visiblement, avec un crayon « normal » pour ne pas attirer l'attention en envoyant une feuille blanche. Il ne manquera au destinataire plus qu'à utiliser la méthode permet de faire apparaître le message en fonction de la solution utilisée.

La liste de ces méthodes n'est bien sûr pas exhaustive mais celles notées ci-dessus sont les plus utilisées et on voit qu'elles ne demandent pas beaucoup de compétences techniques pour être réalisées : il ne faut même pas être un chimiste aguerri d'où la facilité de l'utilisation de l'encre invisible. C'est d'ailleurs la raison pour laquelle, les allemands l'ont choisi pour faire passer leurs messages pendant la Seconde Guerre Mondiale : ils cochaient certaines lettres des journaux à l'encre sympathique avant de se les envoyer. Ne restait plus qu'au destinataire à les rendre visible puis à relier le tout pour obtenir le message.

Petit + :

Ils utilisaient aussi le micropoint qui consiste en la diminution d'une photographie ou d'une image jusqu'à ce que celle-ci ait la taille d'un point.

La stéganographie pure

La première question est : Qu'est-ce que la stéganographie pure?

En fait, c'est extrêmement simple : toutes les méthodes décrites précédemment le message à cacher est directement sur le support, il s'agit d'une modification du support en lui-même et non de son contenu. La stéganographie pure, quant à elle, ne modifie pas le support directement mais son contenu : par exemple, le message à envoyer est caché dans un autre texte...

L'acrostiche

L'acrostiche est la forme la plus simple de stéganographie pure. Dans cette figure de style, utilisée tantôt comme moyen de stéganographie, tantôt par les littéraires pour donner du style à leurs oeuvres, si l'on prend la première lettre de chaque mot ou de chaque vers ou le premier mot de chaque vers, ils doivent former respectivement un mot ou une phrase.

Illustrons ce propos par un exemple bien connu qui est un courrier et sa réponse que Alfred de Musset aurait envoyé à Georges Sand (véridicité de ce fait remise en cause du fait qu'il n'y ait aucune trace de ces lettres dans leur correspondance). Voici ces lettres :

Quand je mets à vos pieds un éternel hommage
Voulez-vous qu'un instant je change de visage ?
Vous avez capturé les sentiments d'un cour
Que pour vous adorer forma le Créateur.
Je vous chéris, amour, et ma plume en délire
Couche sur le papier ce que je n'ose dire.
Avec soin, de mes vers lisez les premiers mots
Vous saurez quel remède apporter à mes maux.

Bien à vous, Eric Jarrigeon

Cette lettre est la réponse de Alfred de Musset à une première lettre de Georges Sand qui sera exposé par la suite car il ne s'agit pas d'un acrostiche. Pour celle-ci, il faut ne lire que le premier mot de chaque vers.
Voici la réponse de Georges Sand toujours sur le même principe :

Cette insigne faveur que votre cour réclame
Nuit à ma renommée et répugne mon âme.

Il existe d'autres formes, moins connues que l'acrostiche qui repose sur le même moyen de stéganographie : c'est-à-dire ne lire que le premier mot d'un vers ou alors que le dernier, etc...

C'est ainsi que le mésostiche est la figure de style qui est utilisée quand les lettres

médianes d'un poème forment un mot et que le téléstiche est la même chose que l'acrostiche sauf qu'il faut lire uniquement la dernière lettre ou le dernier mot de chaque vers. Enfin, la combinaison de l'acrostiche et du téléstiche s'appelle l'acroteleuton.

Il existe bien sûr une infinité de techniques du même genre en plus évoluées pour cacher un message où il est imperceptible de savoir quelles lettres ou quels mots regarder. En guise d'exemple, voici la première lettre envoyée à Alfred de Musset par Georges Sand dans laquelle on trouve de la stéganographie. Elle précède les deux lettres figurant un peu plus haut.

Je suis très émue de vous dire que j'ai
bien compris l'autre soir que vous aviez
toujours une envie folle de me faire
danser. Je garde le souvenir de votre
baiser et je voudrais bien 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 cal-
cul, et si vous voulez me voir aussi
vous dévoiler sans artifice mon âme
toute nue, venez me faire une visite.
Nous causerons en amis, franchement.
Je vous prouverai que je suis la femme
sincère, capable de vous offrir l'affection
la plus profonde comme la plus étroite
en amitié, en un mot la meilleure preuve
dont vous puissiez rêver, puisque votre
âme est libre. Pensez que la solitude où j'ha-
bite est bien longue, bien dure et souvent
difficile. Ainsi en y songeant j'ai l'âme
grosse. Accourrez donc vite et venez me la
faire oublier par l'amour où je veux me
mettre.

Pour celle-ci, il faut ne lire qu'une ligne sur deux pour en tirer le vrai sens.

Un autre exemple :

Apparently neutral's protest is thoroughly discounted and ignored. Isman hard it.
Blockade issue affects pretext for embargo on byproducts, ejecting suets and vegetable oils.

Pour celui-ci, il faut prendre la deuxième lettre de chaque mot qui nous donnent :

Pershing sails from NY June 1.

Il est ici question de l'arrivée de bateaux de type « Pershing », qui sont des bateaux de guerre, en provenance de New York le 1er juin.

Le code de l'Abbé Jean de Trithème

A mi-chemin entre la cryptographie et la stéganographie, on trouve le code de l'abbé Jean de Trithème. Il s'agit d'une substitution monoalphabétique où chaque lettre est remplacée par un mot ou un groupe de mots comme « à tout jamais », « dans la félicité » ou encore « à perpétuité » et qui donne l'illusion une fois le message chiffré qu'il s'agit d'une litanie (prière) anodine. C'est un bel exemple de ce qu'il est possible de faire en associant cryptographie et stéganographie. Voici la table de correspondance des lettres et des groupes de mots qui leurs sont associées :

A	Dans les cieux
B	À tout jamais
C	Un monde sans fin
D	En une infinité
E	À perpétuité
F	Sempiternel
G	Durable
H	Sans cesse
I, J	Irrévocablement
K	Eternellement
L	Dans la gloire
M	Dans la lumière
N	En paradis
O	Toujours
P	Dans la divinité
Q	Dans la déité
R	Dans la félicité
S	Dans son règne
T	Dans son royaume
U, V, W	Dans la béatitude
X	Dans la magnificence
Y	Au trône
Z	En toute éternité

Un exemple de l'utilisation de ce code pour chiffrer et stéganographier l'information suivante : « La récupération se fera demain à midi. »

Dans la gloire et dans les cieux
Dans la félicité et à perpétuité
Un monde sans fin dans la béatitude
Dans la divinité et à perpétuité
Dans la félicité et dans les cieux
Dans son royaume et irrévocablement
Toujours en paradis
Dans son règne et à perpétuité
Sempiternel à perpétuité
Dans la félicité et dans les cieux
En une infinité et à perpétuité
Dans la lumière et dans les cieux
Irrévocablement et en paradis
Dans les cieux et dans la lumière
Irrévocablement et en une infinité
Irrévocablement

Le problème de ce genre de code est la répétition, une simple analyse des fréquences comme on en ferait avec un cryptogramme classique permet de le briser s'il est suffisamment long, ce qui est le cas si l'information à cacher est suffisamment longue aussi. De plus, il faut du temps pour chiffrer et stéganographier un texte dès qu'il devient conséquent et le cryptogramme en devient lui très long.

Le Barncode

Le Barncode est une méthode de stéganographie assez complexe qui ressemble à une lettre anodine une fois le message traité.

Exemple :

Mon cher Pierre,

J'espère que tu voudras bien m'excuser, mais j'ai eu tellement de travail à la maison que je n'ai pas pris le temps d'écrire aux amis. Cependant je t'envoie ce petit mot d'urgence pour te faire savoir que si tu veux des pneus, tu ferais bien de te dépêcher ; en effet :

Hier, Jean est venu nous rendre visite, il descendait du train et s'est arrêté un moment chez nous pour bavarder et donner des nouvelles à mon père de son Paris. En principe, il doit rester quelques jours ici pour mettre en ordre ses affaires avant de repartir pour la capitale. A Paris, c'est calme, mais la veille il avait été dérangé en plein sommeil par les sirènes deux fois dans la nuit ! Ceci mis à part, il doit nous faire envoyer par un ami à lui des pneus neufs pour nos vélos. Il en a pour le moment, profitons-en ! A bientôt de tes nouvelles.

P.-S. Nous irons au mariage de Simone et Henri, dimanche en quinze. Henri est un garçon sympathique qui a connu Simone l'an dernier chez Xavier, notre vieil ami. Il a deux ans de plus qu'elle et nous pensons que Simone va être très heureuse.

Pour trouver le message caché, il faut prendre le dixième mot du texte : ici c'est « Tellement », le placer dans un tableau comme une clef avec son équivalence numérique en dessous puis on y case le texte mot par mot par rangées :

T	E	L	L	E	M	E	N	T
8	1	4	5	2	6	3	7	9
Hier	**Jean**	Est	Venu	Nous	Rendre	Visite	Il	Descendait
Du	Train	Et	S'est	**Arrêté**	Un	Moment	Chez	Nous
Pour	Bavarder	Et	Donner	Des	Nouvelles	**À**	Mon	Père
De	Son	**Paris**	En	Principe	Il	Doit	Rester	Quelques
Jours	Ici	Pour	**Mettre**	En	Ordre	Ses	Affaires	Avant
De	Repartir	Pour	La	Capitale	**A**	Paris	C'est	Calme
Mais	La	Veille	Il	Avait	Eté	Dérangé	**En**	Plein
Sommeil	Par	Les	Sirènes	Deux	Fois	Dans	La	Nuit
Ceci	Mis	À	Part	Il	Doit	Nous	Faire	**Envoyer**
Par	**Un**	Ami	A	Lui	Des	Pneus	Neufs	Pour
Nos	Vélos	Il	En	**A**	Pour	Le	Moment	Profitons
En	A	Bientôt	De	Tes	Nouvelles			

Le texte apparaît ensuite lu horizontalement, un mot par ligne, repéré à la ligne indiquée par la valeur numérique de la clé dans cette colonne. Ce qui nous donne ici : « Jean arrêté à Paris. Mettre A en sommeil. Envoyer un A. »

Il a été convenu que les mots trop explicites devaient être remplacés par un « A ».

Ils sont en fait stéganographiés et chiffrés par un Playfair dans le Post-Scriptum.

Par convention, le code commence avec la première lettre du quatrième mot, puis on saute chaque fois trois mots.

"Nous irons au **mariage** de Simone et **Henri**, dimanche en quinze. **Henri** est un garçon **sympathique** qui a connu **Simone** l'an dernier chez **Xavier**, notre vieil ami. **Il** a deux ans **de** plus qu'elle et **nous** pensons que Simone **va** être très heureuse." Soit: **M**ariage, **H**enri, **H**enri, **S**ympathique, **S**imone, **X**avier, **I**l, **D**e, **N**ous, **V**a.

Le texte chiffré à décoder est: MH HS SX ID NV. Avec la clé correspondante, on reconstitue la table de Playfair puis on déchiffre pour obtenir nos deux mots.

Ici, ils donnent :

Premier «A » = Réseau
Deuxième « A » = OPR (opérateur de liaison)

Au final, on obtient : « Jean arrêté à Paris. Mettre réseau en sommeil. Envoyer un opérateur de liaison. »

La stéganographie informatique

Depuis les récents progrès en informatique, la stéganographie informatique est devenue à la mode, laissant de côté les autres techniques toujours aussi efficaces mais un peu tombées dans l'oubli dans un monde qui vit à l'ère du numérique.

Cacher du texte dans une page web

La méthode de stéganographie la plus simple qui soit est sûrement celle qui consiste à cacher du texte dans une page (x)HTML. Ce langage de développement web interprète en effet de manière identique un, deux ou trois voire beaucoup plus d'espaces. Il suffit donc, par exemple d'associer une valeur numérique à chaque lettre de l'alphabet et de mettre entre chaque mot autant d'espaces que la valeur de la lettre numérique à inscrire.

Exemple :

ILLUSION donne
9 12 12 21 19 9 15 14

Voilà ce que cela donnerait dans le code HTML de la page :

Bienvenue sur mon site ! J'espère que vous y trouverez votre bonheur!

Et ce que les visiteurs verront sur la page du site :

Bienvenue sur mon site ! J'espère que vous y trouverez votre bonheur!

Avantage : facile à cacher et il suffit d'un simple navigateur pour afficher le code source et retrouver le texte stéganographié.

Inconvenient : L'ouverture, l'enregistrement avec un logiciel d'édition comme Front Page peut suffire à perdre les données!

Cacher du texte dans une image

Cacher une information dans un support média numérique comme une image est sans la plus intéressante des nouvelles possibilités de la stéganographie.
Une image n'est finalement rien d'autre qu'une succession de pixels, point microscopiques, de couleurs différentes qui représente les formes, le dessin ou la photo que l'on a prise.

Chaque couleur présente sur les différents pixels est représentée par 3 nombres codés sur 8 bits (de 0 à 255 en décimal donc) qui forment en décimal le code RGB de couleurs (R = Red, G = Green, B = blue, les 3 couleurs primaires). Le blanc est par exemple représenté : R = 11111111 G = 11111111 B = 11111111 et le noir :

R = 00000000 G = 00000000 B = 00000000

Si l'on modifie ne serait-ce que le dernier bit de chaque couleur primaire composant la couleur de chaque pixel (soit plus simplement dit, le dernier chiffre de chacun des trois nombres du code RGB définissant la couleur) ou même les 2 derniers, cela serait imperceptible par l'oeil nu car la nuance ne serait que de 3 au maximum (11 en binaire) sur 255 nuances possibles, ce qui est bien sûr trop peu pour être visible par un oeil humain. C'est de cette manière que sont dissimulés des messages dans une image : on converti le message en binaire puis on remplace les deux derniers bits du rouge du premier pixel par les deux premiers bits de l'information à cacher, puis les deux derniers bits du green par les deux suivants du texte, idem pour le vert puis on continue avec le pixel suivant. A la fin de l'opération, il est impossible de voir une différence entre l'image initiale et l'image qui sert de stégo-médium.

Exemple :

Prenons le message, « 110011001011 »

Avec la partie d'image : R = 10010100 G = 10110111 B = 10101010
R = 10010101 G = 10111000 B = 10101110

On masque le message et on obtient :

R = 10010**11** G = 10110**00** B = 10101**11**
R = 10010**00** G = 10110**10** B = 10101**11**

La modification pour couleur primaire est donc entre 0 et 3 sur 255 soit totalement invisible.

Cacher une image dans une image

Pour cacher une image dans une autre image, il n'y a pas grand chose à expliquer : au lieu de coder les bits d'un texte sur les bits de poids faible de l'image support, il suffit de coder les bits des couleurs de chaque pixel à la place. On se rend compte néanmoins que l'on doit dans ce cas avoir une image support beaucoup plus grande que l'image à masquée du fait que l'on sépare une couleur primaire d'un pixel sur 1 pixel et le tiers d'un autre (de quoi insérer 8 bits en utilisant les deux derniers de chaque couleur primaire). Ou alors, il faut utiliser plus de bits pour chaque couleur de chaque pixel mais dans ce cas, il faut faire attention à ne pas prendre une trop grande partie de la couleur sinon l'image une fois l'autre image stéganographiée risque d'être visiblement différente de l'originale.

Conclusion

En conclusion, la stéganographie est un domaine important de la sécurité des communications qui existe depuis l'Antiquité comme la cryptographie. Les techniques possibles sont quasi-infinies et uniquement limitées par les limites de l'esprit humain. Depuis le développement de l'informatique, la stéganographie a très nettement évoluée vers le monde moderne et permet de cacher des informations de manière beaucoup plus sophistiquée et sécurisée que les techniques moins récentes mais qui sont toutes aussi efficaces quand elles sont utilisées dans le bon contexte.

La plupart des techniques présentées ici sont les techniques les plus importantes, il en existe beaucoup d'autres permettant par exemple de cacher du texte dans du son ou dans une vidéo ou une image dans une vidéo, etc mais elles sont plus compliqués. La liste des techniques n'est donc pas exhaustive, très loin de là.