

Introduction

L'information a toujours été convoitée et recherchée. Depuis fort longtemps, l'Homme essaie de dissimuler certaines informations au regards des autres, tout en désirant percer les secrets de ses congénères.

Nous n'aborderons pas ici la cryptographie, moyen le plus répandu d'empêcher les autres d'intercepter un message. En effet nous aborderons un sous domaine de la dissimulation d'information : *la stéganographie*.

Historique

Ethymologie

C'est un mot issu du grec *steganos*, signifiant *couvert* et *graphein*, signifiant *écriture*. L'éthymologie de ce mot le définit assez bien : la stéganographie (*écriture couverte*) qui est l'art de la dissimulation, à l'opposé de la cryptographie qui est l'art du secret.

En effet, l'objet de la stéganographie n'est pas de rendre un message inintelligible mais de le rendre furtif. Par analogie, crypter peut être assimilé à poser une serrure sur un coffre, la stéganographie serait d'enterrer le coffre.

Anciennes méthodes

La stéganographie existe depuis très longtemps. Citons par exemple *L'Enquête*, de l'historien grec Hérodote : en 484 av JC, Xerxès, le roi Perse décide d'envahir la Grèce. Il prépare son armée et déclare la guerre quatre ans plus tard. Or, les Grecs sont depuis le début au courant de ses intentions. En effet, Démarate, un réfugié originaire de Grèce a ainsi transmis l'information : «il prit une tablette double, en gratta la cire, puis écrivit sur le bois les projets de Xerxès; ensuite il recouvrit de cire son message : ainsi le porteur d'une tablette vierge ne risquait pas d'ennuis». Dans la même oeuvre historique, « il fit raser la tête de son esclave le plus fidèle, lui tatoua son message sur le crâne et attendit que les cheveux eussent repoussé; quand la chevelure fut redevenue normale, il fit partir l'esclave pour Milete».

Parmi les autres astuces historiques, on note les encres invisibles, les messages cachés dans des oeufs durs (en écrivant sur la coquille à l'aide d'une solution de vinaigre et d'alun), les minuscules trous d'épingle dans des caractères sélectionnés, message camouflé dans un clou lui-même enfoncé dans une planche de bois.

En Chine, on écrivait le message sur de la soie, qui ensuite était placée dans une petite boule recouverte de cire. Le messager avalait ensuite cette boule.

Dès le 1er siècle av JC, Plinie l'Ancien décrit comment réaliser de l'encre invisible. Les enfants de tous les pays s'amusaient à le faire en écrivant avec du lait ou du jus de citron : le passage de la feuille écrite sous un fer à repasser chaud révèle le message.

Durant la Seconde Guerre Mondiale, les agents allemands utilisaient la technique du micropoint de *Zapp*, qui consiste à réduire la photo d'une page en un point d'un millimètre voire moins. Ce point est ensuite placé dans un texte normal, au dessus d'un 'j' ou d'un 'i'.

Pourquoi la stéganographie

Dans la plupart des cas, c'est l'art de cacher un message secret au sein d'un message anodin, de sorte que l'existence même du secret soit dissimulée. Avec la cryptographie, on espère que la clé ne soit pas trouvée, avec la stéganographie on espère que le message caché ne soit pas découvert : l'objectif principal est la **furtivité**. La stéganographie diffère de la cryptographie seulement par la méthode.

Nous savons que la cryptographie permet de rendre un message illisible. Mais si une tierce personne intercepte le message et réussit à le décoder, il pourra interagir avec le destinataire en usurpant l'identité de l'émetteur. Ce dernier ne s'en rendra pas compte. C'est pour cela qu'une autre raison d'être de la stéganographie est **d'assurer l'authenticité et l'intégrité** d'un message.

Dans ce cas, le but n'est pas de faire passer un message caché dans un autre, mais de “marquer” un message par un autre. Le meilleur exemple est le filigrane : une image est incrustée sur une feuille de papier, et n'est pas remarquée sans un petit examen de la feuille. La technique du filigrane relève plus du tatouage, puisque l'objectif principal est de marquer l'authenticité du document.

Les applications en deviennent alors toutes autres, notamment en informatique, où copier un document ne prend que quelques secondes : tatouage (certifier l'émetteur du document), fingerprinting (traçabilité des copies), preuve de son intégrité par rapport à l'original, etc...

La stéganographie a aujourd'hui pris un autre sens. Une définition plus appropriée pourrait être : *assurer la dissimulation d'une information dans un flux de données numériques, tel qu'un fichier numérique image ou son.*