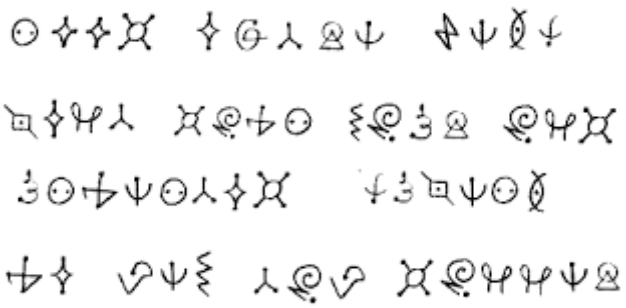
La guerre des codes

Projet Maths en Jeans

Jacky Cresson

La cryptographie est une discipline qui consiste à mettre au point des procédés de codage d'une information, que cette information soit un nombre, un message écrit dans une langue donnée, etc. Une première idée consiste à remplacer les lettres par des symboles : des chiffres, des dessins, etc. Un exemple de ce type de codage est donné ici



Qui est extrait du dessin animé « Futurama » avec les Simpsons.

Dans ce projet nous allons nous concentrer essentiellement sur des codages d'un texte par un autre texte, donc à remplacer les lettres d'un message par d'autres lettres.

Le premier code que nous allons étudier est le code de César qui consiste à décaler l'alphabet d'un nombre de lettre fixé. On représente souvent ce type de code par l'imbrication de deux roues qui peuvent tourner l'une par rapport à l'autre.

La roue du haut est choisie comme référence de l'alphabet. Pour transcrire un message il faut donc lire sur le cercle intérieur la lettre correspondante. Ici le A sera transcrit par un T, le B par un U, etc. Du

coup, par exemple le mot TURING sera codé comme MNKBGZ. On voit bien que c'est efficace car on ne reconnait plus du tout le mot initial.

Plusieurs questions importantes vont se poser par rapport à la donnée de ce code car un code a toujours trois aspects qui peuvent se répartir schématiquement entre ce que nous appellerons le côté AMI et le côté ENNEMI. Nous nous mettrons du côté AMI, c'est-à-dire que nous voulons envoyer en toute sécurité un message à des amis, les ennemis étant ceux qui veulent décoder le message que nous voulons transmettre.

Du côté AMI nous avons les questions suivantes :

1- Le procédé de codage est-il facile à mettre en place ?

2- De quelles données mon ami a-t-il besoin pour décoder l'information ?

3- Le procédé de décodage est-il long ou non ?

Du côté ENNEMI, le questionnement est tout-autre :

1- Le code possède-t-il des faiblesses qui permettent de le décoder ?

2- Si oui, en combien de temps peut se faire se décodage ?

Ces questions vont nous permettre d'améliorer le code de César en se mettant soit du côté AMI, soit du côté ENNEMI .

Une première étape est de répondre aux questions précédentes pour le code de César. Pour les questions 1,2 et 3 du côté AMI vous trouverez tout seul. Par contre, on voit que du côté ENNEMI la réponse aux questions 1 et 2 est loin d'être évidente car elle suppose a priori d'avoir de l'informations sur le procédé de codage utilisé. Nous allons donc simplifier le problème en supposant que les ENNEMIS savent qu'un code de César a été utilisé. Dans ce cas, quelles sont les faiblesses de ce codage ?

1- Si on trouve comment se décode une lettre alors on a le décodage de toutes les lettres car le décodage d'une lettre donne accès au décalage du code de César utilisé. Si par exemple on trouve une lettre T toute seule dans un texte il est fort probable que ce soit un A, un Y ou un L.

2- Une lettre est codé par une lettre est une seule. Donc par exemple si on observe des répétitions de deux lettres dans un mot codé comme EPPOR il est fort probable que le P code des S ou des L.

3- Les particularité d'écriture d'une langue doivent donc se retrouver dans le code de César. En Français nous avons peut de mots commençant par Z ou Y mais on a souvent des E dans les mots et ensuite des A. La connaissance de la langue va donc permettre d'analyser le texte codé et de retrouver le codage.

Comme on le voit, tout cela n'est pas aussi évident que cela. Les réponses à ces questions vont nous permettre de réfléchir à la mise en place de code plus performants en essayant soit de simplifier le codage, le décodage ou en supprimant certaines faiblesses du codage existant.

Notre but est d'arrivé à la compréhension de la machine ENIGMA mise au point par les Allemands durant la seconde guerre mondiale pour protéger leurs messages concernant le déplacement des troupes et les attaques. Ce code sera « craqué » par Alan Turing et ses collaborateurs pendant la guerre au prix d'un effort intellectuel et technique important.

La vie d'Alan Turing est exceptionnelle et tragique. Pour comprendre ENIGMA, nous construirons un modèle simplifié en papier afin de pouvoir décortiquer son fonctionnement et comprendre à la lumière des travaux que nous aurons réalisé sur d'autres codes pourquoi son décodage est un exploit.