

L'atelier de cryptographie a fonctionné avec des élèves de seconde.

L'objectif général consistait à coder (crypter de M1 à M2) un message puis à décoder le message incompréhensible (décrypter de M2 à M1) pour retrouver son contenu initial "en clair". Les méthodes disponibles sont variées et leurs qualités et défauts respectifs sont instructifs.

Nous avons découvert, en parallèle, les manipulations des nombres entiers, les caractéristiques de certains d'entre eux qu'on explore en arithmétique, et les possibilités d'un logiciel de "Calcul formel", précisément "Maple", pour qu'il effectue certaines tâches répétitives ou volumineuses à notre place.

1) Nous avons d'abord utilisé le codage de César (décaler les lettres de l'alphabet de 3 : A devient D, B devient E, etc.) et programmé sur Maple des procédures de chiffrement et déchiffrement des chaînes de caractères (c'est à dire des phrases).

2) Nous avons ensuite essayé de (et réussi à) déchiffrer un texte codé par une méthode inconnue, en utilisant des tables de fréquence d'apparition des lettres dans un texte en Français, que nous avons constituées statiquement nous même à partir de textes classiques et d'un traitement de texte. (Par exemple la lettre E est la plus fréquente en Français).

Il est alors clairement apparu que l'on peut déchiffrer un message assez long (pour que les fréquences soient significatives) et qui utilise systématiquement les mêmes substitutions de lettres (quand un A est toujours transformé en un G par exemple). Ce qui nous a montré que certains procédés sont trop limités, par exemple le codage de Vigenere, et que d'autres méthodes sont nécessaires.

3) D'où l'idée de transformer un message en nombre entier (de M1 à N1) avec une procédure (A devient 01, B devient 02, etc. et BABA devient 02010201) qui est clairement réversible (on peut retrouver M1 à partir de N1), et de manipuler cet entier N1 par un procédé arithmétique pour qu'il devienne méconnaissable (N1 devient N2)

Nous avons d'abord constaté que nous calculions déjà "modulo" 24 pour les heures, "modulo" 7 pour les jours de la semaine, ou "modulo" 360 pour les angles en degré.

Nous avons alors calculé des tables d'addition et de multiplication "modulo 11" puis "modulo 12", et discuté de bijection à propos des résultats (pour qu'un N2 corresponde à un seul N1 et que le codage n'amène pas d'ambiguïté).

Nous avons aussi pratiqué Maple sur divers exemples d'introduction pour nous familiariser avec le logiciel, sa syntaxe et ses pièges.

4) Nous avons ensuite calculé des exponentielles modulaires (calcul de  $a^k \text{ modulo } n$ ), qui pour  $a$  et  $n$  bien choisis, fournit une méthode pour transformer l'entier  $k$  en un autre entier imprévisible pour les humains actuels. Nous avons ainsi essayé de calculer le résultat de façon ultra-rapide avec des nombres premiers très grands, tout en mesurant qu'un calcul explicite de toutes les images, pour essayer de décoder, est interminable.

5) Chemin faisant, nous avons découvert que les méthodes actuelles sont constamment utilisées dans les banques et les entreprises, qu'elles évolueront au fur et à mesure des progrès en Mathématiques.

En résumé, nous avons découvert que l'Arithmétique est un sujet très actuel pour l'économie de notre société, qu'elle est un domaine ouvert où beaucoup de recherches sont nécessaires, et qu'un ordinateur est un outil utile quand on prend le temps de le maîtriser.