Codage de César

Dès 12 ans

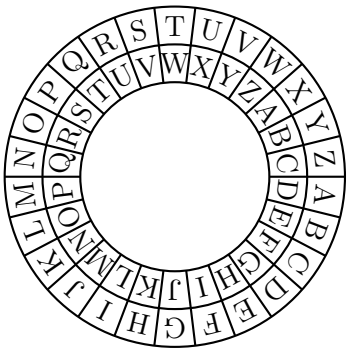
Une introduction à la cryptographie avec un code simple. Coder et décoder des messages secrets... mais aussi casser le code !

Depuis des milliers d'années, que ce soit pour se protéger d'un ennemi, pour éviter des indiscrétions, ou même simplement par jeu, des techniques pour communiquer par messages secrets existent : c'est l'art de la cryptographie. De nos jours, la cryptographie est même devenue omniprésente (transactions sur Internet...). Dans cet atelier, on prend l'exemple d'un codage très simple, utilisé par Jules César, pour présenter les deux aspects de la science des messages secrets :

- du point de vue de ceux qui se les transmettent (ici, César et ses alliés), il s'agit d'avoir une « clé » pour coder et décoder les messages ;
- du point de vue de leurs adversaires, qui essayent d'intercepter les messages mais ne connaissent pas la « clé », il s'agit de trouver un moyen pour la deviner et déchiffrer le message... autrement dit casser le code !

Principe du codage de César

Le codage de César repose sur un simple décalage de l'alphabet. On remplace chaque lettre du message en clair par (par exemple) la lettre qui est située 3 rangs plus loin dans l'alphabet : avec ce décalage, *a* devient *d*, *b* devient *e*, *c* devient *f*, et ainsi de suite en bouclant à la fin de l'alphabet : *x* devient *a*, *y* devient *b*, *z* devient *c*. Le décalage particulier (3 dans l'exemple) est choisi par les correspondants. C'est ce décalage qu'on appelle la *clé*. Pour décoder, il suffit de décaler dans l'autre sens.
Pour visualiser facilement les décalages de l'alphabet, on dispose de deux disques concentriques, chacun ayant les lettres de l'alphabet sur le bord, comme sur la figure. On peut faire tourner les disques pour régler le décalage.



a) Coder et décoder des messages

Pour cette partie de l'atelier, il faut d'abord se mettre d'accord sur un décalage. Les participants peuvent alors coder des messages (par exemple un ou plusieurs mots) en utilisant cette clé, se les échanger puis les décoder. On peut recommencer avec un autre décalage.

b) Casser le code

Pour cette partie, on dispose de plusieurs petits papiers avec un message long d'une dizaine de mots, codé avec le codage de César, mais les participants, qui incarnent maintenant un adversaire, ne connaissent pas la clé !

- Est-il envisageable d'essayer toutes les clés ? (combien y a-t-il de décalages possibles ?) Pour un adversaire qui n'est pas pressé, oui, mais il y a mieux :

- Peut-on deviner certaines lettres ? Dans un message en clair, certaines lettres ont des propriétés particulières (par exemples celles qui peuvent être doublées). Celles qui ont cette propriété dans le message codé peuvent donc être identifiées. Quelle est la lettre la plus facilement distinguable dans un texte en français ? (le *e*, parce qu'il apparaît le plus fréquemment)
- Utiliser la fréquence des lettres permet de casser facilement le code de César, mais on s'est appuyé sur plusieurs hypothèses : que le message est en français, et que la lettre la plus fréquente est *e*. On peut parler de *La disparition* de Georges Perec qui ne vérifie pas la deuxième hypothèse !

Pour aller plus loin

- Le codage de Vigenère (XVI^{e} siècle) : on utilise plusieurs décalages différents, passant successivement de l'un à l'autre pour coder chaque lettre. L'analyse des fréquences des lettres ne fonctionne plus, car une même lettre peut être codée de plusieurs façons !

Références

- Simon Singh, *Histoire des codes secrets. De l'Égypte des pharaons à l'ordinateur quantique.* Un classique très accessible sur l'évolution des techniques cryptographiques, disponible en livre de poche.