Photo © Mathieu Rod

Message secret !

Message secret !

Crypter et décrypter un message secret est un jeu d'enfant quand on sait fabriquer une roue de César !

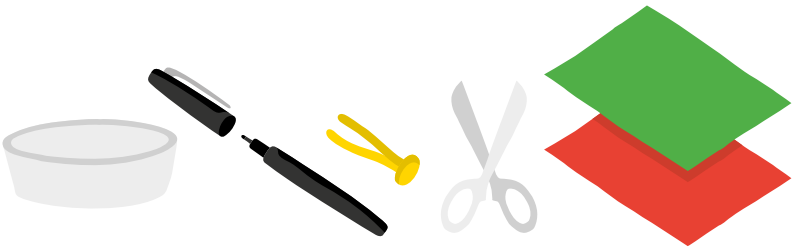
1

À l'aide d'un compas, ou en faisant le contour d'un bol, trace sur du papier fin deux cercles de tailles différentes. Découpe-les. Plie ensuite ces disques 5 fois par la moitié pour obtenir 32 secteurs.

2

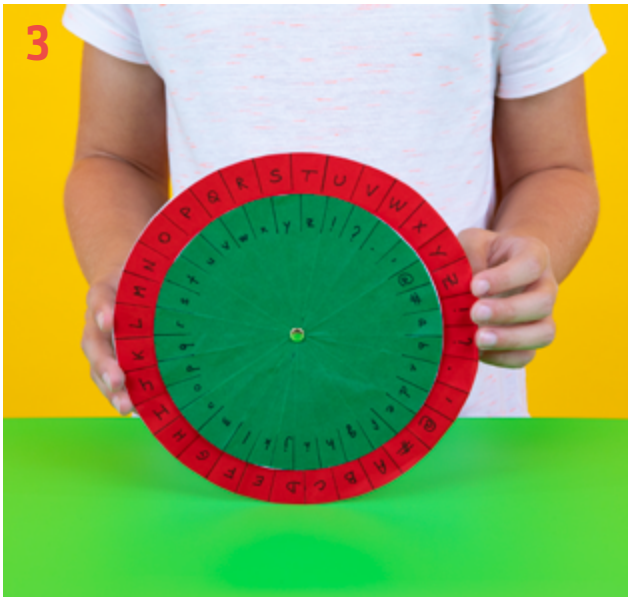
À l'aide d'un stylo feutre noir, inscris une lettre dans chaque secteur : de *A* à *Z* majuscules sur le grand disque et de *a* à *z* minuscules sur le petit. Puis complète la liste avec les signes *! ?. , @ #*.

Document extrait de *Petite collection d'expériences qui font PSCHITT !* – www.pschitt.ch
Ce livre est publié sous une licence *Creative Commons Attribution CC BY-NC-ND 4.0*



Matériel : 1 compas ou 1 bol, 1 crayon/stylo, des ciseaux, 1 attache parisienne et du papier fin

3



Perce ensuite un petit trou au milieu des deux disques (pour que ce soit plus solide, tu peux les coller sur du carton), superpose-les, puis assemble-les à l'aide d'une attache parisienne.

4

Choisis ton décalage, tu peux placer le *A* majuscule en face du *c* minuscule par exemple. Décrypte alors le message *ucnwv*. Trouvé ? En copiant la lettre majuscule en face de chacune de ces lettres, on obtient *SALUT* !

Document extrait de *Petite collection d'expériences qui font PSCHITT !* – www.pschitt.ch
Ce livre est publié sous une licence *Creative Commons Attribution CC BY-NC-ND 4.0*

Que se passe-t-il ?

La cryptographie est l'art de transformer un message afin de le rendre indéchiffrable pour qui ne possède pas la clé. Au fil de l'histoire, les êtres humains ont rivalisé d'ingéniosité pour mettre au point des outils de cryptage toujours plus sophistiqués. Et aujourd'hui, avec l'informatique, la cryptographie s'est encore complexifiée. La roue de César, elle, est l'un des procédés de cryptage les plus anciens que l'on connaisse. Elle permet de crypter un message via un simple décalage de l'alphabet. En décidant par exemple, comme dans cette expérience, que A = c, c'est ce qu'on appelle la clé.

Pour aller un peu plus loin...

Notre moyen de cryptage à l'aide de la roue de César est-il sûr ? Est-ce qu'un intrus, interceptant le message mais ne connaissant pas le décalage, pourrait quand même parvenir à retrouver le message en clair, c'est-à-dire non crypté ?

Avec la roue de César, une fois le décalage choisi et partagé avec le destinataire du message, une lettre est toujours cryptée par une même lettre. Ainsi, dans notre exemple, *A* sera toujours cryptée par *c*, *B* par *d*, etc.

Différentes techniques de cryptanalyse, c'est-à-dire de « piratage » pour tenter de comprendre un message crypté sans en connaître la clé, existent.

Pour la roue de César, on peut procéder à une analyse de fréquence. Une lettre étant toujours cryptée par une même lettre, il s'agit de compter les occurrences de chacune des lettres dans le message crypté. On connaît ensuite les statistiques de la langue française, le E revient le plus souvent, suivi du *A*, puis du *I*, etc. jusqu'au *K* et au *W*. Les cryptanalystes peuvent donc faire des hypothèses sur le décalage en alignant les occurrences de chacune des lettres dans le message crypté et dans la langue française.

Pour que l'analyse de fréquence fonctionne, il faut que le message crypté soit suffisamment long, pour qu'il soit possible de faire des statistiques sur la répartition des lettres.

Pour rendre l'analyse de fréquence impossible, il suffirait de décaler la roue d'un cran, à chaque fois qu'on crypte une nouvelle lettre. Ainsi, une lettre sera cryptée à chaque fois par une lettre différente.

La machine Enigma, utilisée par les nazis pendant la seconde guerre mondiale, est basée sur ce principe (décalage à chaque lettre, et cryptage à l'aide de plusieurs roues). Les alliés, dont le célèbre Alan Turing, parvinrent tout de même à cryptanalyser les messages générés par la machine Enigma, ce qui leur permit d'obtenir de précieuses informations.

Document extrait de *Petite collection d'expériences qui font PSCHITT !* – www.pschitt.ch
Ce livre est publié sous une licence *Creative Commons Attribution CC BY-NC-ND 4.0*