

# //CRYPTOLOGIE101

De tout temps, des personnes ont communiqué en essayant de coder leurs informations pour éviter que quelqu'un d'autre que le destinataire puisse comprendre quel était le sujet du message.

De nos jours, la cryptologie est omniprésente puisqu'on la retrouve dans l'univers de l'informatique. En effet, c'est grâce à celle-ci que nos mots de passes et données confidentielles sont protégés des personnes malintentionnées. N'importe quel message peut-être dissimulé avec l'aide d'un code secret mais il faut cependant savoir quel est celui utilisé, il en existe des milliers différents.

Dans le cadre de cette initiation en cryptologie réalisée par notre organisme CHERUB, nous allons vous fournir les moyens pour décoder trois des codes secrets les plus utilisés au monde. Vous pourrez ainsi déjouer des attaques terroristes grâce à vos talents. Nous verrons donc ces codes du plus simple au plus difficile: Les Acrostiches, Le code César et Le Chiffre de Vigenère.

## **1- LES ACROSTICHES**

« Survivre est essentiel à CHERUB tout comme Ecouter et comprendre le monde qui nous entoure. Saviez vous que Courage et le mot préféré de nos instructeurs. Même si leur Recette secrète est la souffrance et l'envie ! Cependant, ils ne vous Electrocuterons jamais mais nous vous conseillons de rester vigilant au niveau des Tatamis car ils ne vous laisseront aucune. »

Dans ce texte, ce trouve un message codé facile à trouver, il est constitué de six lettres. Pour découvrir ce dernier, il suffit de relever la première lettre de chaque ligne. Ainsi, le mot "SECRET" apparaît. Ce code est surtout utilisé pour brouiller les pistes car ceux qui l'emploient savent qu'il est facile de le décrypter et ne veulent pas que des personnes les observant puissent récupérer des informations sensibles. Il ne faut pas non plus négliger ce mot car il peut également être une référence précieuse.

## **2- LE CODE CÉSAR**

Le code de César est plus compliqué que celui que nous venons d'expliquer. En effet, le message n'apparaît pas clairement aux yeux du lecteur. Pour décrypter ce code, il faut user d'observation et de recherche.

Prenons par exemple cette phrase : « Les agents de CHERUB sont exceptionnels ». Une fois codée, cette phrase peut ressembler à : « MFT BHFOUT EF DIFSVC TPOU FYDFQUJPOOFMT »

On commence par remarquer que les groupement de lettres sont inchangés:  
Les = MFT, «agents = BHFOUT, ...

Il faut maintenant comprendre quel stratagème est utilisé. Sachant que dans notre langage, la lettre de l'alphabet la plus utilisée est le E, on peut aisément décoder le message. Pour cela, il suffit de trouver quelle est la lettre la plus utilisée dans le message codé: ici, on retrouve le plus souvent la lettre F donc le F codé correspond au E décodé. Dans l'alphabet, le F se trouve juste après le E, on a donc effectué un décalage de 1 et il en est de même pour les autres lettres voici la correspondance des lettres:

clair : a b c d e f g h i j k l m n o p q r s t u v w x y z  
code : b c d e f g h i j k l m n o p q r s t u v w x y z a

Si le décalage était de 3, le code serait : « OHV DJHQWV GH FKHUXE VRQW HAFHSWLRQQHOV ». A ce moment là, le H codé correspond au E décodé et la correspondance des lettre serait:

clair : a b c d e f g h i j k l m n o p q r s t u v w x y z  
code : d e f g h i j k l m n o p q r s t u v w x y z a b c

### **3- LE CHIFFRE DE VIGENÈRE**

Ce code est complexe mais une fois compris, le déchiffrement est effectué aisément. Il faut, dans un premier temps être en possession de l'alphabet de Vigenère ou alors le connaître par coeur. ([Voir tableau Vigenère](#))

Le message codé : « Les agents secrets » avec la clé « CHERUB » est : « NLW RAFPAW JYDTLXJ »

Pour décoder le message, on regarde la première lettre de la clé : C et la première lettre du message codé : N.

Dans le tableau, les lettres de la colonne clé sont celles de CHERUB. Dans la ligne du C (première lettre de la clé), il faut trouver le N et regarder la correspondance en "clair" qui est "L". Vous avez ainsi la première lettre du message. Ensuite, dans la ligne du H (deuxième lettre de la clé), il faut trouver L. Sa correspondance est E.

Vous avez donc décodé ce qui est en majuscule : « LEs agents secrets ». Une fois arrivé au bout de la clé, il faut recommencer. Donc une fois arrivé au B de CHERUB, vous continuez en reprenant du C.

Cependant, sans être en possession de la clé, le déchiffrement est compliqué. Les terroristes utilisant ce code peuvent transmettre cette clé dans une conversation mais généralement de façon codé !

**//RESTRICTED\_DATA\_01010100//**