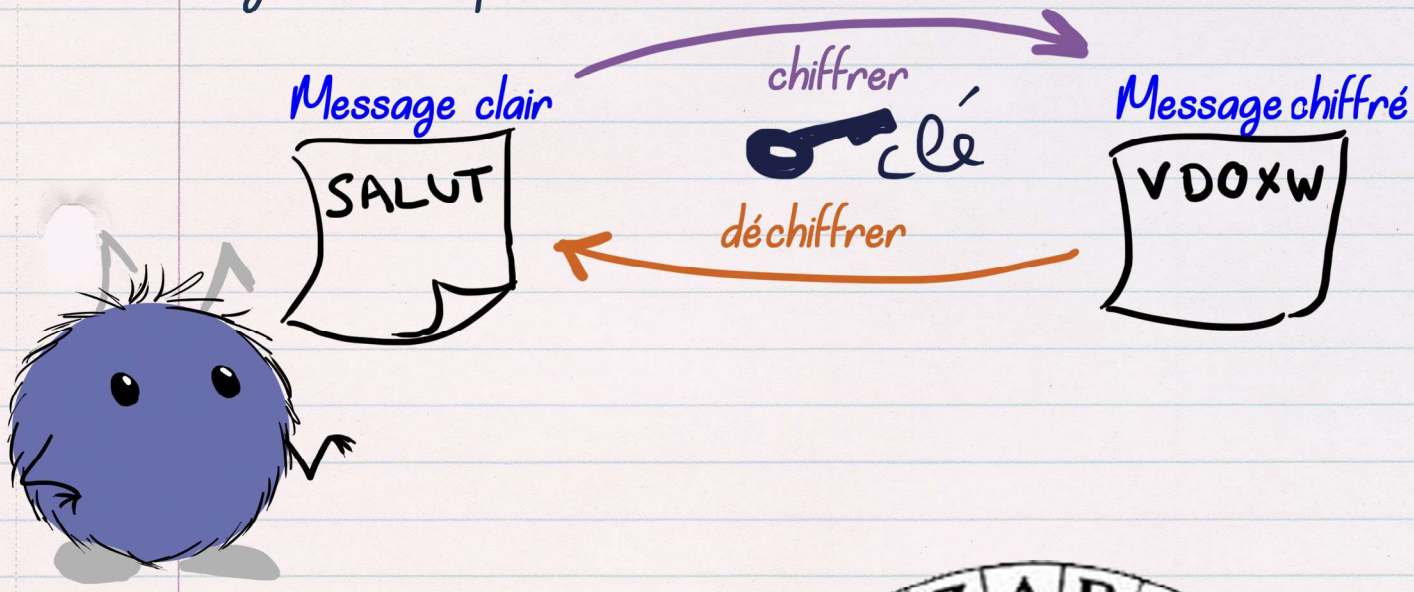
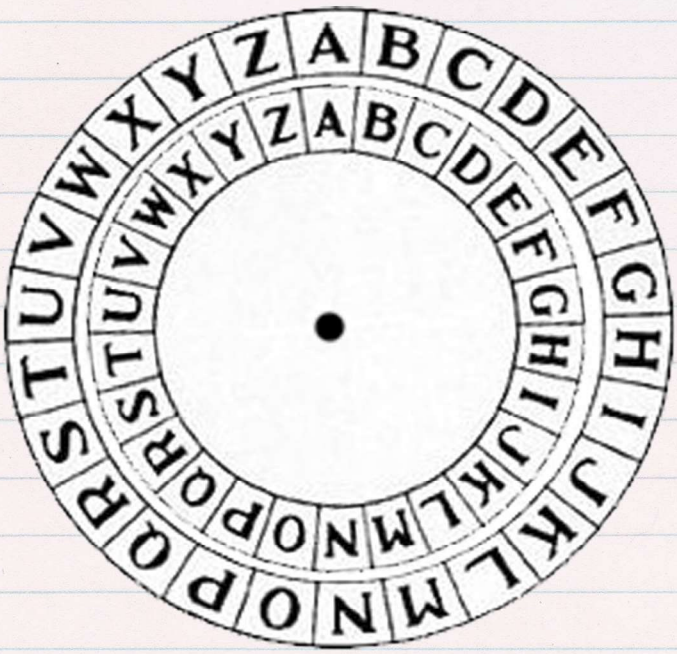
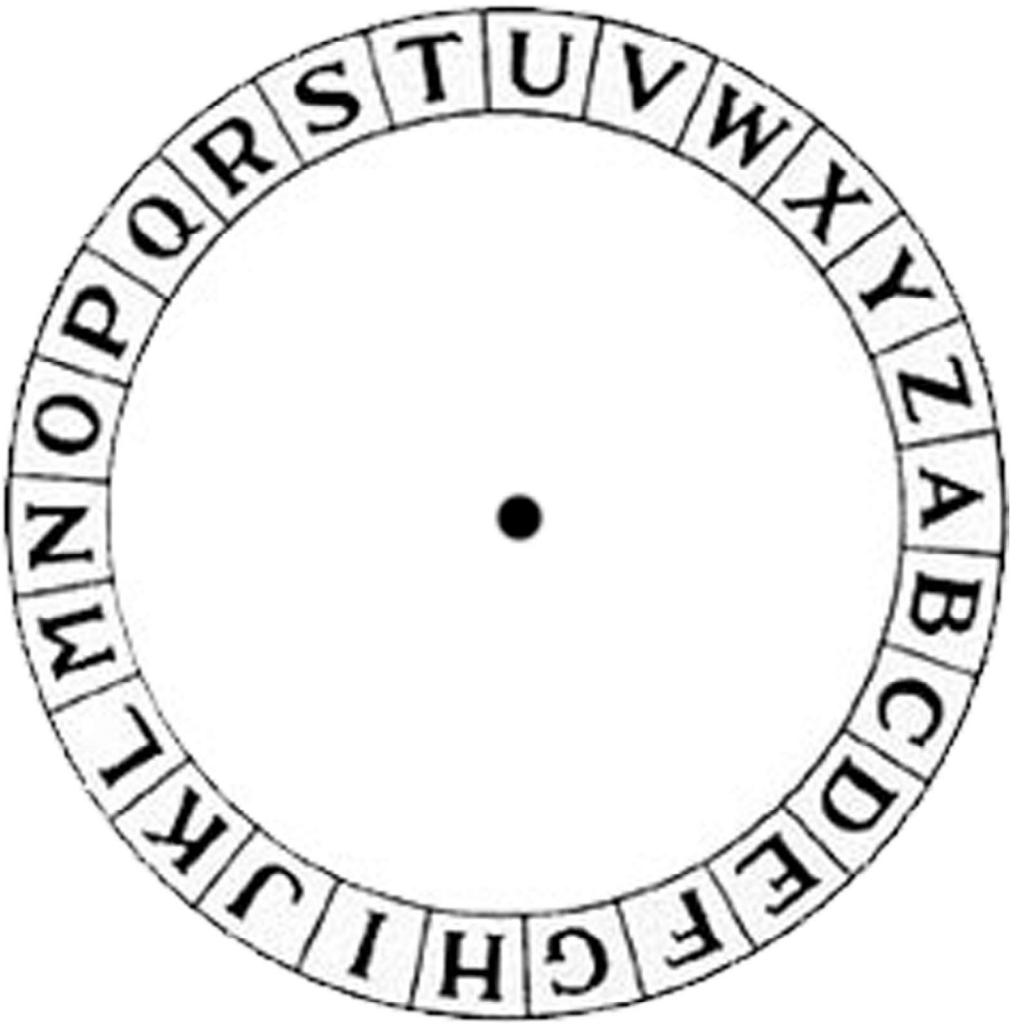
CODE CÉSAR

La cryptographie est l'art de **protéger** un message clair avec un code secret, aussi appelé **clé**. Pour pouvoir lire le message chiffré, il faut connaître la clé. Ainsi, on peut échanger des messages que seuls ceux ayant la clé peuvent lire.



Découvrons l'une des premières méthodes de chiffrement : le **code César** ! Avec l'aide d'un adulte, imprime la page **22** et découpe les deux disques. Pose le **petit disque** sur le **grand**, tu peux les fixer à l'aide d'une attache parisienne par exemple. Voilà ce que tu obtiens :




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

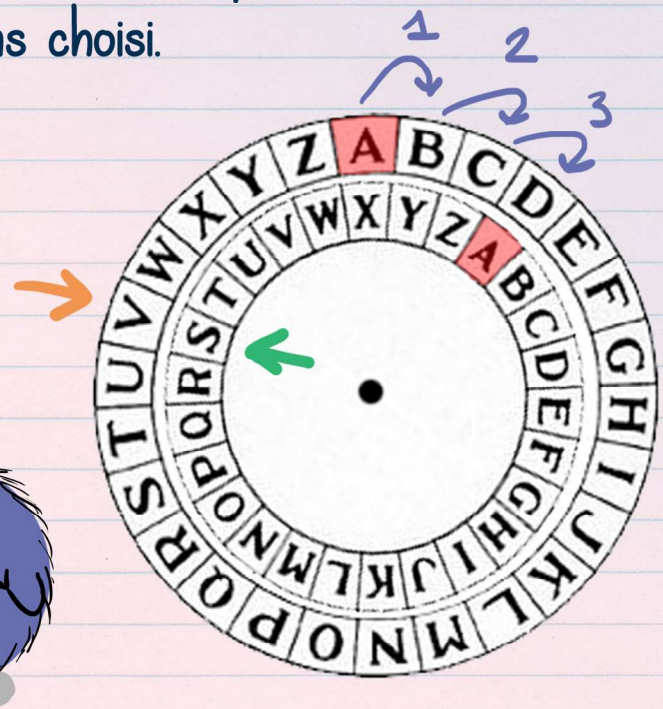

A B C D E F G H I J K L M N O P Q R S T U V W X Y Z

CODE CÉSAR

Nous allons utiliser ces disques pour chiffrer un message. D'abord, choisis le **message** que tu veux chiffrer.

SALUT JE SUIS BUGGY

Ensuite, choisis un **nombre** entre 1 et 25 : c'est notre clé. Fais tourner le petit disque vers la droite, d'autant de lettres que le chiffre que tu as choisi.



Jules César utilisait un décalage de 3, aujourd'hui cette méthode porte son nom !

Maintenant, trouve la **première lettre** de ton message sur le petit disque, et lis la lettre se trouvant à la même place sur le grand disque : ce sera la première lettre du message chiffré. En répétant cela sur tout ton message, tu obtiens ton message chiffré ! Buggy obtient :

VDOXW MH VXLV EXJJB

CODE CÉSAR

Correction page 25

Buggy t'a envoyé un message chiffré :

JZIDW IOMVB AMKZMB

Pour **déchiffrer** le message, il suffit de répeter les mêmes étapes que pour le chiffrement en lisant la lettre chiffrée sur le grand disque, et la lettre en clair sur le petit disque. Peux-tu retrouver le mesage original de Buggy ?

Psst, j'ai choisi comme clé : 8

Lorsqu'on ne connaît pas la clé, il faut essayer les **26 possibilités** (tour complet du disque) pour **décrypter** le message. Cela peut être fastidieux sur papier, mais très rapide pour un ordinateur. Aujourd'hui, des méthodes plus **complexes** sont utilisées, beaucoup plus difficiles à décrypter. On s'en sert par exemple pour envoyer des **données sécurisées** sur Internet.

CODE CÉSAR

Correction

Buggy t'a envoyé ce message chiffré :

JZIDW IOMVB AMKZMB

Buggy t'a également donné **sa clé** pour déchiffrer le message : **8.**
Il faut donc que tu décales le petit disque de 8 lettres pour déchiffrer le message. Cela veut dire qu'en face de la lettre A (sur le petit disque) tu dois avoir la lettre I (sur le grand disque)

Tu as fait le plus difficile. Maintenant, **pour chaque lettre** du message de Buggy, voilà ce qu'il faut faire :

1 - Trouve la lettre sur le grand disque
2 - Regarde la lettre qui correspondant sur le petit disque
3 - C'est la lettre du "vrai" message (le clair), écris la sur un papier
4 - Passe à la lettre suivante

Tu obtiens alors :

BRAVO AGENT SECRET