# Seconde – SNT

## Code de CESAR Généralités…

Le fichier est disponible en ligne sur le site dimension-k.com sur la page secondes 2023, dans la partie SNT. Vous y trouverez aussi d'autres documents importants pour cette activité.

## Partie°1 : activité déconnectée

Bien avant Sherlock Holmes, en fait depuis l'antiquité, les hommes ont toujours éprouvé le besoin de modifier un texte afin de le soustraire à la vue des personnes non autorisées, cette science s'appelle la cryptographie.

L'un des premiers codages utilisés est le code de César qui doit son nom à l'empereur romain Jules César, il consiste à décaler chaque lettre de l'alphabet de trois rangs :

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

Ainsi le mot « ANTIQUITE », devient après codage : « DQWLTXLWH », de même le mot codé « UDQJHU » s'écrit « RANGER » après décodage.

Par extension, tout codage obtenu en décalant les lettres de l'alphabet d'un même rang est appelé code de César, le rang constant est appelé la clé du codage.

Par exemple un codage de César de clé 8, signifie qu'on décale chaque lettre de 8 rangs, A est remplacé par I, B par J ...

Ce qui donne la correspondance suivante :

| 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 |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| 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 |

**Exercice 1 :** A l'aide du tableau précédent :

1. Coder le texte : « LES MATHEMATIQUES SONT LA REINE DES SCIENCES »

2. Décoder le texte « YCQ DI BZMA TWQV UMVIOM AI UWVBCZM »

Pour faciliter le cryptage et le décryptage d'un texte, on peut utiliser les cercles concentriques de la page 2, on les fixe par le centre, celui de plus grand diamètre est fixe et l'autre mobile, en le faisant tourner, on obtient le décalage des lettres, donc la correspondance.

**Exercice 2 :** En utilisant un codage de César, clé 17

1. Coder le texte : « LES PETITS RUISSEAUX FONT DE GRANDES RIVIERES»

2.Décoder le texte « UV HLZ JFEK TVJ JVIGVEKJ HLZ JZWWCVEK JLI EFJ KVKVJ»

**Exercice 3 :** Un codage de César, transforme « SUBSTITUTION » en « KMTKLALMLAGF »

Quelle est la clé ?

**Exercice 4 :** En utilisant un codage de César, décoder le texte :

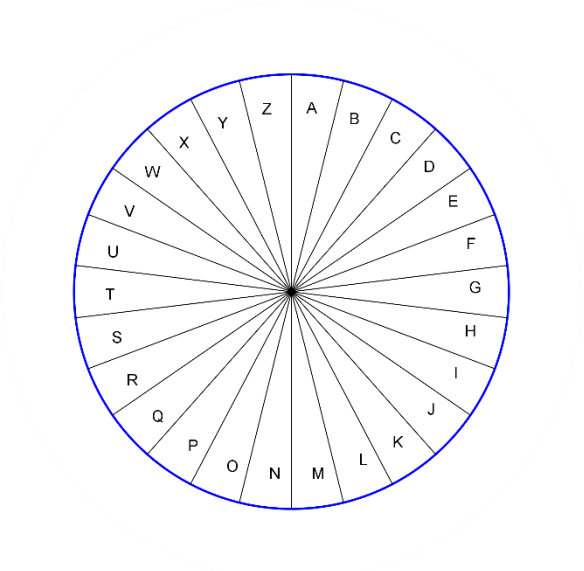
«KXDSMYXCDSDEDSYXXOVVOWOXD OCD VO WYD VO ZVEC VYXQ NO VK VKXQEO PBKXMKSCO»

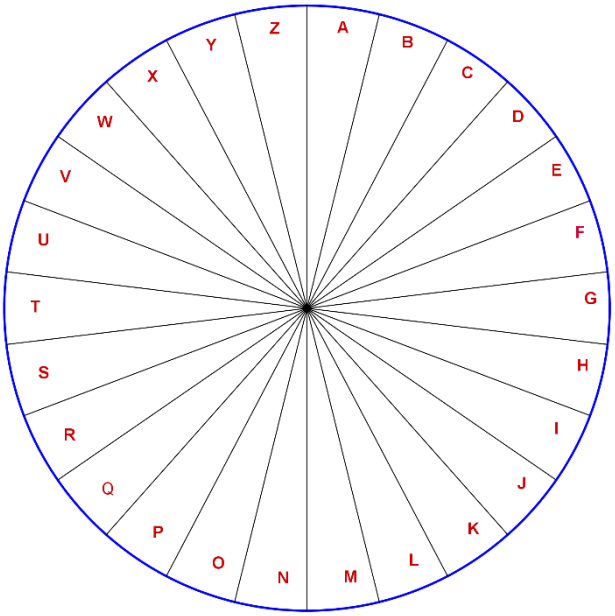
**Exercice 5 :** En utilisant un codage de César, décoder le texte :

«SB OTTOWFSG WZ BS TOIH DOG HFWQVSF»

**Exercice 6 :** En utilisant un codage de César, décoder le texte :

«PS F H WSBZPLBYZ MHJVUZ KL YLZVBKYL JL WYVISLTL»



## Partie 2 : préparation au crypteur décrypteur de César

Demander à python de faire un décalage de plusieurs lettres sur l'alphabet ne va pas marcher car il n'y a pas de fonction intégrée permettant de faire une telle action. Il nous faut l'inventer. Pour lui les lettres de l'alphabet n'ont pas de sens particulier, ce sont juste des caractères qu'il stocke et manipule sous la forme de nombres.

Notre but dans un premier temps sera de crypter un texte avec la méthode césar classique en utilisant python.

1. Sur python tester la fonction ord( ) sur des nombres compris entre 65 et 91. Consulter le document table ASCII sur le site, et dire à quoi sert la fonction ord.

2. Utiliser la fonction chr(.. ) sur les lettres ''A'', ''B'', deviner ce que l'on obtient en tapant **chr(''F'')** et **chr(''Z'')**

3. En vous référent au premier tableau du polycopié « Code de César – généralité » dire ce que l'on peut observer en comparant les résultats obtenus en appliquant la fonction chr( .. ) à une lettre de départ et sa lettre transformée. Dans le cadre suivant, faites quelques exemples, généraliser et expliquer.

4. Si la variable lettre contient une lettre à coder, compléter l'expression pour qu'elle permette de la transformer en lettre cryptée : **chr(ord(lettre) + ...)** . Vérifier votre choix avec les lettres ''G'' , ''M'', et ''R''. Ajuster votre choix si nécessaire.
5. D'après le tableau de référence sur l'autre polycopié que devrait nous afficher cette méthode quand on veut transformer ''X'', ''Y'' et ''Z'' ? Est-ce que c'est ce que l'on obtient ? et pourquoi ?

6. Nous allons devoir corriger notre approche pour gérer ces cas exceptionnels. Compléter le cadre :

ord(''X'')+3 = …….. on voulait ''A'' qui a pour code ASCII : …….
ord(''Y'')+3 = …….. on voulait ''B'' qui a pour code ASCII : …….
ord(''Z'')+3 = …….. on voulait ''C'' qui a pour code ASCII : …….
Quel est l'écart entre les codes dans chaque paire ; ……

7. Compléter le correctif :

```
    if ord(lettre)+3> … :
        nouvelleLettre=chr(ord(lettre)+3 - …… )
```

```
    else :
         nouvelleLettre=chr(ord(lettre)+ … )
```

8. Maintenant on va s'intéresser au décryptage. Quand est ce que la formule **chr(ord(lettre) -3)** va poser problème ? (pour quelles lettres ?)

9. Adapter le correctif à ce cas de figure

```
    if                          :
        nouvelleLettre=chr(ord(lettre)- 3+26 )
    else :
         nouvelleLettre=
```

Maintenant on veut généraliser ça. La clé pourra être différente de 3. Si elle est positive la fonction servira pour crypter et si elle est négative alors la fonction servira pour décrypter.

Par exemple un texte crypté avec une clé 5, sera décrypté avec une clé -5.

10. Copier le texte suivant (sauf les numéros de lignes dans la zone programme de votre éditeur) puis en vous inspirant de ce qui précéde compléter les lignes 1 , 9 et 12 .

```
1  def cryptCesar(texte,cle):
2      """la clé du codage sera comprise entre -26 et 26"""
3      textdep=texte.upper()
4      textfin=""
5      for lettre in textdep :
6          if 65<=ord(lettre)<=90 : #on ne cryptera que les lettres
7              if ord(lettre) + cle >  :
8                  textfin+=chr(ord(lettre) + cle-26)
9              elif                        :
10                 textfin+=chr(ord(lettre) + cle+26)
11             else :
12
13         else :                  # la ponctuation est reproduite
14             textfin+=lettre     # sans changement
15     return textfin
```

11. Après quelques bricolages dans votre console ou recherche en ligne expliquer la ligne 3, et la raison de sa présence dans notre code.

## Partie 3 : Comme Sherlock j'analyse les fréquences (activité déconnectée)

Si on ne connait pas la clé, le code de César est assez facile à décrypter, une méthode certes un peu longue, appelée brute-force consiste à essayer toutes les 25 clés possibles. Une autre est l'analyse des fréquences. Suivant la langue, toutes les lettres n'ont pas la même fréquence d'apparition dans un texte. Le tableau suivant donne la fréquence théorique d'apparition des lettres d'un texte de la langue française.

| Fréquences théoriques des lettres dans un texte (en %) | | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|
| **E** | **S** | **A** | **I** | **N** | **T** | **R** | **U** | **L** | **O** | **D** | **C** | **P** |
| 17,52 | 8,17 | 8,01 | 7,35 | 7,22 | 7,07 | 6,69 | 6 | 5,77 | 5,43 | 3,91 | 3,23 | 2,94 |
| | | | | | | | | | | | | |
| **M** | **V** | **Q** | **G** | **F** | **H** | **B** | **X** | **J** | **Y** | **Z** | **K** | **W** |
| 2,90 | 1,41 | 1,14 | 1,06 | 1,06 | 0,88 | 0,88 | 0,47 | 0,44 | 0,30 | 0,12 | 0,05 | 0,02 |

**Exercice 1** Déchiffrer le texte suivant :
YRF RYRIRF QR PRGGR PYNFFR BAG QR OBAF ERFHYGNGF RA ZNGURZNGVDHRF

***Marche à suivre :*** Compléter le tableau suivant, puis comparer la fréquence d'apparition des lettres dans ce texte (arrondir au centième) avec la fréquence théorique d'apparition des lettres d'un texte de la langue française. En déduire le décryptage du texte.

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

Message décrypté :

**Exercice 2** Dans la corbeille, sur du papier froissé, les enquêteurs ont trouvé le message suivant : ODFSG AOWBHSG FSQVSFQVSG JWUSBSFS RCBBS IBS WBRWQOHWCB DFSBRFS GSDH SH HFCWG

Déchiffrer le et faire des recherches à l'aide d'internet, sur le nom y apparaissant.

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

Message décrypté :