CyberSécurité
Introduction Crypto (2)
TD2 - 2023

TD individuel
Attention de bien lire le TD : 1-Objectif et 2-Réalisation pour le prochain TD
« L'homme et sa sécurité doivent constituer la première préoccupation de toute aventure technologique. »
Albert Einstein

• Objectif du TD

- **L'ensemble des exercices de ce TD devra être réaliser avec Jupiter-lab**
  - Installation de Jupyter-Lab : https://jupyter.org/install
  - Documentation de Jupiter-lab : https://docs.jupyter.org/en/latest/
  - **Spyder : https://docs.spyder-ide.org/current/installation.html**

- **La remise du TD se fera obligatoirement déposer sur DVO**
  - Votre .zip contiendra obligatoirement :
    - L'ensemble des programmes Python dans jupyter-lab au format « ipynb »
      - Votre ipynb devra contenir obligatoirement:
        - Votre nom et prénom
        - N° du TD
        - N°de l'exercice
        - Question et réponse à l'exercice
        - Code Python, une fonction par cellule avec commentaires

1 Home Works – Réalisation Obligatoire avant le prochain TD

1.1 Cette présentation individuelle comprendra un PowerPoinT (.ppt) et doit être remis sur DVO pour le prochain TD minimum de 10 Slides avec **au minimum 1 slide par Item.**:

- Biographie :
  - Joan Ball
  - Elizabeth Feinler
- Le Bios
  - Comment est programmé le Bios ?
  - Trouver des outils qui permettre de récupérer un Bios d'une carte mère
    - Les tester (attention uniquement en lecture)
    - Comment valider leur fonctionnement ?
    - Démonstration si possible (Python ?, C ? ,….)
  - Peut-on récupérer le bios d'un HDD ou SDD ?
    - Comment et avec quels outils ? Y-a -t'il un historique ?

1.2 ...

2 Exercices – Analyse de fréquences

2.1 **Exo2_1 :** Analyser le fichier « les tontons flingueurs.txt».

- Écrire un programme en python qui analyse ce fichier et le traduit en tableau de fréquence des lettres comme l'exemple du tableau ci-dessous
  - En ne tenant pas compte des accents
    - Exemple : é, è, ê, ë, => e
  - Mettre toutes les lettres en majuscule
  - Donner le nombre exact de lettres totale
  - Créer un « tableau » comme celui ci-dessous trie par fréquence de la plus forte a la plus faible :

•

Fréquence d'apparition des lettres			
Lettre	Fréquence	Lettre	Fréquence
A	8.40 %	N	7.10 %
B	1.00 %	O	5.20 %
C	3.00 %	P	3.00 %
D	4.10 %	Q	0.90 %
E	9.00 %	R	6.50 %
F	1.10 %	S	8.00 %
G	1.20 %	T	7.00 %
H	0.90 %	U	5.70 %
I	7.30 %	V	1.30 %
J	0.30 %	W	0.05 %
K	0.05 %	X	0.40 %
L	6.00 %	Y	0.30 %
M	2.90 %	Z	0.10 %

2.2 **Exo2.3 :** Écrire une fonction python qui analyse le fichier et le traduit en tableau de fréquence des mots

- ▪ En ne tenant pas compte des accents
  - Exemple : é, è, ê, ë, => e
- Mettre toutes les lettres en majuscule
- Donner le nombre de mot dans le texte
  - en tenant compte (« QU'EST » sont 2 Mots => « QU » et « EST »)
- Donner le nombre de mot dans le texte sans les articles (LE, LA ,LES , DE, DES, ...)
- Créer un fichier avec les mots unique trouvé

```
2362
1510
['TONTONS', 'FLINGUEURS', 'USINE', 'MONTEZ', 'VENT', 'FRISQUET', 'COUVERTURE', 'ARRIERE', 'GERMAINE', 'MIS', 'THERMOS',
'QUININE', 'MONTAGNE', 'PARS', 'TIBET', 'EME', 'GUSTAVE', 'BATTRA', 'POUVIEZ', 'MAXIMUM', 'ALIGNER', 'STAND', 'TACHEZ',
'DEPANNEUSE', 'MONOLOGUE', 'POUSSENT', 'INTERDICTION', 'ABANDONNE', 'CACTUS', 'REVIENNE', 'BECHAMEL', 'INFERNALE', 'SUFF
ISAMMENT', 'COMMENCAIT', 'IMPATIENCES', 'PREUVE', 'SURPRISES', 'BORNES', 'TAILLER', 'CLAMSER', 'MACAQUES', 'REVU', 'TRON
CHE', 'AMIE', 'PENSAIS', 'ENVIE', 'MANQUAIS', 'GOUVERNEMENT', 'RAPPELE', 'COUPE', 'CANER', 'ENTERRER', 'PANTIN', 'VIOQUE
S', 'AMERIQUES', 'CHOUETTE', 'CARBURE', 'RIGUEUR', 'OS', 'DECAMBUTE', 'BETEMENT', 'MOUFLETTE', 'BONNES', 'CONNUE', 'OSEI
LLE', 'TOURNENT', 'SEULES', 'EXPLIQUERA', 'BAH', 'ROULETTE', 'VELOURS', 'PLAN', 'EMMERDEMENTS', 'MISE', 'MIENNES', 'LEGA
LES', 'POTES', 'LIVRERAIS', 'VAUTOURS', 'NOMBRE', 'MALFAISANTS', 'PAILLE', 'DEPOUILLER', 'ELEVER', 'APPRENDRE', 'ANGLAIS
', 'FINIRA', 'ENTENDS', 'GUIGNOL', 'CAME', 'NANAS', 'CHIALER', 'RENDS', 'SALIGAUD', 'MOURIR', 'CAPABLE', 'BARRE', 'REVIE
NS', 'ENTENDRE', 'ENTREZ', 'FIEVRE', 'PARLENT', 'GONZESSES', 'TAILLENT', 'CEDER', 'PARTS', 'SUCCEDE', 'EXACT', 'ORGANISE
R', 'REFERENDUM', 'OBJECTIONS', 'RETENIR', 'DECONNE', 'FOUS', 'INTERESSE', 'FILE', 'DIRECTEMENT', 'AVION', 'AMBULANCE',
```

2.3 Exo-2.3 : Écrire une fonction Python qui permettra de chiffrer tout le fichier « Les_tontons_flingueurs.txt »

- En tenant compte de toutes les lettres
- En tenant compte de la fréquence des lettres

- En prenant comme clé le décalage la lettre médiane des fréquences de l'exercice précédent.
  - Définition : Médiane c'est lorsque qu'une série statistique est ordonnée, la médiane est la valeur entière qui partage cette série en deux séries de même effectif. Il y a donc autant de valeurs inférieures à la médiane que de valeurs supérieures.
- Écrire le résultat dans le fichier « Les_tontons_Code.txt »
- Écrire le déchiffrement dans le fichier « Les_tontons_Decode.txt »

2.4 **Exo-2.5 :Écrire une fonction python qui calcule l'indice de coïncidence pour le fichier codé** « Les_tontons_Code.txt » et **retourner l'indice et la langue du message.**

2.5 **Exo-2.6 : Écrire une fonction Python qui trouve la clé via un dictionnaire et ensuite decode le message ci-dessous**

- Le principe est le suivant :
  - En utiliser le fichiers « Les_tontons.txt » comme dictionnaire
    - Trier les mots précédemment trouvées par ordre de grandeur
    - Comme les espaces ne sont pas codés,
      - La longueur des mots vous donnera par statistique la clé.
    - Decode le texte et de trouver la clé

FR.message 9 :

« "Tj kf tvjt eftdfoev,
kf of sfhsfuufsbj bctpmvnfou sjfo.
Mb ufsnjujfsf gvuvsf n'fqpvwbouf.
Fu kf ibjt mfvs wfsuv ef spcput.

Npj, k'fubjt gbju qpvs fusf kbsejojfs."
Mft efsojfsft mjhoft e'vof mfuusf besfttff b Qjfssf Ebmmpa, fdsjuf mb wfjmmf ef tb npsu, mf 30 kvjmmfu 1944.

Ufyuft
Boupjof ef Tbjou-Fyvqfsz »

2.6 **.Exo-2.6 : En utilisant les méthodes d'indice de coïncidence et d'analyse fréquentielles du tableau créer avec le fichier « les_tontons.txt » sera t'elle efficace ?**

- **Écrire une fonction Python qui trouve la clé permet de déchiffrer le messages 10 par la fréquence des lettres (pour déterminer la clé), en vous aidant de votre fonction du calcul de coïncidence (qui détermine la langue du message)**

message 10 :

"Ow cfgo ozsl ow sjw, tml cfgo fgl ozsl ow esq tw."
Oaddase Kzscwkhwsjw

2.7 .