**CHALLENGE KRYPTON**

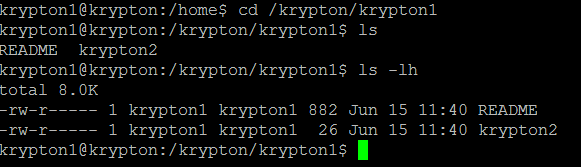
**Krypton1**

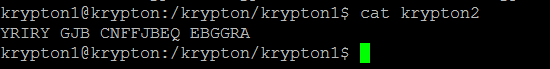
Décodage de la clé en Base64 : **KRYPTONISGREAT**



**Krypton2**

Affichage de la clé pour Krypton2 :



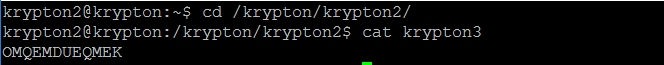


Décodage la clé (ROT13) : **ROTTEN**

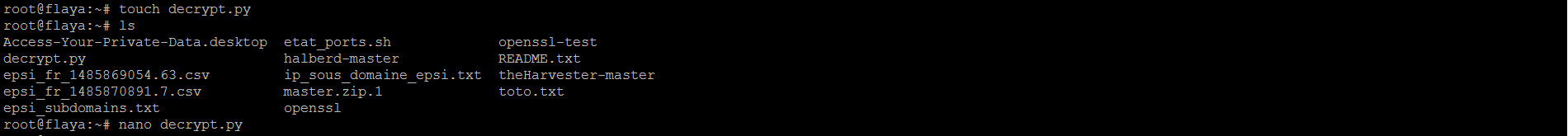


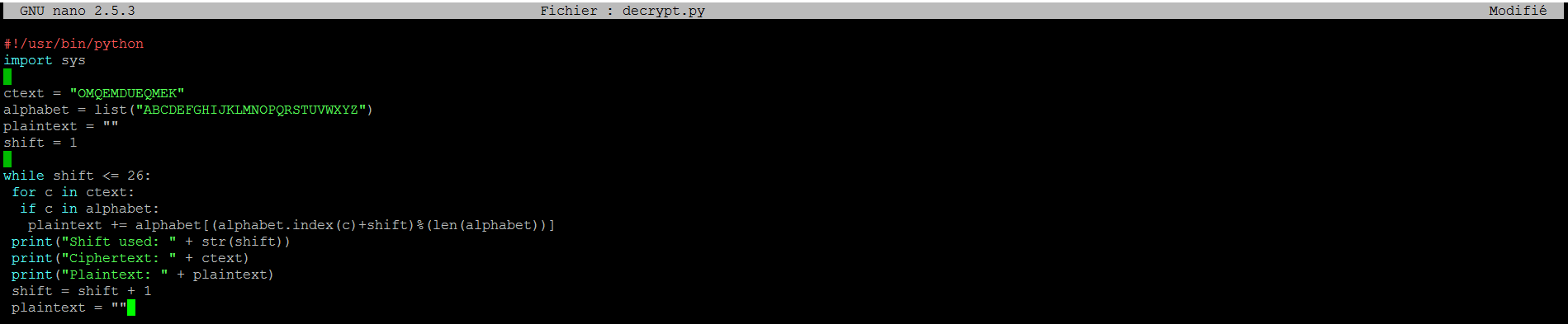
**Krypton3**

Affichage de la clé pour Krypton3 :

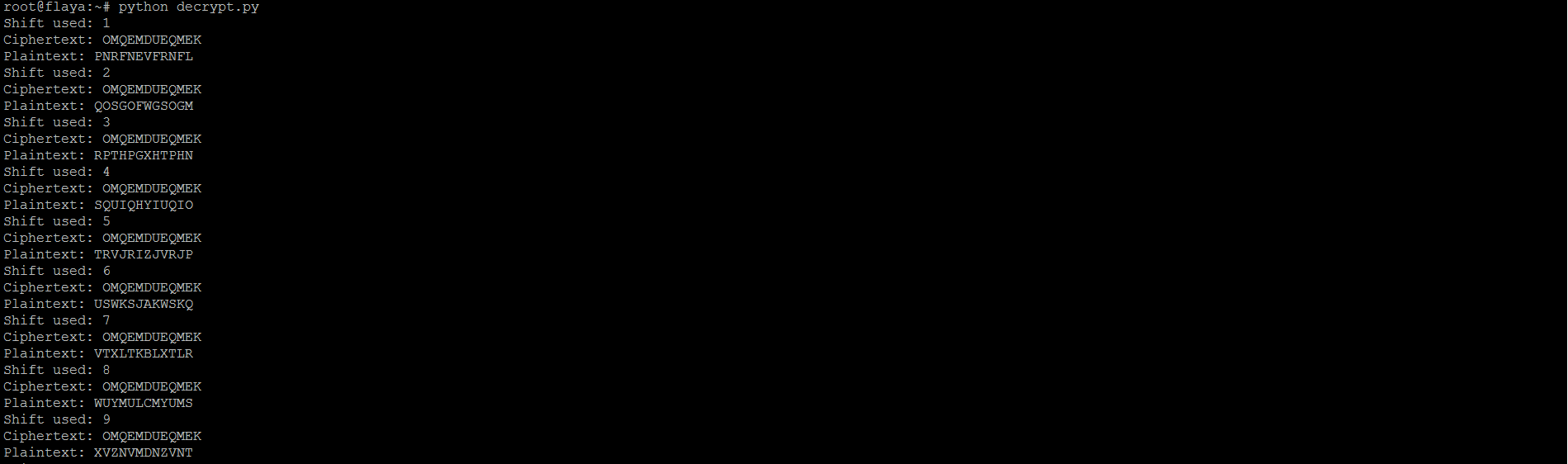


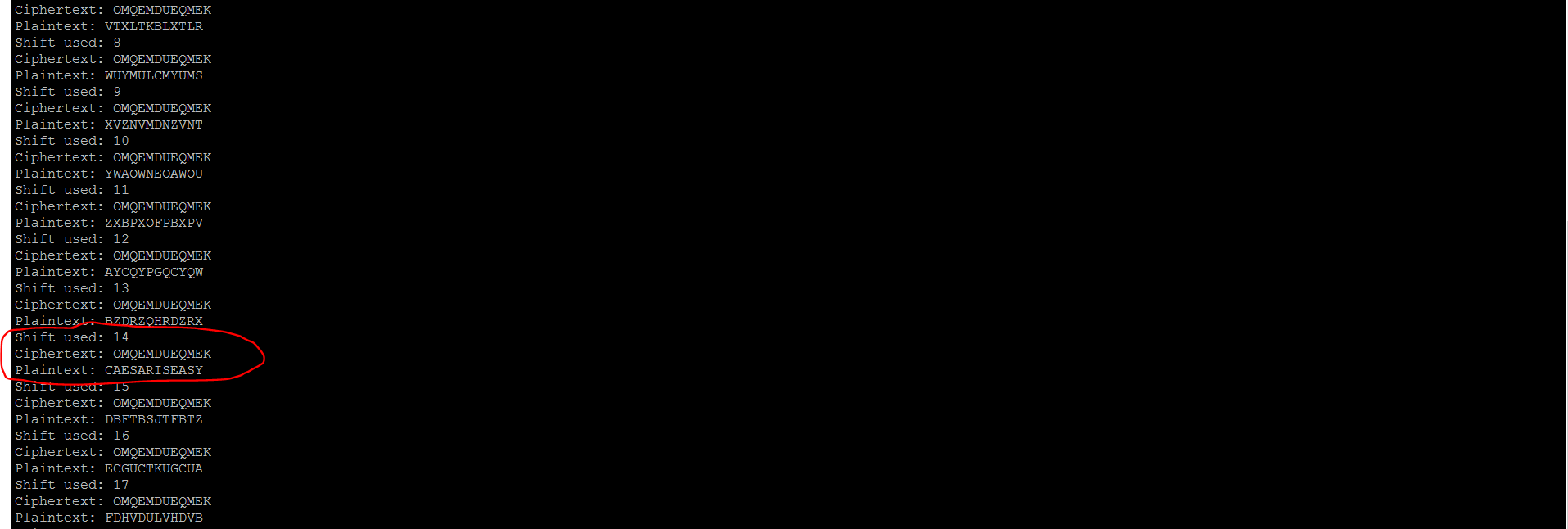
Création d’un script python (en local) :





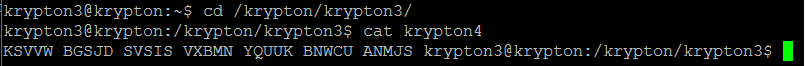
Récupération du résultat le plus probable : **CAESARISEASY**





**Krypton 4**

Affichage de la clé pour Krypton4 :



Analyse de fréquence :

Fréquence des mots anglais

|  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **A** | **B** | **C** | **D** | **E** | **F** | **G** | **H** | **I** | **J** |
| 8.2 | 1.5 | 2.8 | 4.3 | 12.7 | 2.2 | 2.0 | 6.1 | 7.0 | 0.2 |
| **K** | **L** | **M** | **N** | **O** | **P** | **Q** | **R** | **S** | **T** |
| 0.8 | 4.0 | 2.4 | 6.7 | 7.5 | 1.9 | 0.1 | 6.0 | 6.3 | 9.1 |
| **U** | **V** | **W** | **X** | **Y** | **Z** |  |  |  |  |
| 2.8 | 1.0 | 2.4 | 0.2 | 2.0 | 0.1 |  |  |  |  |

On peut les classer par fréquence

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

En utilisant un site d’analyse de fréquence on peut analyser la fréquence des lettres dans les fichiers *found1*, *found2*, et *found3*.

Classement sur *found1*

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

Classement sur *found2*

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

Classement sur *found3*

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

Correspondance

La phrase à décrypter est : **KSVVW BGSJD SVSIS VXBMN YQUUK BNWCU ANMJS**

On cherche les correspondances pour les lettres de la phrase uniquement (classées par fréquence) :

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

Par substitution, on trouve que les meilleures possibilités pour le premier de mot de 5 lettres sont :

WELLD ou WELLU.

On remplace les lettres :

**WELL**WBG**E**JD**ELE**I**EL**XBMNYQUUKBNWCUANMJ**E**

En analyse de fréquence de mot en anglais, il est très probable que la combinaison JDS corresponde à THE.

On remplace :

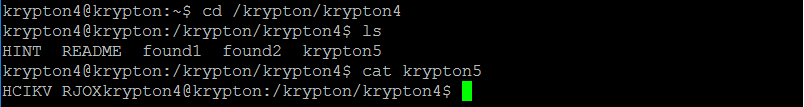
**WELL**WBG**ETHELE**I**EL**XBMNYQUUKBNWCUANM**TE**

**WELLDONETHELEVEL**X**O**MNYQUUK**O**N**D**CUANM**TE**

**WELLDONETHELEVELFOURPASSWORDISBRUTE => Le mot de passe est BRUTE**

**Krypton 5**

Affichage de la clé pour Krypton5 :



Nous allons utiliser la technique suivante pour décrypter le Vigenère :

Tout d’abord, il est nécessaire de diviser le texte en 6 sous-texte correspondant à chaque caractère étant crypté par la même lettre :

**Y**YICSJ**I**ZIBAG**Y**YXRIEWVIXAFNJOOVQ**Q**VHDLC**R**KLBSS**L**YXRIQ**Y**IIOXQ**T**WXRIC**R**VVKPB**H**ZXIYL**Y**ZPDLC**D**IIKG…

Par exemple, la première séquence est :

**YIYWNQRLYTRHYDJTWZSLNNHTMJJYFNYIJJSLWNMFXBBKXIMJTBMIYJJNTYBWKWWLFGWISJSZYSYPJNFJQFWTYWKJJMMNSYWKYSAYMTSQZJRFDMKXFJJPKFSTTTJMBMJDSQIJPFJTSJWJPJIKXISJFFYXMQMYIMZYFSJWJNTWGJYGZTMTYSFFJTWJQBSFSJSJIJJNKWSXZYZKXMSSIFTXSSKTJTYWMYKLTISNJFITWIXNBSJHJF**

Nous allons utiliser la technique de l’analyse de fréquence pour définir une équivalence entre deux lettres. On obtient la liste de fréquence suivante (uniquement les 8 plus fréquents) :

**J** => 37  
**S** => 24  
**Y** => 22  
**T** => 20  
**F** => 18  
**W** => 17  
**M** => 16  
**I** => 14

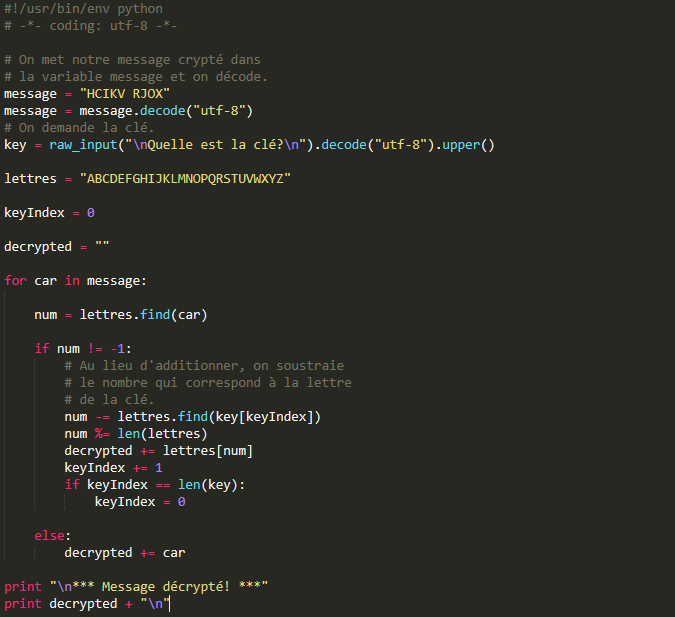
On peut donc en déduire que la lettre la plus fréquente correspond au **E**. Par conséquent le décalage entre **J** et **E** est de 6. La première lettre de la clé est donc **F**.

On répète l’opération pour chacun des 5 sous-textes restants.

On obtient les décalages suivants :

**6 17 5 11 5 25** soit la clé **FREKEY**

On utilise le script Python suivant pour décrypter le mot de passe :



Décryptage du mot de passe avec la clé : **CLEAR TEXT**

