TP1

Exercice 1

Mon programme contient plusieurs arguments possibles :

- **friedman** : calcule la longueur de la clé avec le test de Friedman
- **friedman debug** : idem, avec des logs explicatifs
- **decrypt** : décrypte le message chiffré
- **decrypt debug** : idem, avec des logs explicatifs

Question 1

Pour ceci, il faut se référer à la classe *FriedmanKeyLengthFinder*.

- On sait que la clé a une longueur plus petite ou égale à 9.
- Pour chaque longueur de clé possible (1 à 9) :
  - On génère les sous-textes créées par une clé de cette taille
    - Pour cela, on garde les lettres aux positions $n_k * i + i_k$,
      - n_k: taille de la clé
      - i, : itération pour chaque lettre du sous-texte
      - i_k : itération pour chaque sous-texte
  - Pour chaque sous-texte :
    - On calcule l'indice de coïncidence
      - Pour cela, on se réfère à cette formule
      - $I_C(x) = \frac{\sum_{i=0}^{25} n_i(n_i-1)}{n(n-1)}$
  - On calcule la moyenne des indices de coïncidence des sous-textes
- On garde la moyenne de coïncidence la plus proche de celle de l'anglais (0.066).
- La longueur de clé qui a généré cette moyenne est probablement la bonne.

Question 2

Pour ceci, il faut se référer à la classe *VigenereDecrypter*.

- On utilise la taille de la clé trouvée à la question 1.
- On génère les sous-textes créées par une clé de cette taille (même technique qu'à la question 1)
- Pour chaque sous-texte :
    - Pour chaque décalage possible (0 à 25) :
        - On obtient le sous-texte décalé avec le décalage
            - Il suffit de décaler chaque lettre du sous-titre
            - Si on dépasse l'alphabet, on le recommence.
        - On obtient la distribution des lettres du sous-texte décalé
            - Pour cela, il faut calculer le nombre d'occurence de chaque lettre dans le sous-texte décalé et diviser par sa longueur
        - On compare avec la distribution des lettres en anglais, en calculant le produit scalaire.
    - On garde le décalage qui a obtenu le plus grand produit scalaire. C'est le décalage le plus probable pour ce sous-texte.
- On rassemble les sous-textes décalés, en faisant l'inverse du décalage expliqué à la question 1.
- Voilà, on a le message en clair!