# Cryptographie

Intervenant : Michael FRANÇOIS (`francois@esiea.fr`)

TD1_2 - - Chiffrement de Jules César

## A. Travail à faire sur papier

- **1.** Expliquer comment fonctionne le chiffrement de Jules César et donner une modélisation algébrique.
- **2.** En utilisant la correspondance suivante :

$$\text{Alphabet} \rightarrow \mathbb{Z}_{26} = \{0, 1, \ldots, 25\}$$

  Numériser le texte : "le monde appartient a ceux qui se levent tot"
- **3.** Chiffrer le message précédent en utilisant la méthode de Jules César avec un décalage de 7.
- **4.** Quelles sont les faiblesses de cette méthode de chiffrement ?
- **5.** Que signifie l'intégrité des données en cryptographie ?

## B. Travail à faire sur ordinateur (prog. C)

- **1.** Écrire une fonction `CHIFF_CESAR`, qui permet de chiffrer le contenu d'un fichier `clair.txt` avec la méthode de Jules César. Les paramètres de cette fonction sont le décalage $k$, le nom du fichier en clair et le nom du fichier qui va contenir le texte une fois chiffré. Voilà le prototype de la fonction :

```
void CHIFF_CESAR (int k, char * nom_fic_clair, char * nom_fic_chiff);
```

  Tester cette fonction en utilisant le message "le monde appartient a ceux qui se levent tot".
- **2.** Écrire une fonction `DECHIFF_CESAR`, qui permet de déchiffrer un message chiffré via la méthode de Jules César. Les paramètres de cette fonction sont le décalage $k$, le nom du fichier chiffré et le nom du fichier qui va contenir le texte une fois déchiffré. Voilà le prototype de la fonction :

```
void DECHIFF_CESAR (int k, char * nom_fic_chiff, char * nom_fic_dechiff);
```

  Tester cette fonction sur le message chiffré obtenu précédemment.

- **3.** Déchiffrer ce message en utilisant un décalage de 16.

```
kdujuhdkucudjlyebudjfukjlekivqyhuvhqsjkhuhkduseju
```

► **4.** Récrire cette fois-ci les deux précédentes fonctions pour utiliser un chiffrement/déchiffrement sur la table ASCII.