# Introduction à la sécurité informatique - cryptologie
## TP1 : cryptographie antique et mots de passe

## Sujet de projet

Le sujet de projet en introduction à la sécurité consiste en **un rapport contenant les réponses aux différentes questions des sujets de TP et expliquant vos choix, ainsi que les codes sources produits pour résoudre les exercices**. En plus de la qualité technique des réponses, les points suivants seront évalués :

- La qualité de rédaction et la clarté du rapport,
- La facilité d'utilisation des codes sources fournis.

Vous résoudrez de préférence les exercices en utilisant Python. Si vous souhaitez utiliser un autre langage, faites d'abord valider votre choix.

Le projet peut être réalisé seul ou en binôme.

## 1 Cryptographie antique

**Exercice 1 : chiffrement de César**

1. Réaliser un programme permettant de chiffrer et déchiffrer des messages en utilisant le chiffrement de César pour n'importe quel décalage.
2. Réaliser un programme permettant de cryptanalyser le chiffrement de César en utilisant une attaque de type **brute force**. Bonus : proposer un moyen automatique de trouver le bon texte clair parmi les différentes propositions.

**Exercice 2 : chiffrement de Vigenère**

1. Réaliser un programme permettant de chiffrer et déchiffrer des messages en utilisant le chiffrement de Vigénère.
2. Implémenter le test de Kasiski pour retrouver la longueur de la clé utilisée à partir d'un message chiffré. Vous pourrez trouver le principe de fonctionnement de ce test sur Internet.

3. En utilisant la question précédente, réaliser un programme permettant de cryptanalyser le chiffrement de Vigenère, en utilisant par exemple des analyses fréquentielles.

# 2 Mots de passe

**Exercice 3 : mot de passe faible**

Vous avez récupéré le haché de mot de passe suivant :

`5a74dd4eef347734c8a0a9a3188abd11`

Vous savez que :

- L'algorithme utilisé est **MD5**,
- Le propriétaire de ce mot de passe utilise des mots de passe courants.

Quel est le mot de passe associé à ce haché ? Vous pouvez par exemple utiliser la liste de mots de passe **rockyou.txt** pour chercher. Cette liste peut facilement être trouvée sur Internet.

**Exercice 4 : archive zip protégée**

L'archive `archive.zip` est protégée par un mot de passe. Réalisez un programme pour ouvrir l'archive par **brute force**. Note : ce mot de passe ne contient que des lettres minuscules.

**Exercice 5 : authentification**

Le but de cet exercice est de vous authentifier sur le service disponible à l'addresse `51.195.253.124`, port `12345`. Le mot de passe est un code PIN à 4 chiffres.