NOM :
Prénom :
Groupe :

Fiche d'avancement

Période II : Cryptologie

Téléchargez le notebook de cette période. Suivez les instructions et exercices qu'il contient et remplissez au fur et à mesure cette fiche.

Calculs modulaires

1. Déterminer $x \in [\![0; 123[\![$ tel que $987 \equiv_{123} x$.

2. Déterminer $x \in [\![0; 987[\![$ tel que $1234 \equiv_{987} x$.

Chiffrement de César par paquet de 1

1. Chiffrer le message *BONJOUR* par paquet de 1 avec 29 pour clef.

2. Déchiffrer le message *ADWLSALMFWXGAK* obtenu par le cryptosystème de César par paquet de de 1 avec 2020 pour clef.

Chiffrement de César par paquet de n

1. Quelle est la valeur de retour de `mod2base(5)` ?

2. Déchiffrer le message suivant obtenue par un chiffrement de César par paquet de 2 avec 1983 pur clef.

   $2500 - 1996 - 2190 - 2395 - 2396 - 1359 - 2401 - 1372 - 2001 - 1265 - 2291 - 2488 - 259 - 268 - 2383$

Brute force

1. En langue française, quelle est la `pertinence` de la phrase *COMMENTCAVA* ?

2. En langue anglaise, quelle est la `pertinence` de la phrase *COMMENTCAVA* ?

3. Combien de temps l'attaque du `MESSAGE` vous a pris avec une brute force ? Avec une brute force avec dictionnaire ?

Chiffrement de Vigénère

1. Chiffrer le message *VIGENERECESTGRAVEFACILE* avec *CLEF* pour clef.

2. Qui était Vigénère ?

3. Qui était Kasiski ?

4. Sans compter les espaces, caractères ponctués ou spéciaux (bref en appliquant le `Filtre`), quelles sont les cinq lettres les plus fréquentes de "Les misérables" de V. Hugo ?

Lettre					
Freq					

5. Qui est l'auteur du dernier message du TP et qui en est le traducteur ?